The exact L^1–L^2 constant of biased bits for every $q \in (0,1)$: a complete proof of Conjecture S

$$R(q) = 2\sqrt{q(1-q)}\ \max_{k\ge 1} \sqrt{k}\,\hat{q}^{\,k-1}, \qquad \hat{q} = \max(q, 1-q).$$

Solvers: RQ-A, RQ-B, RQ-C, RQ-D
Auditor: RQ-AUD Referees: RQ-REF1, RQ-REF2, RQ-REF3

Assembled by RQ-A for Paata Ivanisvili

23 October 2026

Every proof below is transcribed from a source that the team's auditor and an independent referee both rated VALID. Notation and numbering were harmonised; no mathematics was changed. The few editorial additions are set in sans-serif and listed in Appendix C.

Abstract

For $q \in (0,1)$ let $\chi_1, \chi_2, \dots$ be independent random variables, each equal to $\sqrt{(1-q)/q}$ with probability q and to $-\sqrt{q/(1-q)}$ with probability $1-q$, and let

$$R(q) = \sup_{n \geq 1} \sup_{\alpha \in \mathbb{R}^n \setminus \{0\}} \frac{\mathbb{E}\left|\sum_{i=1}^n \alpha_i \chi_i\right|}{\|\alpha\|_2}$$

be the best constant in the L^1–L^2 inequality for these normalised biased bits. We prove Conjecture S: for every $q \in (0,1)$,

$$R(q) = 2\sqrt{q(1-q)} \max_{k \geq 1} \sqrt{k}\, \hat{q}^{\,k-1}, \qquad \hat{q} = \max(q, 1-q),$$

and the supremum is attained by equal coefficients on k coordinates.

The proof has five parts.

- Part I proves the formula on the middle range $[q_6, 1-q_6] = [1-\sqrt{5/6}, \sqrt{5/6}]$, one regime $k = 1, \dots, 5$ at a time. It splits off the largest coefficients and bounds the rest by moment certificates; the finitely many inequalities left are checked in exact rational arithmetic or in outward-rounded interval arithmetic.
- Part II reduces the range $(0, q_5]$, $q_5 = 1 - 2/\sqrt{5}$, to one q-free inequality $\mathrm{ID}^*(C_5)$ for centred infinitely divisible laws Z_K, by Poissonisation. Here $C_5 = g(2\ln\frac{5}{4}) = 0.85510\dots$ and $g(\lambda) = 2\sqrt{\lambda}\, e^{-\lambda}$.
- Part III shows that only Kolmogorov measures K carried by $[-1.54, 1.54]$ are needed.
- Part IV proves $\mathrm{ID}^*(C_5)$ on a band around the Dirac laws and on the heavy part of the far region. Part V proves $\mathbb{E}|Z_K| \leq \frac{171}{200} < C_5$ on the light part. Both parts are computer-assisted, with every decision made in ball or exact rational arithmetic.

The mirror $q \mapsto 1-q$ covers $[1-q_5, 1)$.

Every link was rated VALID by the team's auditor and by an independent referee. The referees re-did every computer-assisted step with their own code. This document contains the verified proofs in full. Only notation and numbering were harmonised, and every choice this required is listed in Appendix C.

Contents

Abstract **i**

Introduction **vi**
The problem and the theorem . . . vi
History . . . vii
The strategy in plain language . . . vii
Status: audit and referee . . . viii
How this document was assembled . . . ix

Notation and conventions **x**
Global notation . . . x
Local notation . . . xi
Numbering and cross-references . . . xii

Roadmap and the proof of the Main Theorem **xiii**
Which result covers which values of q . . . xiii
How the small-q chain fits together . . . xiii
Proof of the Main Theorem . . . xiii

I The middle range $[q_6, 1 - q_6]$ **1**

1 The central range $[q_2, 1 - q_2]$: Theorem 1 (RQ-A) **2**
1.1 Statement . . . 3
1.2 Reductions . . . 3
1.3 Moments of the remainder . . . 4
1.4 Six-moment certificates . . . 5
1.5 The quartic two-extremiser certificate . . . 7
1.6 The near-dictator range . . . 9
1.7 The computer-assisted verifications . . . 10
1.8 Proof of Theorem 1.1 . . . 12
1.9 Remarks . . . 12
A sample certificate (appendix of the source paper) . . . 13

2 The $k = 2$ regime $[q_3, q_2]$: Theorem 2 (RQ-A) **14**
2.1 Statement . . . 15
2.2 Reductions . . . 15
2.3 Exact evaluations . . . 17

2.4 Moments of the remainder . . . 18
2.5 The one-coordinate route ($a_1 \le \frac{9}{20}$) . . . 20
2.6 The two-coordinate route: box certificates . . . 20
2.7 Near the extremiser: the near-circle lemma . . . 21
2.8 Near the triple point: the m-split . . . 22
2.9 Computer verification . . . 23
2.10 Proof of Theorem 2.1 . . . 25
2.11 Remarks . . . 26

3 The $k = 3$ regime, upper part $[q_L, q_3]$: Theorem 3 (RQ-A) 27
3.1 Statement . . . 28
3.2 Reductions . . . 29
3.3 Exact evaluations . . . 30
3.4 Moments of the remainder . . . 32
3.5 The one-coordinate route ($a_1 \le \frac{2}{5}$) . . . 33
3.6 The two-coordinate route: box certificates . . . 34
3.7 Near $(e_1 + e_2)/\sqrt{2}$: the near-circle lemma . . . 35
3.8 Near the extremiser $(e_1 + e_2 + e_3)/\sqrt{3}$: the m-split . . . 35
3.9 Computer verification . . . 37
3.10 Proof of Theorem 3 . . . 39
3.11 Remarks . . . 39

4 The $k = 3$ regime, lower part $[q_4, q_L]$: Theorem 4 (RQ-A) 41
4.1 Statement . . . 42
4.2 Reductions . . . 43
4.3 Exact evaluations . . . 45
4.4 Moments of the remainder . . . 47
4.5 The one-coordinate route ($a_1 \le \frac{7}{20}$) . . . 49
4.6 The two-coordinate route: vertex certificates . . . 49
4.7 Near $(e_1 + e_2)/\sqrt{2}$: the near-circle lemma . . . 52
4.8 Near the extremisers: the m-split . . . 53
4.9 Computer verification . . . 56
4.10 Proof of Theorem 4 . . . 58
4.11 Remarks . . . 59

5 The $k = 4$ regime $[q_5, q_4]$: Theorem 5 (RQ-A) 60
5.1 Statement . . . 61
5.2 Reductions . . . 62
5.3 Exact evaluations . . . 64
5.4 Moments of the remainder . . . 66
5.5 The one-coordinate route ($a_1 \le \frac{33}{100}$) . . . 68
5.6 The two-coordinate route: vertex certificates . . . 69
5.7 Near $(e_1 + e_2)/\sqrt{2}$: the near-circle lemma . . . 73
5.8 Near the extremisers: the m-split . . . 74
5.9 Computer verification . . . 79
5.10 Proof of Theorem 5 . . . 82
5.11 Remarks . . . 83

6 The $k = 5$ regime $[q_6, q_5]$: Theorem 6 (RQ-A) 84
6.1 Statement . . . 85
6.2 Reductions . . . 86
6.3 Exact evaluations . . . 88
6.4 Moments of the remainder . . . 90
6.5 The one-coordinate route ($a_1 \le \frac{1}{4}$) . . . 92
6.6 The two-coordinate route: vertex certificates . . . 93
6.7 Near $(e_1 + e_2)/\sqrt{2}$: the near-circle lemma . . . 97
6.8 Near the extremisers: the m-split . . . 98
6.9 Computer verification . . . 101
6.10 Proof of Theorem 6 . . . 105
6.11 Remarks . . . 106

II Poissonisation: the reduction of $(0, q_5]$ to a q-free inequality 108

7 Level-one form, Poissonisation and the reduction (RQ-B; RQ-A U.1–U.3) 109
7.1 Setting and notation . . . 110
7.2 Equal coefficients . . . 110
7.3 Level-one form . . . 111
7.4 Poissonization . . . 111
7.5 Size of the window . . . 114
7.6 RQ-A's formulation of the reduction: U.1–U.3 . . . 115

III Localisation of maximisers 117

8 Localisation of maximisers at finite q (RQ-C, claim C15) 118
8.1 Notation . . . 118
8.2 Statement and proof . . . 119

IV The band and the heavy far region 121

9 The band lemma and the heavy far region (RQ-D) 122
9.1 Setting . . . 124
9.2 Exact identities . . . 124
9.3 A comparison lemma for stop-loss terms . . . 125
9.4 The jump law and the band bound . . . 127
9.5 The band lemma for C5 . . . 128
9.6 The band lemma in the form needed at finite q . . . 130
9.7 The heavy part of the far region . . . 135

V The light far region 143

10 The light far region (RQ-B, Section 13) 144
10.1 Notation . . . 145
10.2 The split chain . . . 145

10.3 Cells and certificates . . . 146
10.4 Decomposition and cells . . . 147

A Computer-assisted steps **150**
Which steps are computer-assisted . . . 150
Conventions . . . 150
Overview . . . 151
Safeguards . . . 152
Part I: the middle range (Theorems 1–6) . . . 152
Part IV: the band (Theorem 9.13) . . . 155
Part IV: the heavy far region (Theorem 9.16) . . . 156
Part V: the light far region (Theorem 10.1) . . . 156
Numerical constants of Parts II and III . . . 158
Tight margins . . . 158
Evidence that is not part of the proof . . . 158
Register of programs and data files . . . 158

B Audit and referee ledger **162**
Sources of this ledger . . . 162
Vocabulary . . . 162
The reporting rule and how it was met . . . 162
Audit verdicts on the links of the proof . . . 163
The referees . . . 164
Fixes and remarks . . . 165
Timeline . . . 166

C Transcription notes **167**
Source files . . . 167
Mechanical changes . . . 168
The editorial apparatus . . . 168
Edits to source text . . . 170
Plain-text sources . . . 170
Machine checks . . . 170
How this document is built . . . 171

D Concordances **172**
RQ-A's papers and claims . . . 172
RQ-B's paper . . . 172
RQ-D's paper . . . 173
RQ-C's claim C15 . . . 173
RQ-REF3's links and this document . . . 173

References **175**

Introduction

The problem and the theorem

Let $q \in (0,1)$ and put

$$u = \sqrt{\frac{1-q}{q}}, \qquad v = \sqrt{\frac{q}{1-q}} = \frac{1}{u}, \qquad \tau = \sqrt{q(1-q)} = qu = (1-q)v.$$

Let $\chi, \chi_1, \chi_2, \dots$ be independent and identically distributed with $\mathbb{P}(\chi = u) = q$ and $\mathbb{P}(\chi = -v) = 1-q$. Then $\mathbb{E}\chi = 0$, $\mathbb{E}\chi^2 = 1$ and $\mathbb{E}|\chi| = 2\tau$; equivalently $\chi = (X-q)/\tau$ with $X \sim \text{Bernoulli}(q)$. Define

$$R(q) = \sup_{n \geq 1} \sup_{\alpha \in \mathbb{R}^n \setminus \{0\}} \frac{\mathbb{E}\left|\sum_{i=1}^n \alpha_i \chi_i\right|}{\|\alpha\|_2}.$$

Cauchy–Schwarz gives $R(q) \leq 1$, and replacing χ by $-\chi$ gives $R(q) = R(1-q)$ (Lemma 1.2). One coordinate gives $R(q) \geq 2\tau$. If $q \leq \frac{1}{2}$ and $kq < 1$, then k equal coefficients give

$$\frac{\mathbb{E}|\chi_1 + \cdots + \chi_k|}{\sqrt{k}} = T_k(q) := 2\sqrt{kq}\,(1-q)^{k-1/2} = 2\sqrt{k}\,(1-q)^{k-1}\,\tau$$

(Theorem 7.4).

Main Theorem (Conjecture S)**.** *For every $q \in (0,1)$,*

$$R(q) = M(q) := 2\sqrt{q(1-q)}\,\max_{k \geq 1} \sqrt{k}\,\hat{q}^{\,k-1}, \qquad \hat{q} = \max(q, 1-q). \tag{S}$$

Let $p = \min(q, 1-q)$. The maximum in (S) *is attained at $k = \lfloor 1/(p(2-p)) \rfloor$, and also at $k-1$ exactly when $p = 1 - \sqrt{(k-1)/k}$. The supremum defining $R(q)$ is attained at $\alpha = (1, \dots, 1)/\sqrt{k} \in \mathbb{R}^k$.*

With $q_k := 1 - \sqrt{(k-1)/k}$ $(k \geq 2)$, the maximiser is k on the closed band $[q_{k+1}, q_k]$, where $M = T_k$; the neighbours $k \pm 1$ tie with k at the two ends. So $M(q) = 2\tau$ on $[q_2, \frac{1}{2}]$, $M(q) = 2\sqrt{2}\,(1-q)\tau$ on $[q_3, q_2]$, $M(q) = 2\sqrt{3}\,(1-q)^2\tau$ on $[q_4, q_3]$, and so on, with $M(1-q) = M(q)$. The proof is assembled in the Roadmap chapter (page xiii).

Remark (an equivalent Boolean form). By Lemma 7.5, $R(q)^2 = 4q(1-q)\sup_f D(f)$, where f runs over all functions $\{0,1\}^n \to [0,1]$ $(n \geq 1)$, the cube carries the product Bernoulli(q) measure, $\Delta_i(f) = \mathbb{E}[f \mid x_i = 1] - \mathbb{E}[f \mid x_i = 0]$ and $D(f) = \sum_i \Delta_i(f)^2$. So the Main Theorem says that

$$\sum_i \Delta_i(f)^2 \leq \max_{k \geq 1} k\,\hat{q}^{\,2k-2}$$

for every such f, with equality for the OR of k bits if $q \leq \frac{1}{2}$, and for the AND of k bits if $q \geq \frac{1}{2}$, where k attains the maximum. (This restatement is editorial; it is immediate from Lemma 7.5.)

Remark (extremisers). On $[q_6, 1-q_6]$ the extremisers are determined completely: part (c) of Theorem 1 and part (b) of Theorems 2–6 list them (for example, on $(q_2, 1-q_2)$ they are $\pm e_i$). For $q < q_6$ or $q > 1-q_6$ the proof gives the value $R(q)$ and the equal-coefficient extremiser, but it does not show that there are no others.

History

The constant $R(q)$ comes from the study of the L^1-Poincaré inequality on the Hamming cube. Ivanisvili, Li, van Handel and Volberg [ILvHV, Theorem 3.1] showed that $R(q) < 1$ for q in a small interval around $\frac{3}{4}$, and used this to improve the constant $\frac{\pi}{2}$ in the L^1-Poincaré inequality on the cube. Van Handel then proved the quantitative bound $R(q) \le \big(1 - \frac{1}{480}\min\{4q^3(1-q)^3, (2q-1)^4 q(1-q)\}\big)^{1/2}$ (a private communication, quoted as [IS, (1.7)]), and Ivanisvili and Stone [IS, Corollary 2] improved it to $R(q) \le 1 - \min\{4q^3(1-q)^3, (2q-1)^4 q(1-q)\}/(45 - 3(q(1-q))^3)$. These upper bounds are close to 1. Stone's thesis [St] computes two families exactly: two coefficients (its Section 4.2, where $\alpha = (1,1)/\sqrt{2}$ beats one coordinate for $q < 1 - 1/\sqrt{2}$) and equal coefficients (its Theorem 4.3.1). The value of k equal coefficients, maximised over k, is the right-hand side of (S). It is quoted as [IS, (1.10)], and [IS, Remark 1.3] works out what would follow for the L^1-Poincaré inequality if $R(q)$ were equal to it. We call the statement that $R(q)$ equals it for every $q \in (0,1)$ Conjecture S.

For the central range, BF3 [BF3], a report by an earlier team of AI agents on list-decoding thresholds of approximate polymorphisms that was supplied with the problem, proved in its Theorem K (Section 9.4) that $R(q) = 2\sqrt{q(1-q)}$ for $q \in [\frac{3}{8}, \frac{5}{8}]$. The proof uses Stein's method and an exact rational interval computation. BF3 conjectured [BF3, Remark 9.8(c)] that $R(q) = 2\sqrt{q(1-q)}$ holds exactly for $1 - \frac{1}{\sqrt{2}} \le q \le \frac{1}{\sqrt{2}}$; at $q = 1 - \frac{1}{\sqrt{2}}$ both e_1 and $(e_1 + e_2)/\sqrt{2}$ would be extremal.

This document reports the work of a team of AI agents on Paata Ivanisvili's question "can you find $R(q)$ for all q?", between 21 and 23 October 2026. The team had four solvers (RQ-A, RQ-B, RQ-C, RQ-D), a hostile auditor (RQ-AUD), and three independent referees (RQ-REF1, RQ-REF2, RQ-REF3). The BF3 conjecture is Theorem 1 (Chapter 1). Theorems 2–6 (Chapters 2–6) extend the formula, regime by regime, to $[q_6, 1-q_6]$. Chapters 7–10 handle all small q at once.

The strategy in plain language

What is being maximised. Each χ_i is a centred, normalised coin that comes up "heads" with probability q. We weight n such coins and ask how large the mean absolute value of the sum can be, relative to its standard deviation. For q near $\frac{1}{2}$ the best choice is to put all the weight on one coin. As q decreases, heads become rare events, and it pays to spread the weight evenly over k coins. Then the sum is negative only when all k coins show tails, and k is about $1/(2q)$. The best k jumps at the thresholds q_k. So the conjectured answer $M(q)$ is the upper envelope of the curves T_k. The lower bound $R \ge M$ is this computation (Theorem 7.4). All the work is in the upper bound $R \le M$.

The middle range (Part I). For each $k = 1, \dots, 5$ we prove $\mathbb{E}|\sum \alpha_i \chi_i| \le T_k(q)\|\alpha\|_2$ for q in the band of k. Write the sum as $a\chi_1 + b\chi_2 + (\text{remainder})$ with the largest coefficients $a \ge b$ in front. Exact identities reduce the problem to bounding an expectation of a piecewise-linear function of the remainder. The first six moments of the remainder are fixed by power sums of its coefficients, and these are controlled by a and b. A polynomial "moment certificate" then bounds the expectation

on a cell of (a, b)-space. The certificates must be exact at the extremisers, so they degenerate there; separate lemmas (the near-circle lemma, the m-split, the quartic certificate, the bit lemmas) cover small neighbourhoods of the extremisers. Finitely many polynomial inequalities remain, and they are checked by computer in exact rational arithmetic or in outward-rounded interval arithmetic. This works for each fixed k, but every k needs a new and larger computation, so it cannot reach all small q.

Small q: Poissonisation (Part II). When q is small, a sum of many rare coins looks like a compound Poisson variable. Poissonisation makes this exact at every fixed q. Take a maximiser, and let f be the indicator that its sum is positive. Replace each bit x_i by the event that a Poisson(s) count is positive, where $s = \ln \frac{1}{1-q}$. Stein's identity for the Poisson law then gives $R_n(q) \le \sqrt{q/((1-q)s)}\, \mathbb{E}|Z_K|$, where Z_K is a centred compound Poisson variable whose jump sizes are the normalised coefficients. The expected number of jumps of size at least θ is always an integer multiple of s, and this is exactly what produces the discrete maximum over k in (S). So everything reduces to one q-free inequality:

$$\mathrm{ID}^*(C): \qquad \mathbb{E}|Z_K| \le \max\bigl(g(\lambda_\theta^+(K)),\, g(\lambda_\theta^-(K)),\, C\bigr),$$

where $\lambda_\theta^{\pm}(K)$ is the expected number of jumps of size $\ge \theta$ (resp. $\le -\theta$), and $g(\lambda) = 2\sqrt{\lambda}\, e^{-\lambda}$ is $\mathbb{E}|Z|$ when all jumps have the same size. With $C = C_5$ this yields $R = M$ on all of $(0, q_5]$ (Theorem 7.9).

No huge coefficients (Part III). The first-order optimality conditions of a maximiser show that no coefficient can be large: every jump of the measure K produced above lies in $[-A'(q), A'(q)]$, and $A'(q) \le A'(q_5) = 1.53804\ldots < 1.54$ (Theorem 8.1). So $\mathrm{ID}^*(C_5)$ is needed only for K carried by $[-1.54, 1.54]$.

Proving $\mathrm{ID}^*(C_5)$ (Parts IV–V). Fix $\theta = 0.85$ and sort K by the masses V_+ and V_- that it puts on the large jumps $[0.85, 1.54]$ and $[-1.54, -0.85]$.

- *Band* ($V_+ \ge \frac{4}{5}$ or $V_- \ge \frac{4}{5}$). This region contains the Dirac laws $K = \delta_a$, where the inequality holds with equality, so the bound must be sharp to first order. An exact identity isolates the extremal Poisson part. The residual enters only through two stop-loss terms, which a new comparison lemma bounds (Theorem 9.13).
- *Heavy far region* ($\frac{1}{2} \le V_\pm < \frac{4}{5}$). The large jumps are replaced by their chord law, which is larger in convex order. Everything else enters through a degree-16 moment certificate (Theorem 9.16).
- *Light far region* ($V_+ < \frac{1}{2}$ and $V_- < \frac{1}{2}$). Here there is room to spare: $\mathbb{E}|Z_K| \le \frac{171}{200} = 0.855 < C_5 = 0.85510\ldots$ The proof spreads windows of jumps to two points (a convex-order step) and uses 10 966 exact moment certificates (Theorem 10.1).

Assembly. The middle range, the small-q range $(0, q_5]$ and its mirror image cover $(0, 1)$, and adjacent ranges share their closed endpoints.

Status: audit and referee

The team rule (Paata Ivanisvili's locked note) was: report only results rated VALID by the auditor *and* by an independent referee. The auditor RQ-AUD rebuilt every proof from its hypotheses and

re-ran every computation with its own code. Three referees, who took no part in the work, then did the same independently. RQ-REF1 refereed Theorems 1–4, RQ-REF2 Theorems 5–6, and RQ-REF3 the small-q chain (Parts II–V) and the composition. Every verdict on every link is VALID, with no fix affecting a proof. Appendix B lists the verdicts with their identifiers, the report files and their md5 sums, and the referees' remarks. The coordinator reported the complete result to Paata Ivanisvili at 20:10 PT on 22 October 2026 (03:10 UTC on 23 October).

How this document was assembled

- The proofs are transcribed from the refereed source files, identified by md5 in each chapter's source box and in Appendix C. Chapters 1–6 and 9 reproduce entire papers. Chapters 7 and 10 reproduce the sections of RQ-B's paper that the chain uses. Chapter 8 transcribes into LaTeX RQ-C's claim C15, whose source is plain text. A script (`scripts/build_full_proof.py`) extracts the LaTeX sources and checks their md5 sums.
- The only changes are mechanical: label names are prefixed by the chapter, sectioning levels are shifted, abstracts become quoted blocks, and the theorem styles are unified. Editorial material is set in sans-serif: footnotes headed "Editorial note", bracketed source tags, framed blocks headed "Supplement transcribed from ...", and the chapter source boxes. No mathematical statement or proof was altered. Slips that the auditor or a referee noted are kept as written and flagged in a footnote.
- Cross-references inside a chapter are live. References between the source papers by file name, for example "Theorem 5 of `MAIN_RESULT_K4`", are kept as written. The table on page xii and Appendix D translate them.

Notation and conventions

Global notation

The following symbols have the same meaning in every chapter, except where a local redefinition is listed in the next section.

symbol	meaning
q, $\hat{q}$, p	$q \in (0,1)$; $\hat{q} = \max(q, 1-q)$; $p = \min(q, 1-q)$ (used in the Introduction only)
u, v, τ	$u = \sqrt{(1-q)/q}$, $v = \sqrt{q/(1-q)} = 1/u$, $\tau = \sqrt{q(1-q)} = qu = (1-q)v$
χ, χ_i, $\chi^{(q)}$	i.i.d., $\mathbb{P}(\chi = u) = q$, $\mathbb{P}(\chi = -v) = 1-q$; $\chi = (X-q)/\tau$ with $X \sim \text{Bernoulli}(q)$; the superscript shows the parameter when two values occur
L, $R_n(q)$, $R(q)$	$L = \sum_i \alpha_i \chi_i = \alpha \cdot \chi$ for a unit vector α; $R_n(q) = \max_{\lvert\alpha\rvert=1,\, \alpha \in \mathbb{R}^n} \mathbb{E}\lvert L\rvert$; $R(q) = \sup_n R_n(q)$
e_i, $\mathbf{1}_S$	standard basis vectors; $\mathbf{1}_S = \sum_{i \in S} e_i$
$T_k(q)$	$2\sqrt{kq}\,(1-q)^{k-1/2} = 2\sqrt{k}\,(1-q)^{k-1}\tau$, the value of $\mathbf{1}_k/\sqrt{k}$ when $kq < 1$, $q \le \frac{1}{2}$ (Chapters 3 and 4 write T for T_3; Chapters 1–2 write 2τ and T, resp. S_2)
$M(q)$	$2\tau \max_{k \ge 1} \sqrt{k}\,\hat{q}^{\,k-1}$; for $q \le \frac{1}{2}$, $M(q) = \max_k T_k(q)$
q_k $(k \ge 2)$	$1 - \sqrt{(k-1)/k}$, where $T_{k-1}(q_k) = T_k(q_k)$; $M = T_k$ on $[q_{k+1}, q_k]$
	$q_2 = 1 - \frac{1}{\sqrt{2}} = 0.292893\ldots$, $q_3 = 1 - \sqrt{2/3} = 0.183503\ldots$,
	$q_4 = 1 - \frac{\sqrt{3}}{2} = 0.133974\ldots$,
	$q_5 = 1 - \frac{2}{\sqrt{5}} = 0.105572\ldots$, $q_6 = 1 - \sqrt{5/6} = 0.087129\ldots$
q_L	$\frac{25}{169} = 0.147928\ldots$, the boundary between Chapters 3 and 4
$s = s(q)$	$\ln \frac{1}{1-q}$, so that $1 - q = e^{-s}$
$g(\lambda)$	$2\sqrt{\lambda}\,e^{-\lambda}$ $(\lambda \ge 0)$; $\max g = g(\frac{1}{2}) = \sqrt{2/e} = 0.857763\ldots$
$C(q)$, C_K	$C(q) = \max_{k \ge 1} g(ks)$; for $q \le \frac{1}{2}$, $M(q) = \sqrt{q/((1-q)s)}\,C(q)$, equation (7.1); $C_K = \min_{0 < q \le q_K} C(q) = C(q_K)$ (Theorem 7.9(d))
C_5	$g(2\ln\frac{5}{4}) = 1.28\sqrt{2\ln 1.25} = 0.855100455470819\ldots$; $C_4 = 0.853343\ldots$, $C_6 = 0.855984\ldots$
Kolmogorov measure K	a finite Borel measure on $\mathbb{R}$ (in Parts II–V usually a probability measure)
Z_K	the centred infinitely divisible law with $\log \mathbb{E}e^{itZ_K} = \int (e^{itx} - 1 - itx)x^{-2}K(dx)$; $\mathbb{E}Z_K^2 = K(\mathbb{R})$; for finitely supported $K = \sigma^2\delta_0 + \sum_j w_j \delta_{a_j}$: $Z_K = \sigma G + \sum_j a_j(N_j - w_j/a_j^2)$, $N_j \sim \text{Poisson}(w_j/a_j^2)$

symbol	meaning (continued)
$\lambda_\theta^{\pm}(K)$	$\int_{\pm x \ge \theta} x^{-2} K(dx)$ (closed thresholds): the expected number of jumps of size $\ge \theta$, resp. $\le -\theta$. Chapter 7 writes $\lambda_\pm(K)$, Chapter 10 does not use it, and in Chapter 9 $\Lambda = \lambda_\theta^+(K)$
$\mathrm{ID}^*(C)$	every finitely supported probability measure K on $\mathbb{R} \setminus \{0\}$ has some $\theta = \theta(K) > 0$ with $\mathbb{E}\lvert Z_K\rvert \le \max(g(\lambda_\theta^+(K)), g(\lambda_\theta^-(K)), C)$ (Theorem 7.9(d)); the chain proves it with $\theta = \frac{17}{20}$ for every K carried by $[-\frac{77}{50}, \frac{77}{50}]$
θ, A, $V_\pm$	in Parts IV–V: $\theta = \frac{17}{20}$, $A = \frac{77}{50}$, $V_+ = K([\theta, A])$, $V_- = K([-A, -\theta])$
$A'(q)$	$\sqrt{2q/s}/(1-q)$ (Theorem 8.1(f)); increasing, with $A'(q_5) = \sqrt{5q_5/\ln\frac{5}{4}} = 1.538044391650755\ldots < \frac{77}{50}$
$\Delta_i(f)$, $D(f)$	for $f : \{0,1\}^n \to [0,1]$ under the Bernoulli(q) product measure, $\Delta_i(f) = \mathbb{E}[f \mid x_i = 1] - \mathbb{E}[f \mid x_i = 0]$, $D(f) = \sum_i \Delta_i(f)^2$
K_f, $\tilde{K}$	$\sum_i \beta_i^2 \delta_{\beta_i/\sqrt{s}}$ with $\beta = \Delta(f)/\sqrt{D(f)}$ (Chapter 7 writes K_f, Chapter 8 writes $\tilde{K}$)
OR_S, OR_k	the indicator that some bit of S (of k given bits) equals 1
R_{ID}	$\sup_K \mathbb{E}\lvert Z_K\rvert$ over probability Kolmogorov measures (Definition 7.1)
$X \le_{cx} Y$	convex order: $\mathbb{E}f(X) \le \mathbb{E}f(Y)$ for every convex f

Two names that must not be confused. *Conjecture C5* (no subscript; Conjecture 7.3) is the statement $R_{\mathrm{ID}} = \sqrt{2/e}$. It is *not* used in the proof of the Main Theorem. The *constant* C_5 (with subscript) is $g(2\ln\frac{5}{4})$. Chapters 7 and 9 also state C5 conclusions as by-products. These rest on results of RQ-B that are not reproduced here, and the Main Theorem does not depend on them.

Local notation

The sources reuse some letters locally. We kept the source notation inside each chapter (changing it would change the transcribed text), so the reader should note the following.

- q_0. In Chapters 1 and 2, and in RQ-B's text in Chapter 7, $q_0 = 1 - \frac{1}{\sqrt{2}}$, which is q_2 in the global notation.
- M. In Chapters 1–6, M usually denotes the remainder $\sum \beta_i \chi_i$ (a random variable), not the function $M(q)$. In Section 9.7, $M(a,b) = a\tau^2 + bA^2$, and in the band computations of Chapter 9 M is a bound for $2me^{-\Lambda}$.
- τ. In Sections 9.5.1 and 9.6.1, $\tau(x) = \mathbb{E}(G-x)_+^2$, and in Section 9.7, $\tau = \frac{17}{20}$ (the threshold that is called θ elsewhere).
- g. Proposition 7.11 uses $g(x) = \sqrt{2ex}\,e^{-x} = g_{\mathrm{global}}(x)/\sqrt{2/e}$; Remark 7.8 uses $g(y) = \ln(1-y) + y/(1-\frac{2}{3}y)$; the proof of Theorem 7.6 uses a bounded test function g; the proof of Theorem 8.1(a) uses $g(t) = R_n(1 + 2t\alpha_i + t^2)^{1/2}$; Section 9.7 uses $g(x) = x^{j-2} - s_3 x - s_4 x^2$ in inequalities (a) and (b).
- K. In Chapter 7, K is an integer in q_K, C_K and a measure elsewhere.
- s. In Lemma 10.6, $s = K_W([\theta, b])$ is a mass; in Section 9.7, s_3, s_4 are multipliers; in the data descriptions of Chapters 2–6, $s = \pm 1$ labels the two slab families.

- P, Pr, $\mathbb{P}$. Chapter 8 writes $P(\cdot)$ and RQ-B's text writes Pr for probability; in Chapter 10, $P = (P_a, P_b)$ is the lower corner of a box of rates.
- A. Remark 7.8 uses $A(s)$ for the atomic Poisson constant; Chapter 8 uses A for any support bound larger than $A'(q)$.
- D, E, $\mathcal{C}$. In Chapter 10, D is the even degree of a certificate, E_W and E_w are error terms, and $\mathcal{C}$ is a rest class; E_k in Chapter 7 is a window constant.

Numbering and cross-references

- In Chapters 1–6 and 9, item n of the source paper (theorem, lemma, corollary, definition, remark, proposition, all on one counter) is numbered $c.n$ in chapter c. Likewise Section n becomes Section $c.n$ and equation (n) becomes $(c.n)$. The team's "Theorem 1" and "Theorem 2" are Theorems 1.1 and 2.1; Theorems 3, 4, 5 and 6 keep their fixed names in Chapters 3–6.
- Chapter 7 numbers its items in order. Each carries a tag [RQ-B tex ...; md ...] with the numbers of RQ-B's `MAIN_RESULT.tex` and `MAIN_RESULT.md`. In Chapter 10, item 10.n is item 12.n of RQ-B's `MAIN_RESULT.tex`, and the tags give the names in RQ-B's `MAIN_RESULT.md` (Theorem 13.1, Lemmas S1–S5, C, D, E).
- File names in the text refer to the source papers:

name in the text	in this document
`MAIN_RESULT` (RQ-A), "Theorem 1"	Chapter 1, Theorem 1.1
`MAIN_RESULT_K2`, "Theorem 2"	Chapter 2, Theorem 2.1
`MAIN_RESULT_K3`, "Theorem 3"	Chapter 3
`MAIN_RESULT_K3B`, "Theorem 4"	Chapter 4
`MAIN_RESULT_K4`, "Theorem 5"	Chapter 5
`MAIN_RESULT_K5`, "Theorem 6"	Chapter 6
RQ-B Theorem 1, Lemma 2.1, Theorem 3, Theorem 3.4 (md numbering)	Theorem 7.4, Lemma 7.5, Theorem 7.6, Theorem 7.9
RQ-B C19, RQ-A U.1–U.3	Theorem 7.9, Section 7.6
RQ-C C15	Theorem 8.1
RQ-D Lemma n, Theorem n, Corollary n	Lemma, Theorem, Corollary 9.n
RQ-B Theorem 13.1 (md) = Theorem 12.1 (tex)	Theorem 10.1
audit "A.n", "RQ-AUD"	RQ-AUD's `AUDIT.md`; see Appendix B

Roadmap and the proof of the Main Theorem

Which result covers which values of q

Figure 1 and Table 2 show how the results cover $(0, 1)$. All intervals are closed at every finite endpoint where two results meet. The point 0 is excluded, since $q \in (0, 1)$.

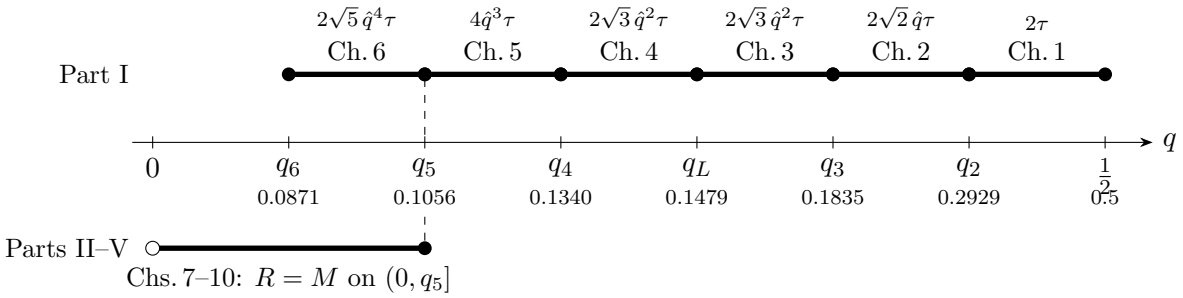

Figure 1: The range $(0, \frac{1}{2}]$, not to scale. Thick bars are closed intervals (filled dots); the small-q chain is open at 0 and closed at q_5. Above each bar is the chapter and the value $M(q)$ there. The range $[\frac{1}{2}, 1)$ is the mirror image under $q \mapsto 1 - q$, where every chapter of Part I proves the mirror statement and $R(q) = R(1 - q)$, $M(q) = M(1 - q)$ give the rest. The overlap $[q_6, q_5]$ of Chapter 6 and the chain is not needed for the value.

How the small-q chain fits together

Table 3 lists the links used on $(0, q_5]$, and Figure 2 shows how the three theorems of Parts IV–V divide the measures K.

Proof of the Main Theorem

The proof below only composes results proved in Chapters 1–10. It follows the composition that the auditor (A.40) and RQ-REF3 (overall verdict) checked. The facts about the maximum in (S) are Theorem 7.4.

Proof of the Main Theorem. Step 0: symmetry. By Lemma 1.2, $R(q) = R(1-q)$, and the extremisers for q and $1-q$ coincide. Since $\hat{q}$ and $q(1-q)$ are invariant under $q \mapsto 1-q$, also $M(q) = M(1-q)$. For $q \le \frac{1}{2}$, $\hat{q} = 1 - q$ and $M(q) = \max_k T_k(q)$.

closed range of q	$R(q) =$	proved in	audit	referee
$[q_2, 1-q_2]$	2τ	Theorem 1.1 (Ch. 1)	A.6	RQ-REF1
$[q_3, q_2] \cup [1-q_2, 1-q_3]$	$2\sqrt{2}\,\hat{q}\,\tau$	Theorem 2.1 (Ch. 2)	A.11	RQ-REF1
$[q_L, q_3] \cup [1-q_3, 1-q_L]$	$2\sqrt{3}\,\hat{q}^2\tau$	Theorem 3 (Ch. 3)	A.14	RQ-REF1
$[q_4, q_L] \cup [1-q_L, 1-q_4]$	$2\sqrt{3}\,\hat{q}^2\tau$	Theorem 4 (Ch. 4)	A.18	RQ-REF1
$[q_5, q_4] \cup [1-q_4, 1-q_5]$	$4\hat{q}^3\tau$	Theorem 5 (Ch. 5)	A.25	RQ-REF2
$[q_6, q_5] \cup [1-q_5, 1-q_6]$	$2\sqrt{5}\,\hat{q}^4\tau$	Theorem 6 (Ch. 6)	A.37	RQ-REF2
$[q_5, 1-q_5]$	$M(q)$	Corollary 5.2 (Theorems 1–5)	A.25, A.40	RQ-REF2
$[q_6, 1-q_6]$	$M(q)$	Corollary 6.2 (Theorems 1–6)	A.37	RQ-REF2
$(0, q_5]$	$M(q)$	Chapters 7–10, see Table 3	A.7a, A.10, A.10a, A.10c, A.26, A.28, A.30, A.32, A.34, A.38, A.39	RQ-REF3
$[1-q_5, 1)$	$M(q)$	mirror (Lemma 1.2)	A.40	RQ-REF3
$(0, 1)$	$M(q)$	Main Theorem (Section "Proof of the Main Theorem")	A.40	RQ-REF3

Table 2: The q-ranges and their proofs. "A.n" is the audit identifier in RQ-AUD's `AUDIT.md`; every audit and every referee verdict listed is VALID (details in Appendix B).

Step 1: the middle range $[q_5, 1-q_5]$. Corollary 5.2 gives (S) for every $q \in [q_5, 1-q_5]$. It combines Theorem 1.1 on $[q_2, 1-q_2]$, Theorem 2.1 on $[q_3, q_2] \cup [1-q_2, 1-q_3]$, Theorem 3 on $[q_L, q_3] \cup [1-q_3, 1-q_L]$, Theorem 4 on $[q_4, q_L] \cup [1-q_L, 1-q_4]$ and Theorem 5 on $[q_5, q_4] \cup [1-q_4, 1-q_5]$. These are closed intervals, and consecutive ones share an endpoint. (Corollary 6.2 adds Theorem 6 and extends this to $[q_6, 1-q_6]$; the value of R does not need it.)

Step 2: the lower bound on $(0, \frac{1}{2}]$. By Theorem 7.4, for $q \in (0, \frac{1}{2}]$ the maximum of $T_k(q)$ over $k \geq 1$ is attained at $k = \lfloor 1/(q(2-q)) \rfloor$, this k satisfies $kq < 1$, and $\mathbb{E}|\chi_1 + \cdots + \chi_k| / \sqrt{k} = T_k(q) = M(q)$. Hence $R(q) \geq M(q)$, with this $\alpha = \mathbf{1}_k / \sqrt{k}$.

Step 3: reduction of the upper bound on $(0, q_5]$. Fix $q \in (0, q_5]$ and put $A = \frac{77}{50}$, $C = C_5$. We check the two hypotheses of Theorem 8.1(f).

- $A > A'(q)$: by Theorem 8.1(g), A' is strictly increasing, so $A'(q) \leq A'(q_5) = \sqrt{5q_5 / \ln \frac{5}{4}} = 1.538044\ldots < 1.54 = A$.
- $C\sqrt{q/((1-q)s)} \leq M(q)$: by Theorem 7.9(d), $C(q) \geq C_5$ on $(0, q_5]$, and by (7.1), $M(q) = \sqrt{q/((1-q)s)}\, C(q) \geq \sqrt{q/((1-q)s)}\, C_5$.

Theorem 8.1(f) uses the bound

$$\mathbb{E}|Z_K| \leq \max\bigl(g(\lambda_\theta^+(K)),\, g(\lambda_\theta^-(K)),\, C_5\bigr) \qquad (*)$$

only at the single finitely supported probability measure $K = \tilde{K}$, which is carried by $[-A, A]$; and its proof works for every $\theta > 0$, because $\lambda_\theta^\pm(\tilde{K})$ is an integer multiple of s for every θ. So $R(q) = M(q)$ follows once we show:

Claim. Every finitely supported probability measure K on $[-\frac{77}{50}, \frac{77}{50}]$ satisfies $(*)$ with $\theta = \frac{17}{20}$.

Step 4: proof of the Claim. Let $V_+ = K([\frac{17}{20}, \frac{77}{50}])$ and $V_- = K([-\frac{77}{50}, -\frac{17}{20}])$. Exactly one of the following three cases occurs.

link	statement used	where	verdicts
L0	$R(q) \geq M(q)$ for $q \leq \frac{1}{2}$ (equal coefficients)	Theorem 7.4	A.10 (Theorem 1), A.40 (step 2), RQ-REF3 link 1
L1	if ID* holds at every K_f with constant $C \leq C(q)$, then $R(q) \leq M(q)$; $\min_{(0,q_5]} C = C_5$	Lemma 7.5, Theorems 7.6, 7.9(a)–(d), equation (7.1), Proposition 7.11; Section 7.6	A.7a, A.10a, A.10c, A.26, RQ-REF3 link 1
L2	only K carried by $[-A, A]$ with $A > A'(q)$ are needed; $A'(q) \leq A'(q_5) < \frac{77}{50}$	Theorem 8.1(f),(g)	A.28, RQ-REF3 link 2
L3	band: $V_+ \geq \frac{4}{5}$ or $V_- \geq \frac{4}{5} \Rightarrow \mathbb{E}\lvert Z_K\rvert \leq \max(g(\lambda^{\pm}_{17/20}(K)), C_5)$	Theorem 9.13 (with Sections 9.2–9.6)	A.30, A.32, A.34, RQ-REF3 link 3
L4	heavy: $\frac{1}{2} \leq V_+ < \frac{4}{5}$ or $\frac{1}{2} \leq V_- < \frac{4}{5} \Rightarrow \mathbb{E}\lvert Z_K\rvert < C_5$	Theorem 9.16 (with Section 9.7)	A.38, RQ-REF3 link 3
L5	light: $V_+ < \frac{1}{2}$ and $V_- < \frac{1}{2} \Rightarrow \mathbb{E}\lvert Z_K\rvert \leq \frac{171}{200} < C_5$	Theorem 10.1	A.39, RQ-REF3 link 4

Table 3: The links of the small-q chain. All verdicts are VALID. The composition (the proof below) is A.40 and RQ-REF3's overall verdict.

(i) $V_+ \geq \frac{4}{5}$ or $V_- \geq \frac{4}{5}$. Theorem 9.13 gives $\mathbb{E}\lvert Z_K\rvert \leq \max(g(\lambda^+_{0.85}(K)), C_5)$, resp. $\mathbb{E}\lvert Z_K\rvert \leq \max(g(\lambda^-_{0.85}(K)), C_5)$, and either bound implies $(*)$.

(ii) Not (i), and $V_+ \geq \frac{1}{2}$ or $V_- \geq \frac{1}{2}$. Then $\frac{1}{2} \leq V_+ < \frac{4}{5}$ or $\frac{1}{2} \leq V_- < \frac{4}{5}$, and Theorem 9.16 gives $\mathbb{E}\lvert Z_K\rvert < C_5$.

(iii) $V_+ < \frac{1}{2}$ and $V_- < \frac{1}{2}$. Theorem 10.1 gives $\mathbb{E}\lvert Z_K\rvert \leq \frac{171}{200} < C_5$, since $C_5 - \frac{171}{200} = 1.0045\ldots\cdot 10^{-4} > 0$.

In each case $(*)$ holds. The cases are exhaustive: if (i) fails then $V_\pm < \frac{4}{5}$, and if (ii) fails too then $V_\pm < \frac{1}{2}$.

Step 5: conclusion. Steps 2–4 give $R(q) = M(q)$ for every $q \in (0, q_5]$. By Step 0 this also holds on $[1 - q_5, 1)$. With Step 1, (S) holds on $(0, q_5] \cup [q_5, 1 - q_5] \cup [1 - q_5, 1) = (0, 1)$. Finally, for $q \leq \frac{1}{2}$ the vector $\mathbf{1}_k/\sqrt{k}$ of Step 2 attains $R(q) = M(q)$, and by Step 0 it also attains $R(1-q)$; this proves the remaining statements, with $p = \min(q, 1 - q)$. □

Remark. RQ-D's Corollaries 9.14 and 9.17 state the same composition of Steps 4(i)–(iii) as implications. Nothing in the chain uses Conjecture C5, Conjecture S itself, or RQ-D's Theorem 9.10 and Corollary 9.11; RQ-REF3 checked this (Appendix B).

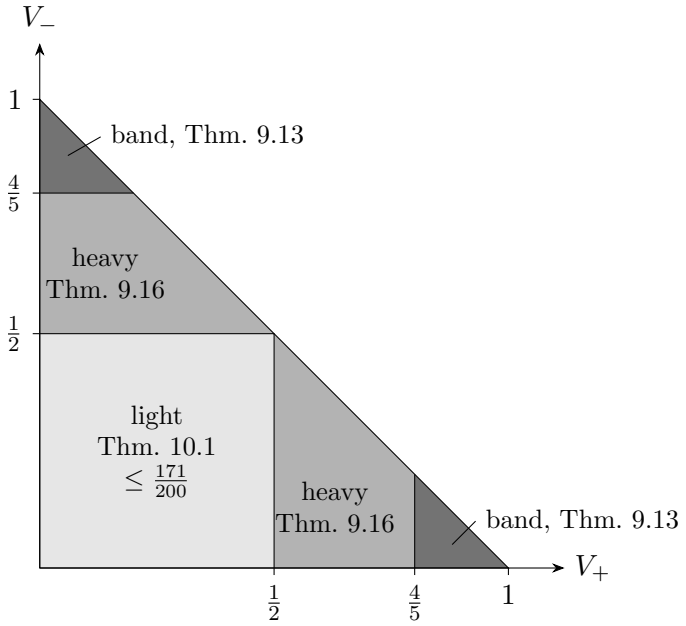

Figure 2: The masses $V_+ = K([\frac{17}{20}, \frac{77}{50}])$ and $V_- = K([-\frac{77}{50}, -\frac{17}{20}])$ of a probability measure K on $[-\frac{77}{50}, \frac{77}{50}]$ satisfy $V_\pm \geq 0$, $V_+ + V_- \leq 1$. The light region is $\{V_+ < \frac{1}{2}, V_- < \frac{1}{2}\}$; the heavy region is $\{\frac{1}{2} \leq V_+ < \frac{4}{5}\} \cup \{\frac{1}{2} \leq V_- < \frac{4}{5}\}$; the band is $\{V_+ \geq \frac{4}{5}\} \cup \{V_- \geq \frac{4}{5}\}$. The lines $V_\pm = \frac{1}{2}$ belong to the heavy region and the lines $V_\pm = \frac{4}{5}$ to the band, so the three regions cover the triangle with no gap.

Part I

The middle range $[q_6, 1 - q_6]$

Chapter 1

The exact value of $R(q)$ on the central range: $R(q) = 2\sqrt{q(1-q)}$ if and only if $1 - \frac{1}{\sqrt{2}} \le q \le \frac{1}{\sqrt{2}}$

Source: RQ-A, `MAIN_RESULT.tex` (md5 `38b69350c47c472d401153eac2a270e7`), by "RQ-A (R(q) attack, central range)", dated 22 October 2026. Its main result, Theorem 1.1, is the team's "Theorem 1" (claim MAIN of RQ-A).

Refereed version: md5 `6816732f3c313392f6b5ec547e1747f0`, the file in commit `6ecd564` of RQ-A's repository. The source differs from it in one figure of the appendix, $6.1 \cdot 10^{-3}$ in place of $6.2 \cdot 10^{-3}$ (audit finding A.6 f3; see the editorial footnote there).

Audit: A.6, VALID and NEW (22 October, 06:52 UTC). The typos f1–f2 were fixed before refereeing. Addendum of 23 October, 02:55 UTC: the appendix slip f3; addendum 2, 03:30 UTC: f3 applied and checked.

Referee: RQ-REF1, VALID, no fixes (report `REFEREE.md`, md5 `369c1cfb...`, mirrored at 15:38 UTC on 22 October).

Use in the Main Theorem: Lemma 1.2 in Step 0; Theorem 1.1 in Step 1, through Corollary 5.2.

Transcription: the whole paper, with the mechanical changes of Appendix C. Labels are prefixed by `ch01:`; Section n, item n and equation (n) become Section 1.n, item 1.n and $(1.n)$. The title becomes the chapter title, and the author and date are in this box. The table of contents is dropped, the abstract is set as a quoted block, and the appendix of the source is set as an unnumbered section at the end of the chapter. Two editorial footnotes.

Abstract of the source paper. For $q \in (0,1)$ let $\chi_1, \chi_2, \dots$ be i.i.d. normalised q-biased bits, and let $R(q)$ be the supremum of $\mathbb{E}|\sum \alpha_i \chi_i|$ over unit vectors α (of any length). We prove $R(q) = 2\sqrt{q(1-q)}$ for every $q \in [1 - 1/\sqrt{2},\, 1/\sqrt{2}]$, and that this interval is exactly the set of q where this holds. This settles the conjecture of BF3 (which proved the case $q \in [3/8, 5/8]$). We also determine all extremisers. The proof is not inductive. After the standard reduction $\mathbb{E}|L| = 2\tau a + 2\mathbb{E}R_a(bM)$ we bound $\mathbb{E}R_a(bM)$ by three kinds of certificates on the parameter rectangle (q, a), where a is the largest coefficient. (i) Degree-six polynomial majorants of $R_a(b\,\cdot)$: their expectations are controlled only through the first six moments of M, and these moments are fixed by power sums of the coefficients. (ii) An explicit quartic majorant, tangent at the two atoms of χ, which compares L with the two-coefficient extremiser $a\chi_1 + b\chi_2$ near the critical point $(q, a) = (1 - 1/\sqrt{2}, 1/\sqrt{2})$. (iii) A fourth-moment tail bound for $a \ge 9/10$. Parts (i)

and (ii) are verified by computer: (i) by exact rational arithmetic with Sturm sequences on 379 cells, (ii) by certified interval arithmetic on 641 boxes. Both verifications were repeated by an independent program.

1.1 Statement

Fix $q \in (0,1)$ and put

$$u = \sqrt{\tfrac{1-q}{q}}, \qquad v = \frac{1}{u} = \sqrt{\tfrac{q}{1-q}}, \qquad \tau = \sqrt{q(1-q)}.$$

Let $\chi, \chi_1, \chi_2, \dots$ be i.i.d. with $\Pr[\chi = u] = q$, $\Pr[\chi = -v] = 1-q$; then $\mathbb{E}\chi = qu - (1-q)v = \tau - \tau = 0$, $\mathbb{E}\chi^2 = (1-q) + q = 1$ and $\mathbb{E}|\chi| = 2\tau$. Define

$$R(q) = \sup_{n \ge 1} \sup_{\alpha \in \mathbb{R}^n \setminus \{0\}} \frac{\mathbb{E}\,|\sum_{i=1}^n \alpha_i \chi_i|}{|\alpha|_2}.$$

Let $q_0 = 1 - \frac{1}{\sqrt{2}} \approx 0.29289$; note $1 - q_0 = \frac{1}{\sqrt{2}}$.

Theorem 1.1. *(a) For every $q \in [q_0, 1-q_0]$, every $n \ge 1$ and every $\alpha \in \mathbb{R}^n$ with $|\alpha|_2 = 1$,*

$$\mathbb{E}\Big|\sum_{i=1}^n \alpha_i \chi_i\Big| \le 2\sqrt{q(1-q)}.$$

Consequently $R(q) = 2\sqrt{q(1-q)}$ for $q \in [q_0, 1-q_0]$.

(b) For $q \in (0, q_0) \cup (1-q_0, 1)$, $R(q) \ge 2\sqrt{2}\,\max(q, 1-q)\sqrt{q(1-q)} > 2\sqrt{q(1-q)}$. Hence $\{q : R(q) = 2\sqrt{q(1-q)}\} = [q_0, 1-q_0]$.

(c) (Extremisers.) For $q \in (q_0, 1-q_0)$, equality in (a) holds if and only if $\alpha = \pm e_j$. For $q \in \{q_0, 1-q_0\}$, equality holds if and only if $\alpha = \pm e_j$ or $\alpha = \pm\frac{1}{\sqrt{2}}(e_i + e_j)$ with $i \ne j$.

Part (b) is the known two-coefficient example (Lemma 1.10). Part (a) for $q \in [3/8, 5/8]$ is BF3, Theorem K. The new content is (a) on $[q_0, 3/8) \cup (5/8, 1-q_0]$, a proof of (a) that does not depend on BF3, and (c).

Conventions. $x_+ = \max(x, 0)$ and $x^- = \min(x, 0)$. All polynomials in the computer-assisted parts have rational coefficients. "Verified" means verified in exact rational arithmetic or in outward-rounded interval arithmetic, as specified in Section 1.7.

1.2 Reductions

1.2.1 Symmetry and the rational parametrisation

Lemma 1.2. *The law of $-\chi^{(q)}$ equals the law of $\chi^{(1-q)}$. Hence $\mathbb{E}|\sum \alpha_i \chi_i^{(q)}| = \mathbb{E}|\sum \alpha_i \chi_i^{(1-q)}|$, $R(q) = R(1-q)$, and the extremisers for q and $1-q$ coincide.*

Proof. $-\chi^{(q)}$ takes the value $-u_q$ with probability q and v_q with probability $1-q$. Since $u_{1-q} = \sqrt{q/(1-q)} = v_q$ and $v_{1-q} = u_q$, the variable $\chi^{(1-q)}$ takes the value v_q with probability $1-q$ and $-u_q$ with probability q. Finally $|\sum \alpha_i(-\chi_i)| = |\sum \alpha_i \chi_i|$. □

From now on $q \le \frac{1}{2}$, i.e. $u \ge 1$. We parametrise everything by u:

$$q = \frac{1}{1+u^2}, \quad 1-q = \frac{u^2}{1+u^2}, \quad v = \frac{1}{u}, \quad \tau = \frac{u}{1+u^2}. \tag{1.1}$$

The map $u \mapsto q$ is a decreasing bijection $[1,\infty) \to (0, \frac{1}{2}]$. The interval $q \in [q_0, \frac{1}{2}]$ corresponds to $u \in [1, u_0]$ with $u_0 = \sqrt{1+\sqrt{2}} \approx 1.5537740$: indeed $(1-q_0)/q_0 = \frac{1/\sqrt{2}}{1-1/\sqrt{2}} = \frac{1}{\sqrt{2}-1} = 1+\sqrt{2}$. On $u \ge 1$ the function $\tau(u) = u/(1+u^2)$ is decreasing, $u \mapsto u^2/(1+u^2)$ is increasing, and $u \mapsto 1/(1+u^2)$ is decreasing. We fix the rational number

$$\bar{u}_0 = \frac{776887}{500000} = 1.553774 > u_0$$

(indeed $\bar{u}_0^4 - 2\bar{u}_0^2 - 1 > 0$, which is equivalent to $\bar{u}_0^2 > 1+\sqrt{2}$).

1.2.2 Splitting off the largest coefficient

Let $|\alpha|_2 = 1$ and $L = \sum \alpha_i \chi_i$. Replacing α by $-\alpha$ does not change $\mathbb{E}|L|$, and permuting coordinates does not change the law of L. So we may assume $a := \max_i |\alpha_i| = \alpha_1 > 0$. If $a = 1$ then $L = \chi_1$ and $\mathbb{E}|L| = 2\tau$. Otherwise $0 < a < 1$; put $b = \sqrt{1-a^2} > 0$, $\beta_i = \alpha_i / b$ for $i \ge 2$, and

$$M = \sum_{i \ge 2} \beta_i \chi_i, \qquad \sum_{i \ge 2} \beta_i^2 = 1, \qquad \max_{i \ge 2} |\beta_i| \le \min\Big(1, \frac{a}{b}\Big).$$

Then $L = a\chi_1 + bM$, M is independent of χ_1, $\mathbb{E}M = 0$ and $\mathbb{E}M^2 = 1$.

Lemma 1.3 (BF3, Lemma 9.4)**.** *For $a \ge 0$ let*

$$R_a(y) = (1-q)(y-av)_+ + q(-y-au)_+ = \max\{0,\ (1-q)(y-av),\ q(-y-au)\}.$$

If Y is integrable and independent of χ, then $\mathbb{E}|a\chi + Y| = 2\tau a + (2q-1)\mathbb{E}Y + 2\mathbb{E}R_a(Y)$. In particular

$$\mathbb{E}|L| = 2\tau a + 2\mathbb{E}R_a(bM), \qquad \text{so} \qquad \mathbb{E}|L| \le 2\tau \iff \mathbb{E}R_a(bM) \le \tau(1-a).$$

Proof. The two expressions for R_a agree because the positive parts are supported on the disjoint sets $\{y > av\}$ and $\{y < -au\}$ (if $a = 0$ they are $\{y > 0\}$ and $\{y < 0\}$). For fixed y, use $|x| = x + 2(-x)_+$ for the first term and $|x| = -x + 2x_+$ for the second:

$$\begin{aligned} q|au+y| + (1-q)|y-av| &= q(au+y) + 2q(-au-y)_+ + (1-q)(av-y) + 2(1-q)(y-av)_+ \\ &= a\big(qu + (1-q)v\big) + (2q-1)y + 2R_a(y) = 2\tau a + (2q-1)y + 2R_a(y), \end{aligned}$$

since $qu = (1-q)v = \tau$. Condition on Y and take expectations. □

1.3 Moments of the remainder

Lemma 1.4. *The cumulants of χ are $\kappa_1 = 0$, $\kappa_2 = 1$, and, with $w = u^2 + v^2$,*

$$\kappa_3 = u - v, \quad \kappa_4 = w - 4, \quad \kappa_5 = (u-v)(w-10), \quad \kappa_6 = w^2 - 26w + 64.$$

Proof. By (1.1), $m_k := \mathbb{E}\chi^k = qu^k + (1-q)(-u^{-1})^k = \dfrac{u^k + (-1)^k u^{2-k}}{1+u^2}$. Using $u^4-1 = (u^2+1)(u^2-1)$, $u^6+1 = (u^2+1)(u^4-u^2+1)$, $u^8-1 = (u^2+1)(u^2-1)(u^4+1)$ and $u^{10}+1 = (u^2+1)(u^8-u^6+u^4-u^2+1)$, we get

$$\begin{aligned} m_3 &= \frac{u^4-1}{u(1+u^2)} = \frac{u^2-1}{u} = u - v, \\ m_4 &= \frac{u^6+1}{u^2(1+u^2)} = u^2 - 1 + u^{-2} = w - 1, \\ m_5 &= \frac{u^8-1}{u^3(1+u^2)} = \frac{(u^2-1)(u^4+1)}{u^3} = (u-v)w, \\ m_6 &= \frac{u^{10}+1}{u^4(1+u^2)} = u^4 + u^{-4} - w + 1 = w^2 - w - 1. \end{aligned}$$

For a centred variable with unit variance the cumulants are $\kappa_3 = m_3$, $\kappa_4 = m_4 - 3$, $\kappa_5 = m_5 - 10m_3$ and $\kappa_6 = m_6 - 15m_4 - 10m_3^2 + 30$. With $(u-v)^2 = w-2$ this gives $\kappa_4 = w-4$, $\kappa_5 = (u-v)(w-10)$ and $\kappa_6 = w^2 - w - 1 - 15(w-1) - 10(w-2) + 30 = w^2 - 26w + 64$. All four identities are also verified as identities of rational functions of u, in exact symbolic arithmetic, by `scripts/verify_all.py`, part A1. □

Lemma 1.5. *Let $M = \sum_i \beta_i \chi_i$ (finite sum, i.i.d. χ_i) with $\sum \beta_i^2 = 1$ and power sums $p_j = \sum_i \beta_i^j$. Then $\mathbb{E}M = 0$, $\mathbb{E}M^2 = 1$ and*

$$\begin{aligned} \mathbb{E}M^3 &= \kappa_3 p_3, & \mathbb{E}M^4 &= 3 + \kappa_4 p_4, \\ \mathbb{E}M^5 &= \kappa_5 p_5 + 10\kappa_3 p_3, & \mathbb{E}M^6 &= 15 + 15\kappa_4 p_4 + 10\kappa_3^2 p_3^2 + \kappa_6 p_6. \end{aligned}$$

Proof. Cumulants of independent sums add, and the j-th cumulant is homogeneous of degree j. So the cumulants of M are $K_1 = 0$, $K_2 = 1$ and $K_j = \kappa_j p_j$. For a centred variable the moment–cumulant relations give $m_3 = K_3$, $m_4 = K_4 + 3K_2^2$, $m_5 = K_5 + 10K_3K_2$ and $m_6 = K_6 + 15K_4K_2 + 10K_3^2 + 15K_2^3$. As a sanity check, the formulas were compared with exact enumeration of $\mathbb{E}M^k$ for 16 choices of rational u and rational unit vectors β (part A2 of `verify_all.py`); they match exactly. □

Lemma 1.6. *Let $0 < m \le 1$ with $\max_i |\beta_i| \le m$ (note that $\max_i |\beta_i| \le 1$ always). Then*

$$p_3^2 \le p_4 \le m^2, \qquad p_4^2 \le p_6 \le m^2 p_4, \qquad |p_5| \le m\, p_4, \qquad 0 \le p_4 \le 1.$$

Proof. $p_3^2 = (\sum \beta_i \cdot \beta_i^2)^2 \le \sum \beta_i^2 \sum \beta_i^4 = p_4$ by Cauchy–Schwarz. $p_4 = \sum \beta_i^2 \beta_i^2 \le m^2 \sum \beta_i^2 = m^2$. $p_4^2 = (\sum \beta_i \cdot \beta_i^3)^2 \le \sum \beta_i^2 \sum \beta_i^6 = p_6$. $p_6 = \sum \beta_i^4 \beta_i^2 \le m^2 p_4$. $|p_5| \le \sum |\beta_i| \beta_i^4 \le m\, p_4$. Also $|\beta_i| \le 1$ because $\sum \beta_i^2 = 1$. □

1.4 Six-moment certificates

A *cell* is a rectangle $[u_1, u_2] \times [a_1, a_2]$ with rationals $1 \le u_1 < u_2$ and $0 \le a_1 < a_2 < 1$. Fix a rational $\bar{b} \ge \sqrt{1-a_1^2}$ and a rational $\bar{m} \ge \min\{1, a_2/\sqrt{1-a_2^2}\}$. Define the lines

$$\bar{\ell}_1(y) = \frac{u_2^2}{1+u_2^2}\Big(\bar{b}\, y - \frac{a_1}{u_2}\Big), \qquad \bar{\ell}_2(y) = \frac{1}{1+u_1^2}\big(-\bar{b}\, y - a_1 u_1\big), \qquad \bar{R}(y) = \max\{0, \bar{\ell}_1(y), \bar{\ell}_2(y)\}.$$

Lemma 1.7 (domination on a cell)**.** *For every $u \in [u_1, u_2]$ (with $q = 1/(1+u^2)$), every $a \in [a_1, a_2]$, $b = \sqrt{1-a^2}$, and every $y \in \mathbb{R}$: $R_a(by) \le \bar{R}(y)$.*

Proof. By (1.1), $R_a(by) = \max\{0, \ell_1(y), \ell_2(y)\}$ with $\ell_1(y) = \frac{u^2}{1+u^2}(by - \frac{a}{u})$ and $\ell_2(y) = \frac{1}{1+u^2}(-by - au)$. Suppose $\ell_1(y) > 0$. Then $by > a/u \ge 0$, so $y > 0$. Since $a \ge a_1$, $u \le u_2$ and $b \le \bar{b}$, we get $0 < by - \frac{a}{u} \le \bar{b}y - \frac{a_1}{u_2}$. Also $0 < \frac{u^2}{1+u^2} \le \frac{u_2^2}{1+u_2^2}$. Hence $\ell_1(y) \le \bar{\ell}_1(y)$. Suppose $\ell_2(y) > 0$. Then $-by > au \ge 0$, so $y < 0$. Since $-y > 0$ and $b \le \bar{b}$, we have $-by \le -\bar{b}y$; since $a \ge a_1 \ge 0$ and $u \ge u_1 > 0$, we have $-au \le -a_1 u_1$. So $0 < -by - au \le -\bar{b}y - a_1 u_1$, and with $\frac{1}{1+u^2} \le \frac{1}{1+u_1^2}$ we get $\ell_2(y) \le \bar{\ell}_2(y)$. In all cases $\max\{0, \ell_1, \ell_2\} \le \max\{0, \bar{\ell}_1, \bar{\ell}_2\}$. □

Cumulant enclosures on $[u_1, u_2]$. For $u \ge 1$ the functions $\kappa_3 = u - 1/u \ge 0$ and $w = u^2 + u^{-2}$ are increasing. Put $\kappa_3 \in [k_3^-, k_3^+] = [u_1 - \frac{1}{u_1}, u_2 - \frac{1}{u_2}]$ and $w \in [w^-, w^+] = [u_1^2 + u_1^{-2}, u_2^2 + u_2^{-2}]$. We require $w^+ < 13$ (true when $u_2 \le \bar{u}_0$, where $w^+ < 2.83$). Then $\kappa_4 \in [w^- - 4, w^+ - 4]$. Since $x \mapsto x^2 - 26x + 64$ is decreasing on $x < 13$, $\kappa_6 \in [f_6(w^+), f_6(w^-)]$ with $f_6(x) = x^2 - 26x + 64$. Finally $|\kappa_5| \le k_3^+ \max(|w^- - 10|, |w^+ - 10|) =: k_5^+$.

Definition 1.8 (six-moment certificate)**.** A certificate for the cell is a polynomial $P(y) = \sum_{k=0}^{6} c_k y^k$ with rational coefficients such that:

(V1) $P(y) > 0$ for all $y \in \mathbb{R}$;

(V2) $P(y) - \bar{\ell}_1(y) > 0$ for all $y \in \mathbb{R}$;

(V3) $P(y) - \bar{\ell}_2(y) > 0$ for all $y \in \mathbb{R}$;

(V4) with

$$\begin{aligned} A &= c_0 + c_2 + 3c_4 + 15c_6, & \bar{B} &= k_3^+ \,|c_3 + 10c_5|, \\ C^+ &= \max_{\kappa_4 \in [w^- - 4,\, w^+ - 4]} \kappa_4(c_4 + 15c_6), & \bar{D} &= k_5^+ |c_5|, \\ E^+ &= \max\{f_6(w^-)c_6,\ f_6(w^+)c_6\}, & F^+ &= \max\{0,\ 10(k_3^-)^2 c_6,\ 10(k_3^+)^2 c_6\}, \end{aligned}$$

$\Gamma = C^+ + \bar{D}\bar{m} + F^+ + \max(E^+, 0)\bar{m}^2$ and $\varepsilon = \min(E^+, 0)$, the polynomial

$$h(r) = \tau(u_2)(1 - a_2) - A - \bar{B}r - \Gamma r^2 - \varepsilon r^4$$

satisfies $h(r) > 0$ for all $r \in [0, \bar{m}]$.

Lemma 1.9 (certificate lemma)**.** *If the cell has a certificate, then for every $u \in [u_1, u_2]$ and $a \in [a_1, a_2]$, and every $M = \sum \beta_i \chi_i$ with $\sum \beta_i^2 = 1$ and $\max |\beta_i| \le \min(1, a/b)$,*

$$\mathbb{E} R_a(bM) < \tau(u)(1 - a).$$

Proof. By (V1)–(V3), $P \ge \bar{R}$ on $\mathbb{R}$. With Lemma 1.7, $\mathbb{E} R_a(bM) \le \mathbb{E}\bar{R}(M) \le \mathbb{E}P(M)$. By Lemma 1.5,

$$\begin{aligned} \mathbb{E}P(M) &= c_0 + c_2 + c_3\kappa_3 p_3 + c_4(3 + \kappa_4 p_4) + c_5(\kappa_5 p_5 + 10\kappa_3 p_3) \\ &\quad + c_6(15 + 15\kappa_4 p_4 + 10\kappa_3^2 p_3^2 + \kappa_6 p_6) \\ &= A + \kappa_3(c_3 + 10c_5)p_3 + \kappa_4(c_4 + 15c_6)p_4 + \kappa_5 c_5 p_5 + \kappa_6 c_6 p_6 + 10\kappa_3^2 c_6 p_3^2. \end{aligned}$$

Since a/b is increasing in a, $\max|\beta_i| \le \min(1, a_2/\sqrt{1-a_2^2}) \le \bar{m}$. Put $r = \sqrt{p_4} \in [0, \bar{m}]$ (Lemma 1.6). We bound each term, using the cumulant enclosures for the actual $u \in [u_1, u_2]$ and Lemma 1.6:

- $\kappa_3(c_3+10c_5)p_3 \le k_3^+|c_3+10c_5|\,|p_3| \le \bar{B}r$, because $|p_3| \le \sqrt{p_4}$.
- $\kappa_4(c_4+15c_6)p_4 \le C^+r^2$, because $p_4 \ge 0$ and the expression is linear in κ_4.
- $\kappa_5 c_5 p_5 \le k_5^+|c_5|\,m\,p_4 \le \bar{D}\bar{m}r^2$.
- $10\kappa_3^2 c_6 p_3^2 \le F^+p_3^2 \le F^+r^2$, because $F^+ \ge 0$ and $p_3^2 \le p_4$.
- $\kappa_6 c_6 p_6 \le E^+p_6$, because $p_6 \ge 0$ and the expression is linear in κ_6. If $E^+ \ge 0$, then $E^+p_6 \le E^+\bar{m}^2p_4 = E^+\bar{m}^2r^2$. If $E^+ < 0$, then $E^+p_6 \le E^+p_4^2 = E^+r^4$.

Hence $\mathbb{E}P(M) \le A + \bar{B}r + \Gamma r^2 + \varepsilon r^4 = \tau(u_2)(1-a_2) - h(r) < \tau(u_2)(1-a_2)$ by (V4). Finally $\tau(u_2) \le \tau(u)$ (as τ is decreasing on $[1,\infty)$) and $1-a_2 \le 1-a$. □

1.5 The quartic two-extremiser certificate

Near $(q,a) = (q_0, 1/\sqrt{2})$ two configurations are extremal: e_1 and $(e_1+e_2)/\sqrt{2}$. No certificate of Section 1.4 can work at that point, because the target $\tau(1-a)$ is attained there with $M = \chi_2$. Instead we compare L with $a\chi_1 + b\chi_2$.

Lemma 1.10 (two-coefficient value)**.** *If $a,b>0$ and $bu \ge av$, $bv \le au$ (equivalently $q/(1-q) \le b/a \le (1-q)/q$), then $\mathbb{E}R_a(b\chi) = q(1-q)(bu-av)$ and $\mathbb{E}|a\chi_1+b\chi_2| = 2\tau(1-q)(a+b)$. In particular, for $q \le \frac12$, $\mathbb{E}|\chi_1+\chi_2|/\sqrt{2} = 2\sqrt{2}(1-q)\tau$, which exceeds 2τ if and only if $q < q_0$.*

Proof. $R_a(bu) = (1-q)(bu-av)_+ = (1-q)(bu-av)$ and $R_a(-bv) = q(bv-au)_+ = 0$. So $\mathbb{E}R_a(b\chi) = q(1-q)(bu-av)$. By Lemma 1.3, $\mathbb{E}|a\chi_1+b\chi_2| = 2\tau a + 2q(1-q)(bu-av) = 2\tau a + 2(1-q)\tau b - 2q\tau a = 2\tau(1-q)(a+b)$, using $q(1-q)u = (1-q)\tau$ and $q(1-q)v = q\tau$. For $a=b=1/\sqrt{2}$ the hypothesis reads $v \le u$, i.e. $q \le \frac12$. Finally $\sqrt{2}(1-q) > 1 \iff q < 1 - \frac{1}{\sqrt{2}}$. □

The certificate. Let $u>1$ and $a,b>0$ with $a^2+b^2=1$, and let $c_4>0$. With $\tau = u/(1+u^2)$ define

$$B_0 = \tau^4\big(2a - b(u^2-1)\big), \quad s = \tau^3(bu^2-a), \quad B = B_0 - 2c_4u, \quad G = s - B_0u + c_4u^2, \tag{1.2}$$

and

$$P(y) = (y+v)^2\,S_0(y), \qquad S_0(y) = c_4y^2 + By + G.$$

Write $\ell_1(y) = (1-q)(by-av)$ and $\ell_2(y) = -q(by+au)$, so that $R_a(by) = \max\{0,\ell_1,\ell_2\}$. Write $P(y) = \sum_{k=0}^4 c_k y^k$; then $c_3 = B + 2vc_4$.

Lemma 1.11 (algebraic identities)**.** *The following hold identically in u,a,b,c_4 (with q,v,τ given by (1.1)):*

(i) $P(u) = \ell_1(u)$ *and* $P'(u) = \ell_1'(u)$*; trivially* $P(-v) = P'(-v) = 0$.

(ii) $B^2 - 4c_4G = B_0^2 - 4c_4s$.

(iii) $P(y) - \ell_1(y) = (y-u)^2S_1(y)$ *with* $S_1(y) = c_4y^2 + d_1y + d_0$ *and* $d_1^2 - 4c_4d_0 = B_0^2 - 4c_4\big(s + B_0(u+v)\big)$.

(iv) $\kappa_3c_3 + 2\kappa_4c_4 = \kappa_3B_0 - 4c_4$.

(v) $\mathbb{E}P(\chi) = qP(u) + (1-q)P(-v) = q(1-q)(bu-av)$, *and* $2\tau a + 2q(1-q)(bu-av) = 2\tau(1-q)(a+b)$.

(vi) Let $z_0 = au/b$, $\delta = z_0 - v$, $g_1 = 2c_4 z_0 - B$ *and* $g_0 = c_4 z_0^2 - Bz_0 + G$. *Then for all* x,

$$P(-z_0 - x) - \ell_2(-z_0 - x) = e_0 + e_1 x + e_2 x^2 + e_3 x^3 + c_4 x^4,$$

where $e_0 = \delta^2 g_0$, $e_1 = \delta^2 g_1 + 2\delta g_0 - qb$, $e_2 = \delta^2 c_4 + 2\delta g_1 + g_0$ *and* $e_3 = 2\delta c_4 + g_1$. *Moreover* $\ell_2(-z_0 - x) = qbx$.

Proof. (iv) is short. $c_3 = B + 2vc_4 = B_0 - 2c_4(u-v) = B_0 - 2c_4\kappa_3$, so $\kappa_3 c_3 + 2\kappa_4 c_4 = \kappa_3 B_0 - 2c_4(\kappa_3^2 - \kappa_4)$, and $\kappa_3^2 - \kappa_4 = u^2 - 2uv + v^2 - u^2 - v^2 + 4 = 2$ because $uv = 1$.

(ii): $4c_4G - B^2 = 4c_4 s - 4c_4 B_0 u + 4c_4^2 u^2 - (B_0^2 - 4c_4 u B_0 + 4c_4^2 u^2) = 4c_4 s - B_0^2$.

(i): $P(u) = (u+v)^2 S_0(u)$ and $S_0(u) = c_4 u^2 + Bu + G = s$ by (1.2), with $(u+v)^2 = (1+u^2)^2/u^2$. So $P(u) = s(1+u^2)^2/u^2 = \tau^3(bu^2-a)(1+u^2)^2/u^2 = \frac{u(bu^2-a)}{1+u^2}$. Also $\ell_1(u) = \frac{u^2}{1+u^2}(bu - \frac{a}{u}) = \frac{u(bu^2-a)}{1+u^2}$. Next, $P'(u) = 2(u+v)s + (u+v)^2 S_0'(u)$ with $S_0'(u) = 2c_4 u + B = B_0$. This gives

$$\begin{aligned} P'(u) &= \frac{2(1+u^2)}{u}\tau^3(bu^2-a) + \frac{(1+u^2)^2}{u^2}\tau^4\big(2a - b(u^2-1)\big) \\ &= \frac{u^2}{(1+u^2)^2}\big[2(bu^2-a) + 2a - b(u^2-1)\big] = \frac{u^2 b(u^2+1)}{(1+u^2)^2} = \frac{u^2 b}{1+u^2}, \end{aligned}$$

which is $\ell_1'(u) = (1-q)b$.

(iii): By (i), $P - \ell_1$ is a quartic with leading coefficient c_4 and a double root at u. Hence $P - \ell_1 = (y-u)^2(c_4 y^2 + d_1 y + d_0)$. Comparing coefficients of y^3 and y^2 gives $d_1 = c_3 + 2uc_4 = B_0 + 2vc_4$ and $d_0 = c_2 + 2ud_1 - u^2 c_4$, where $c_2 = G + 2vB + v^2 c_4$. Substituting: $d_0 = s + B_0(u+2v) + c_4 v^2$. Then $d_1^2 - 4c_4 d_0 = B_0^2 + 4c_4 v B_0 + 4c_4^2 v^2 - 4c_4 s - 4c_4 B_0(u+2v) - 4c_4^2 v^2 = B_0^2 - 4c_4(s + B_0(u+v))$.

(v): $P(-v) = 0$, $P(u) = \ell_1(u) = (1-q)(bu-av)$, and $q(1-q)u = (1-q)\tau$, $q(1-q)v = q\tau$.

(vi): $\ell_2(-z_0 - x) = -q(-bz_0 - bx + au) = qbx$, since $bz_0 = au$. Next, $(y+v)^2 = (\delta + x)^2$ at $y = -z_0 - x$, and $S_0(-z_0 - x) = c_4(z_0 + x)^2 - B(z_0 + x) + G = c_4 x^2 + g_1 x + g_0$. Expanding $(\delta^2 + 2\delta x + x^2)(c_4 x^2 + g_1 x + g_0) - qbx$ gives the stated coefficients.

All six items are also verified symbolically (sympy, exact) by `verify_all.py`, part A3. □

Lemma 1.12 (quartic certificate lemma)**.** *Let* $1 < u < \frac{19}{10}$, $a, b > 0$ *with* $a^2 + b^2 = 1$, $bu^2 > a$ *and* $au^2 > b$, *and let* $c_4 > 0$ *satisfy*

(Q1) $B_0 > 0$ *and* $4c_4 s - B_0^2 > 0$;

(Q3) $e_0 > 0$ *and* $e_2 - \dfrac{(e_1^-)^2}{4e_0} - \dfrac{(e_3^-)^2}{4c_4} > 0$;

(Q4) $\kappa_3 B_0 - 4c_4 > 0$.

(The numbering follows our notes, where (Q2) denoted the positivity of S_1*; by Step 2 below it is implied by (Q1).) Then for every* $M = \sum \beta_i \chi_i$ *with* $\sum \beta_i^2 = 1$,

$$\mathbb{E}R_a(bM) \le q(1-q)(bu-av) - (1-p_3)(\kappa_3 B_0 - 4c_4),$$

and therefore $\mathbb{E}|a\chi_1 + bM| \le 2\tau(1-q)(a+b)$, *with strict inequality unless* $p_3 = 1$.

Proof. Step 1: $P \geq 0$. By (Q1), $s > 0$ (from $bu^2 > a$), and by Lemma 1.11(ii) the discriminant of S_0 is $B_0^2 - 4c_4 s < 0$. With $c_4 > 0$ this gives $S_0 > 0$ on $\mathbb{R}$, hence $P = (y+v)^2 S_0 \geq 0$.

Step 2: $P \geq \ell_1$. By Lemma 1.11(iii), the discriminant of S_1 is $B_0^2 - 4c_4 s - 4c_4 B_0(u+v) < 0$, since $B_0 > 0$. So $S_1 > 0$ and $P - \ell_1 = (y-u)^2 S_1 \geq 0$.

Step 3: $P \geq \ell_2$. If $y \geq -z_0 = -au/b$, then $\ell_2(y) = -q(by+au) \leq 0 \leq P(y)$. If $y < -z_0$, write $y = -z_0 - x$ with $x > 0$. By Lemma 1.11(vi), $P(y) - \ell_2(y) = f(x) := e_0 + e_1 x + e_2 x^2 + e_3 x^3 + c_4 x^4$. Put $\eta = (e_1^-)^2/(4e_0)$. Then

$$f(x) = \big[e_0 + e_1 x + \eta x^2\big] + x^2\big[(e_2 - \eta) + e_3 x + c_4 x^2\big].$$

The first bracket is $\geq e_0 > 0$ if $e_1 \geq 0$, and equals $(\sqrt{e_0} + e_1 x/(2\sqrt{e_0}))^2 \geq 0$ if $e_1 < 0$. In the second bracket, $D := e_2 - \eta > (e_3^-)^2/(4c_4) \geq 0$ by (Q3). If $e_3 \geq 0$ the bracket is $\geq D > 0$ for $x \geq 0$. If $e_3 < 0$ it is $\geq D - e_3^2/(4c_4) > 0$. Hence $f(x) > 0$ for $x > 0$.

So $P \geq \max\{0, \ell_1, \ell_2\} = R_a(b\,\cdot)$ on $\mathbb{R}$, and $\mathbb{E}R_a(bM) \leq \mathbb{E}P(M)$.

Step 4: comparison with χ. P has degree 4. By Lemma 1.5, $\mathbb{E}P(M) = c_0 + c_2 + c_3\kappa_3 p_3 + c_4(3 + \kappa_4 p_4)$, and $\mathbb{E}P(\chi)$ is the same expression with $p_3 = p_4 = 1$. Here $\kappa_4 = u^2 + u^{-2} - 4 < 0$, because $u^2 < \frac{361}{100} < 2 + \sqrt{3}$; so $c_4\kappa_4 < 0$. Also $p_3^2 \leq p_4 \leq 1$ (Lemma 1.6), so $|p_3| \leq 1$. Therefore

$$\begin{aligned}
\mathbb{E}P(\chi) - \mathbb{E}P(M) &= c_3\kappa_3(1-p_3) + c_4\kappa_4(1-p_4) \geq c_3\kappa_3(1-p_3) + c_4\kappa_4(1-p_3^2) \\
&= (1-p_3)\big(c_3\kappa_3 + c_4\kappa_4(1+p_3)\big) \\
&\geq (1-p_3)\big(c_3\kappa_3 + 2c_4\kappa_4\big) = (1-p_3)(\kappa_3 B_0 - 4c_4).
\end{aligned}$$

The first inequality uses $c_4\kappa_4 \leq 0$ and $1 - p_4 \leq 1 - p_3^2$. The second uses $1 - p_3 \geq 0$, $c_4\kappa_4 \leq 0$ and $1 + p_3 \leq 2$. The last equality is Lemma 1.11(iv).

Step 5. By Lemma 1.11(v), $\mathbb{E}R_a(bM) \leq \mathbb{E}P(M) \leq q(1-q)(bu - av) - (1-p_3)(\kappa_3 B_0 - 4c_4)$. By Lemma 1.3 and Lemma 1.11(v), $\mathbb{E}|a\chi_1 + bM| \leq 2\tau a + 2q(1-q)(bu - av) - 2(1-p_3)(\kappa_3 B_0 - 4c_4) \leq 2\tau(1-q)(a+b)$, with strict inequality if $p_3 < 1$, by (Q4). □

Corollary 1.13. *Under the hypotheses of Lemma 1.12, if moreover $q \geq q_0$ (i.e. $u \leq u_0$), then $\mathbb{E}|a\chi_1 + bM| \leq 2\tau$. Equality forces $q = q_0$, $a = b = 1/\sqrt{2}$ and $M = \chi_j$ for a single j.*

Proof. $(1-q)(a+b) \leq (1-q)\sqrt{2(a^2+b^2)} = \sqrt{2}(1-q) \leq \sqrt{2}(1-q_0) = 1$. Equality needs $a = b$, $q = q_0$ and $p_3 = 1$. If $p_3 = \sum \beta_i^3 = 1 = \sum \beta_i^2$ then $\sum \beta_i^2(1-\beta_i) = 0$ with each $\beta_i \leq 1$; so every $\beta_i \in \{0,1\}$, and exactly one $\beta_j = 1$. □

1.6 The near-dictator range

Lemma 1.14. *Let $u \in [1, u_0]$, $a \in [\frac{9}{10}, 1)$, $b = \sqrt{1-a^2}$, and let $M = \sum \beta_i \chi_i$ with $\sum \beta_i^2 = 1$. Then $\mathbb{E}R_a(bM) \leq 0.9402\,\tau(1-a)$.*

Proof. For $t > 0$ and all real x we have $(x-t)_+ \leq \frac{27}{256\,t^3} x^4$. Indeed, for $x > t$ the ratio $(x-t)/x^4$ is maximised at $x = 4t/3$, where it equals $27/(256t^3)$. Now $R_a(by) = (1-q)b\,(y - \frac{av}{b})_+ + qb\,(-y - \frac{au}{b})_+$. So

$$\begin{aligned}
\mathbb{E}R_a(bM) &\leq \frac{27}{256}\,\mathbb{E}M^4\Big[(1-q)b\frac{b^3}{a^3v^3} + qb\frac{b^3}{a^3u^3}\Big] = \frac{27}{256}\frac{b^4}{a^3}\mathbb{E}M^4\big[(1-q)u^3 + qv^3\big] \\
&= \frac{27}{256}\frac{b^4}{a^3}\mathbb{E}M^4\,\tau(u^4 + v^4),
\end{aligned}$$

using $(1-q)u^3 = \frac{u^5}{1+u^2} = \tau u^4$ and $qv^3 = \frac{v^3}{1+u^2} = \tau v^4$. By Lemma 1.5, $\mathbb{E}M^4 = 3+\kappa_4 p_4 \le 3$, because $\kappa_4 = u^2 + u^{-2} - 4 \le 0$ for $u^2 \le 2+\sqrt{3}$. The function $u^4 + u^{-4}$ is increasing on $u \ge 1$ and equals $(1+\sqrt{2})^2 + (\sqrt{2}-1)^2 = 6$ at u_0. With $b^4 = (1-a)^2(1+a)^2$,

$$\mathbb{E}R_a(bM) \le \tau(1-a) \cdot \frac{81 \cdot 6}{256} \cdot \frac{(1-a)(1+a)^2}{a^3}.$$

The function $(1-a)(1+a)^2/a^3$ is a product of the positive decreasing functions $1-a$ and $(1+a)^2/a^3$ on $(0,1)$ (the derivative of the latter is $(1+a)(2a-3(1+a))/a^4 < 0$). So it is at most its value at $a = 9/10$, and $\frac{486}{256} \cdot \frac{(1/10)(19/10)^2}{(9/10)^3} = 0.940104\ldots < 0.9402$. □

1.7 The computer-assisted verifications

All scripts and outputs are in the repository (directories `scripts/` and `outputs/`). Floating point is used only to *find* certificates: linear programming (HiGHS via scipy) for the six-moment polynomials, and a grid search for c_4. Every *verification* is exact or uses certified interval arithmetic.

1.7.1 Six-moment cells

The region $\mathcal{S} = [1, \bar{u}_0] \times [0, \frac{9}{10}] \setminus \big((\frac{611}{400}, \bar{u}_0) \times (\frac{16}{25}, \frac{77}{100})\big)$ is the union of the eight rectangles in Table 1.1. Each rectangle is partitioned into cells by adaptive bisection from an initial grid. The data of each cell are rationals u_1, u_2, a_1, a_2 and $c_0, \ldots, c_6$; they are stored in `outputs/cover/*.json`. The auxiliary numbers are $\bar{b} = \lceil 10^{15}\sqrt{1-a_1^2} \rceil / 10^{15}$, and $\bar{m} = 1$ if $a_2^2 \ge \frac{1}{2}$, otherwise $\bar{m} = \min\{1, a_2/s_2\}$ with $s_2 = \lfloor 10^{15}\sqrt{1-a_2^2} \rfloor / 10^{15}$. These are computed with integer square roots, and the inequalities $\bar{b}^2 \ge 1 - a_1^2$ and $s_2^2 \le 1 - a_2^2$ are asserted exactly.

file	u-range	a-range	cells
r1a	$[1, \bar{u}_0]$	$[0, \frac{4}{25}]$	94
r1b	$[1, \bar{u}_0]$	$[\frac{4}{25}, \frac{8}{25}]$	59
r1c	$[1, \bar{u}_0]$	$[\frac{8}{25}, \frac{12}{25}]$	32
r1d	$[1, \bar{u}_0]$	$[\frac{12}{25}, \frac{16}{25}]$	71
r2a	$[1, \frac{13}{10}]$	$[\frac{77}{100}, \frac{9}{10}]$	16
r2b	$[\frac{13}{10}, \bar{u}_0]$	$[\frac{77}{100}, \frac{9}{10}]$	47
r3a	$[1, \frac{13}{10}]$	$[\frac{16}{25}, \frac{77}{100}]$	16
r3b	$[\frac{13}{10}, \frac{611}{400}]$	$[\frac{16}{25}, \frac{77}{100}]$	44
total			379

Table 1.1: The six-moment cover. Cell widths range from 0.0079 to 0.139 in u and from 0.0040 to 0.0325 in a.

For each cell, (V1)–(V3) are checked as follows. Each polynomial $p \in \{P,\ P - \bar{\ell}_1,\ P - \bar{\ell}_2\}$ has even degree 6, positive leading coefficient and $p(0) > 0$, and its Sturm sequence, computed in exact rational arithmetic, shows that p has no real root. (V4) is checked as follows: $h(0) > 0$, $h(\bar{m}) > 0$, and the Sturm sequence of h shows that h has no root in $(0, \bar{m}]$.

Two independent programs perform these checks. `exactcert.py` (used during generation) uses sympy's exact real-root counting for (V1)–(V3) and an exact bisection bound for (V4). `verify_all.py`, part C, uses its own Sturm sequence code over Python `Fraction`s for all four conditions and recomputes $\bar{b}$, $\bar{m}$, the lines and the cumulant enclosures from scratch. Both accept

all 379 cells. The Sturm code was cross-checked against sympy on 300 random polynomials, including ones with repeated roots (`break_tests.py`). Every tested decrease of a single coefficient of a stored certificate is rejected, which confirms that the certificates are tight and that the checks are active.

1.7.2 Quartic boxes

Parametrise $a = \frac{2t}{1+t^2}$, $b = \frac{1-t^2}{1+t^2}$ $(0 < t < 1)$. Then $a^2 + b^2 = 1$, a is increasing and b is decreasing in t, and $t \mapsto a(t)$ is a bijection of $[0,1]$ onto $[0,1]$. The box $\mathcal{Q} = [\frac{611}{400}, \bar{u}_0] \times [\frac{9}{25}, \frac{471}{1000}]$ in the (u,t)-plane is partitioned into 641 boxes (stored in `outputs/quartic_cover.json`). Their widths range from 0.0008 to 0.0033 in u and from 0.0017 to 0.0069 in t, and each box carries a rational constant $c_4 > 0$. Since $a(\frac{9}{25}) = \frac{225}{353} < \frac{16}{25}$ and $a(\frac{471}{1000}) = \frac{942000}{1221841} > \frac{77}{100}$, the box $\mathcal{Q}$ contains a preimage of every $(u,a) \in [\frac{611}{400}, \bar{u}_0] \times [\frac{16}{25}, \frac{77}{100}]$.

For each box, with its constant c_4, the following are verified for all (u,t) in the box: $bu^2 - a > 0$, $au^2 - b > 0$, (Q1), (Q3) and (Q4) of Lemma 1.12. All quantities are evaluated in interval arithmetic from the formulas of (1.2) and Lemma 1.11(vi). For (Q3) we use the conservative form $e_2 - \sigma_1 e_1^2/(4e_0) - \sigma_3 e_3^2/(4c_4) > 0$, where $\sigma_k = 0$ if the enclosure of e_k is nonnegative and $\sigma_k = 1$ otherwise. This is valid because $(e^-)^2 \le e^2$, with $(e^-)^2 = 0$ when $e \ge 0$.

Again two independent implementations are used. `quartic_verify.py` (generation) uses exact rational interval arithmetic with dyadic outward rounding (2^{-120}) and the mean value form: an enclosure of f over the box is $f(\text{centre}) + \partial_u f(\text{box})[-h_u, h_u] + \partial_t f(\text{box})[-h_t, h_t]$, intersected with the naive enclosure, where the derivatives are enclosed by forward-mode automatic differentiation in interval arithmetic. `verify_all.py`, part D, uses mpmath's outward-rounded interval arithmetic (120-bit) with naive evaluation. It computes the coefficients of P by expanding $(y+v)^2 S_0$ and the e_k by a Taylor shift of P at $-z_0$ (a different formula path from Lemma 1.11(vi)), and it subdivides each stored box (with the same c_4) until all conditions hold, which takes 20 969 sub-boxes in total. Part D requires (Q4) strictly; the minimum certified lower bound of $\kappa_3 B_0 - 4c_4$ over all boxes is $1.77 \cdot 10^{-3}$. Scaling any tested c_4 by 3 or $1/3$ makes the check fail (`break_tests.py`).

1.7.3 Coverage

`verify_all.py`, part B, checks in exact arithmetic that within each rectangle of Table 1.1, and within $\mathcal{Q}$, the cells lie in the rectangle, have pairwise disjoint interiors, and have total area equal to the area of the rectangle. Then their (closed) union is the whole rectangle: a closed subset of full measure in a rectangle is dense, hence equal to the rectangle. It also checks that the eight rectangles, the rectangle $[\frac{611}{400}, \bar{u}_0] \times [\frac{16}{25}, \frac{77}{100}]$ and the strip $[1, \bar{u}_0] \times [\frac{9}{10}, 1]$ cover $[1, \bar{u}_0] \times [0,1]$. This is done on the grid formed by all breakpoints.

1.7.4 Reproducing

```
pip install numpy scipy sympy mpmath
cd scripts
python3 verify_all.py     # parts A-E, about one minute
python3 break_tests.py    # negative tests
# optional regeneration (a few minutes), e.g.
python3 cover_lp6.py 1 776887/500000 0 4/25 ../outputs/cover/r1a.json
python3 quartic_verify.py 611/400 1553774/1000000 9/25 471/1000 \
        ../outputs/quartic_cover.json
```

The remaining cover rectangles are listed in Table 1.1; `run_cover.sh` runs one rectangle.

1.8 Proof of Theorem 1.1

(a) By Lemma 1.2 we may assume $q \in [q_0, \frac{1}{2}]$, i.e. $u \in [1, u_0]$. Let $|\alpha|_2 = 1$. Reduce as in Section 2[1] to $a = \alpha_1 = \max|\alpha_i| > 0$. If $a = 1$ then $\mathbb{E}|L| = 2\tau$. Let $0 < a < 1$. By Lemma 1.3 it suffices to show $\mathbb{E}R_a(bM) \le \tau(1-a)$. Since $u \le u_0 < \bar{u}_0$, the point (u, a) lies in $[1, \bar{u}_0] \times (0, 1)$, and exactly one of the following applies (we take the first that applies).

(1) $a \ge \frac{9}{10}$: Lemma 1.14 gives $\mathbb{E}R_a(bM) \le 0.9402\,\tau(1-a) < \tau(1-a)$.

(2) $(u, a) \in [\frac{611}{400}, \bar{u}_0] \times [\frac{16}{25}, \frac{77}{100}]$: choose $t \in [\frac{9}{25}, \frac{471}{1000}]$ with $a(t) = a$; then $b(t) = \sqrt{1-a^2} = b$. The point (u, t) lies in a verified box of Section 1.7.2, so the hypotheses of Lemma 1.12 hold at (u, a, b) with that box's c_4 (note $1 < \frac{611}{400} \le u < \frac{19}{10}$). By Corollary 1.13 (here $q \ge q_0$), $\mathbb{E}|L| \le 2\tau$.

(3) Otherwise $(u, a) \in \mathcal{S}$, so it lies in a verified cell $[u_1, u_2] \times [a_1, a_2]$ of Section 1.7.1. Then $\max|\beta_i| \le \min(1, a/b)$, and Lemma 1.9 gives $\mathbb{E}R_a(bM) < \tau(1-a)$.

In every case $\mathbb{E}|L| \le 2\tau$. Since $\alpha = e_1$ gives $\mathbb{E}|L| = 2\tau$, $R(q) = 2\tau$.

(b) By Lemma 1.2 let $q < q_0 \le \frac{1}{2}$. Lemma 1.10 with $a = b = 1/\sqrt{2}$ gives $R(q) \ge \sqrt{2}(1-q)\,2\tau > 2\tau$.

(c) Let $q \in [q_0, \frac{1}{2}]$ and suppose $\mathbb{E}|L| = 2\tau$ with $0 < a < 1$. In cases (1) and (3) the inequality is strict. So case (2) applies, and Corollary 1.13 gives $q = q_0$, $a = b = 1/\sqrt{2}$ and $M = \chi_j$. So $\alpha = (e_1 + e_j)/\sqrt{2}$, up to the global sign and the permutation used in the reduction. Conversely these vectors attain 2τ at q_0 by Lemma 1.10, since $\sqrt{2}(1-q_0) = 1$. If $a = 1$ then $\alpha = \pm e_j$. For $q \in [\frac{1}{2}, 1-q_0]$ use Lemma 1.2. □

1.9 Remarks

1. **Why six moments suffice.** The proof never uses an induction hypothesis, a tail bound, or a bound on $\mathbb{E}|M|$. The only information about the remainder M is its first six moments, which are pinned by Lemma 1.5 to the power sums of the coefficients. When $a = b = 1/\sqrt{2}$ the admissible region contains $p_3 = p_4 = p_5 = p_6 = 1$. A law with the first four moments of χ is the law of χ, because $\mathbb{E}[(M-u)^2(M+v)^2]$ is determined by these moments and vanishes. So the six-moment relaxation is exact at the extremiser $(e_1+e_2)/\sqrt{2}$. Numerically its margin near $(q_0, 1/\sqrt{2})$ is $\approx \sqrt{2}(q-q_0)$, the true margin of the two-coefficient example. This is why the method reaches exactly q_0, and why the quartic certificate (which is exact at that point) is needed only in a small box.

2. **Small a.** As $a \to 0$ the six-moment bound tends to $\sup\{\mathbb{E}|X| : \mathbb{E}X^k = \mathbb{E}Z^k,\ k \le 6\} \approx 0.8881$ (Z standard Gaussian). This is below 2τ exactly when $q > 0.27015$ (the value 0.8880738 equals 2τ at $q = 0.2701496$), so the mechanism has room to spare on $[q_0, \frac{1}{2}]$.

3. **Relation to BF3.** BF3 proved (a) for $q \in [3/8, 5/8]$ by Stein's method (zero-bias coupling and a Stein solution for $|x|$) together with a cubic inequality. That method stops near $q \approx 0.37$. The present argument is independent of BF3 and covers the full conjectured

[1] Editorial note. Section 2 of the source paper, that is, Section 1.2 ("Reductions"). The reference is kept as written; see Appendix C.

range. We independently re-verified BF3's proof on $[3/8, 5/8]$ (logic and exact arithmetic; `verify_thmK_bf3.py`, `check_mills.py`).

4. **Outside the range.** For $q < q_0$ the answer is different, since $(e_1 + e_2)/\sqrt{2}$ already beats e_1. Determining $R(q)$ there is a separate problem.

A sample certificate (appendix of the source paper)

The cell $[\frac{24583497}{16000000}, \bar{u}_0] \times [\frac{63}{100}, \frac{16}{25}]$ (file r1d) has the certificate with coefficients (rounded here; exact rationals are in the file)

$$(c_0, \ldots, c_6) \approx (0.0281054,\ 0.1163502,\ 0.1316753,\ 0.0212156,\ -0.0041259,\ -0.0021216,\ 0.0003276).$$

For example, $c_1 = \frac{114188429368}{981419917709}$ and $c_5 = -\frac{22338039}{10529058835}$. The quartic box containing $(u_0, \sqrt{2} - 1)$, which corresponds to the extremiser $(e_1 + e_2)/\sqrt{2}$ at q_0, is $[1.5521319,\ \bar{u}_0] \times [0.4120313,\ 0.4155]$, with $c_4 \approx 0.0024140$. On that box the certified lower bounds are $4c_4 s - B_0^2 \geq 5.7 \cdot 10^{-4}$ and $\kappa_3 B_0 - 4c_4 \geq 6.1 \cdot 10^{-3}$.[2]

[2] Editorial note. The refereed text (`MAIN_RESULT.tex`, md5 `6816732f...`) read $6.2 \cdot 10^{-3}$ here, a nearest rounding of the certified lower bound $6.158 \cdot 10^{-3}$. RQ-AUD raised this as finding f3 of A.6 (23 October, 02:55 UTC); RQ-A corrected the figure at 03:04 UTC and RQ-AUD checked the correction at 03:30 UTC (A.6, addendum 2: certified $\kappa_3 B_0 - 4c_4 \geq 6.1597 \cdot 10^{-3}$ on this box). This figure is the only difference from the refereed text. The proof does not use it: it uses the verification of every quartic box (Section 1.7.2), and this appendix only illustrates one box.

Chapter 2

The $k = 2$ regime of $R(q)$: $R(q) = 2\sqrt{2}\,(1-q)\sqrt{q(1-q)}$ for $1 - \sqrt{2/3} \le q \le 1 - 1/\sqrt{2}$

Source: RQ-A, `MAIN_RESULT_K2.tex` (md5 `280e80ed1839752895c6874873ec8c12`), by "RQ-A (R(q) attack)", dated 22 October 2026. Its main result, Theorem 2.1, is the team's "Theorem 2" (claim MAIN-2).

Refereed version: md5 `1cb83e45df78e366846d520996c3ea32`, the file in commit `6ecd564`. The source differs from it only in the status item of the closing remarks, which now records the referee's verdict.

Audit: A.11, VALID and NEW, no fix (22 October, 08:52 UTC).

Referee: RQ-REF1, VALID, no fixes (report `REFEREE.md`, md5 `369c1cfb...`, mirrored at 15:38 UTC on 22 October).

Use in the Main Theorem: Step 1, through Corollary 5.2.

Transcription: the whole paper, with the mechanical changes of Appendix C: labels prefixed by `ch02:`, numbers n become $2.n$, the title becomes the chapter title, no table of contents, the abstract as a quoted block. No editorial footnotes.

Abstract of the source paper. For $q \in (0,1)$ let $\chi_1, \chi_2, \dots$ be i.i.d. normalised q-biased bits and let $R(q)$ be the supremum of $\mathbb{E}|\sum \alpha_i \chi_i|$ over unit vectors α. We prove that $R(q) = 2\sqrt{2}\,(1-q)\sqrt{q(1-q)}$, the value of $(e_1+e_2)/\sqrt{2}$, for every $q \in [q_3, q_0] = [1-\sqrt{2/3},\, 1-1/\sqrt{2}] \approx [0.1835, 0.2929]$ (and the mirror statement on $[1-q_0, 1-q_3]$). We also determine all extremisers. The interval is sharp at both ends: below q_3 the vector $(e_1+e_2+e_3)/\sqrt{3}$ is better, and above q_0 the vector e_1 is better. Together with our central-range theorem (Theorem 1 of `MAIN_RESULT`), this determines $R(q)$ for all $q \in [q_3, 1-q_3]$. The proof splits off the two largest coefficients and bounds the conditional expectation, as a function of the remainder, by degree-six polynomials whose expectations depend only on six moments of the remainder. A fourth-moment tail bound handles a neighbourhood of the extremiser. At the triple point $(q_3, (e_1+e_2+e_3)/\sqrt{3})$ we split further according to the size and sign of the largest remaining coefficient. One of the three branches uses a three-coordinate version of the tail bound together with an exact three-bit lemma. The computer-assisted steps (55 515 boxes and 784 cells) use exact rational arithmetic and certified interval arithmetic, and all of them were repeated by an independent program.

2.1 Statement

Fix $q \in (0,1)$ and put

$$u = \sqrt{\tfrac{1-q}{q}}, \qquad v = \frac{1}{u}, \qquad \tau = \sqrt{q(1-q)}.$$

Let $\chi, \chi_1, \chi_2, \dots$ be i.i.d. with $\Pr[\chi = u] = q$ and $\Pr[\chi = -v] = 1-q$, so that $\mathbb{E}\chi = 0$, $\mathbb{E}\chi^2 = 1$ and $\mathbb{E}|\chi| = 2\tau$. Let

$$R(q) = \sup_{n \geq 1} \sup_{\alpha \in \mathbb{R}^n \setminus \{0\}} \frac{\mathbb{E}|\sum_{i=1}^n \alpha_i \chi_i|}{|\alpha|_2}.$$

Put

$$q_0 = 1 - \tfrac{1}{\sqrt{2}} \approx 0.292893, \qquad q_3 = 1 - \sqrt{2/3} \approx 0.183503, \qquad T(q) = 2\sqrt{2}\,(1-q)\,\tau.$$

Theorem 2.1. *(a) For every $q \in [q_3, q_0]$, every $n \geq 1$ and every $\alpha \in \mathbb{R}^n$ with $|\alpha|_2 = 1$,*

$$\mathbb{E}\Big|\sum_{i=1}^n \alpha_i \chi_i\Big| \leq 2\sqrt{2}\,(1-q)\sqrt{q(1-q)}.$$

For $q \in [1-q_0, 1-q_3]$ the same holds with $1-q$ replaced by q. Consequently $R(q) = 2\sqrt{2}\max(q, 1-q)\sqrt{q(1-q)}$ for $q \in [q_3, q_0] \cup [1-q_0, 1-q_3]$.

(b) (Extremisers.) Let $q \in [q_3, q_0] \cup [1-q_0, 1-q_3]$. Equality in (a) holds if and only if $\alpha = \pm\frac{1}{\sqrt{2}}(e_i + e_j)$ with $i \neq j$, or $q \in \{q_0, 1-q_0\}$ and $\alpha = \pm e_i$, or $q \in \{q_3, 1-q_3\}$ and $\alpha = \pm\frac{1}{\sqrt{3}}(e_i + e_j + e_k)$ with i, j, k distinct.

(c) (Sharpness.) For $q \in (0, q_3)$, $R(q) \geq 2\sqrt{3}\,(1-q)^2\tau > T(q)$. For $q \in (q_0, \frac{1}{2}]$, $R(q) \geq 2\tau > T(q)$. Hence $\{q \in (0, \frac{1}{2}] : R(q) = T(q)\} = [q_3, q_0]$.

Corollary 2.2. *With Theorem 1 of `MAIN_RESULT` ($R(q) = 2\tau$ on $[q_0, 1-q_0]$):*

$$R(q) = 2\sqrt{q(1-q)}\,\max\{1,\ \sqrt{2}(1-q),\ \sqrt{2}\,q\} \qquad \text{for all } q \in [q_3, 1-q_3].$$

Part (c) and the lower bound $R \geq T$ in (a) are elementary (Lemma 2.4). The content is the upper bound in (a), and (b).

Conventions. $x_+ = \max(x, 0)$. All polynomials in the computer-assisted parts have rational coefficients. "Verified" means verified in exact rational arithmetic or in outward-rounded interval arithmetic, as specified in Section 2.9. For a rational $x \geq 0$ we write $\lfloor\sqrt{x}\rfloor_{15} = \lfloor 10^{15}\sqrt{x}\rfloor / 10^{15}$ and $\lceil\sqrt{x}\rceil_{15} = (\lfloor 10^{15}\sqrt{x}\rfloor + 1)/10^{15}$ (integer square roots).

2.2 Reductions

2.2.1 Symmetry and parametrisation

Lemma 2.3. *The law of $-\chi^{(q)}$ is the law of $\chi^{(1-q)}$. Hence $\mathbb{E}|\sum \alpha_i \chi_i^{(q)}| = \mathbb{E}|\sum \alpha_i \chi_i^{(1-q)}|$, $R(q) = R(1-q)$, and the extremisers for q and $1-q$ coincide.*

Proof. $-\chi^{(q)}$ takes the value $-u_q$ with probability q and v_q with probability $1-q$; since $u_{1-q} = v_q$ and $v_{1-q} = u_q$, this is the law of $\chi^{(1-q)}$. Finally $|\sum \alpha_i(-\chi_i)| = |\sum \alpha_i \chi_i|$. □

From now on $q \le \frac{1}{2}$, i.e. $u \ge 1$, and

$$q = \frac{1}{1+u^2}, \quad 1-q = \frac{u^2}{1+u^2}, \quad v = \frac{1}{u}, \quad \tau = \frac{u}{1+u^2}, \quad qu = (1-q)v = \tau. \tag{2.1}$$

On $u \ge 1$, τ and q are decreasing and $1-q$ is increasing in u. The target is

$$T = 2\sqrt{2}(1-q)\tau = \sqrt{2}\,\tilde{T}(u), \qquad \tilde{T}(u) = \frac{2u^3}{(1+u^2)^2}, \qquad \frac{d}{du}\frac{u^3}{(1+u^2)^2} = \frac{u^2(3-u^2)}{(1+u^2)^3},$$

so $\tilde{T}$ is increasing on $[1, \sqrt{3}]$ and decreasing on $[\sqrt{3}, \infty)$. In particular, for $1 \le u_1 < u_2$ and $u \in [u_1, u_2]$,

$$T(u) \;\ge\; T^-(u_1, u_2) := S_2 \min\{\tilde{T}(u_1), \tilde{T}(u_2)\}, \qquad S_2 = \lfloor\sqrt{2}\rfloor_{15} < \sqrt{2}. \tag{2.2}$$

The range $q \in [q_3, q_0]$ corresponds to $u \in [u_0, u_3]$ with

$$u_0 = \sqrt{1+\sqrt{2}} \approx 1.5537740, \qquad u_3 = \sqrt{2+\sqrt{6}} \approx 2.1093814,$$

because $(1-q_0)/q_0 = 1/(\sqrt{2}-1) = 1+\sqrt{2}$ and $(1-q_3)/q_3 = \sqrt{2}/(\sqrt{3}-\sqrt{2}) = 2+\sqrt{6}$. We fix the rationals

$$U_- = \frac{1553773}{1000000} < u_0, \qquad U_+ = \frac{1054691}{500000} = 2.109382 > u_3,$$

(indeed $U_-^4 - 2U_-^2 - 1 < 0$, and $U_+^2 > 2$ with $(U_+^2-2)^2 > 6$). The computations cover $u \in [U_-, U_+]$; the theorem uses only $u \in [u_0, u_3]$.

2.2.2 Values of a few vectors

Lemma 2.4. *Let $k \ge 1$ and $q < 1/k$. Then $\mathbb{E}|\chi_1 + \cdots + \chi_k|/\sqrt{k} = 2\sqrt{k}\,(1-q)^{k-1}\tau$. In particular $\mathbb{E}|\chi_1| = 2\tau$, $\mathbb{E}|\chi_1+\chi_2|/\sqrt{2} = T$ (for $q < \frac{1}{2}$; also at $q = \frac{1}{2}$ by continuity), and $\mathbb{E}|\chi_1+\chi_2+\chi_3|/\sqrt{3} = 2\sqrt{3}(1-q)^2\tau$ for $q < \frac{1}{3}$. For $q \le \frac{1}{2}$: $2\tau \le T$ iff $q \le q_0$; and for $q < \frac{1}{3}$: $2\sqrt{3}(1-q)^2\tau \le T$ iff $q \ge q_3$.*

Proof. Let $S = \chi_1 + \cdots + \chi_k$ and let $x_i = \mathbf{1}\{\chi_i = u\}$. If some $x_i = 1$ then $S \ge u - (k-1)v > 0$, because $u^2 > k-1$ is equivalent to $q < 1/k$. If all $x_i = 0$ then $S = -kv < 0$. So $|S| = fS$ with $f = 2\cdot\mathbf{1}\{\exists i : x_i = 1\} - 1 = 1 - 2\cdot\mathbf{1}\{\text{all } x_i = 0\}$. Since $\mathbb{E}\chi_i = 0$, $\mathbb{E}[f\chi_i] = -2\mathbb{E}[\chi_i \mathbf{1}\{\text{all } x = 0\}] = -2(1-q)^k(-v) = 2(1-q)^{k-1}(1-q)v = 2(1-q)^{k-1}\tau$. Summing over i gives $\mathbb{E}|S| = 2k(1-q)^{k-1}\tau$. The comparisons: $2\tau \le 2\sqrt{2}(1-q)\tau$ iff $1-q \ge 1/\sqrt{2}$; and $2\sqrt{3}(1-q)^2\tau \le 2\sqrt{2}(1-q)\tau$ iff $1-q \le \sqrt{2/3}$. □

2.2.3 Splitting off the two largest coefficients

Let $|\alpha|_2 = 1$ and $L = \sum \alpha_i\chi_i$. Changing the sign of α and permuting coordinates does not change $\mathbb{E}|L|$. So we may assume

$$a_1 := \alpha_1 = \max_i |\alpha_i| > 0, \qquad a_2 := |\alpha_2| = \max_{i\ge 2} |\alpha_i|, \qquad |\alpha_3| \ge |\alpha_4| \ge \cdots,$$

and we put $s = \operatorname{sgn}\alpha_2 \in \{1, -1\}$ ($s = 1$ if $\alpha_2 = 0$),

$$r = \sqrt{a_1^2 + a_2^2} \in (0, 1], \qquad b = \sqrt{1-r^2}.$$

If $r < 1$, let $\beta_i = \alpha_i/b$ for $i \geq 3$ and $M = \sum_{i\geq 3} \beta_i \chi_i$. Then

$$L = a_1\chi_1 + s\, a_2\chi_2 + bM, \qquad \sum_{i\geq 3} \beta_i^2 = 1, \qquad m := \max_{i\geq 3} |\beta_i| = \frac{|\alpha_3|}{b} \leq \min\Big(1, \frac{a_2}{b}\Big),$$

and M is independent of (χ_1, χ_2). We use half-angle coordinates for (a_1, a_2):

$$a_1 = r\, c(t), \quad a_2 = r\, d(t), \qquad c(t) = \frac{1-t^2}{1+t^2}, \quad d(t) = \frac{2t}{1+t^2}, \qquad t = \frac{a_2}{r + a_1}.$$

Since $0 \leq a_2 \leq a_1$, the angle θ with $\tan\theta = a_2/a_1$ is in $[0, \pi/4]$ and $t = \tan(\theta/2) \in [0, \sqrt{2} - 1]$. We fix $T_8 = \frac{20711}{50000} = 0.41422 \geq \sqrt{2} - 1$ (indeed $(T_8 + 1)^2 \geq 2$). On $[0, 1]$, c is decreasing and d is increasing in t, and $c^2 + d^2 = 1$. Thus every unit α gives a point

$$(u, t, r, s) \in [U_-, U_+] \times [0, T_8] \times (0, 1] \times \{1, -1\} \qquad (u \in [u_0, u_3]).$$

We put $A_S = \frac{9}{20}$. If $a_1 \leq A_S$ we use the one-coordinate route of Section 2.5; otherwise $r \geq a_1 > A_S$ and we use the two-coordinate route of Sections 2.6–2.8.

2.3 Exact evaluations

2.3.1 Two coordinates

Lemma 2.5 (two-coordinate value)**.** *Let $q \leq \frac{1}{2}$, $c, d \geq 0$, $s \in \{1, -1\}$, and $X = c\chi_1 + s\, d\chi_2$. List the atoms of X as $(\chi_1, \chi_2) = (u, u), (u, -v), (-v, u), (-v, -v)$, with probabilities $p = (q^2,\ q(1-q),\ q(1-q),\ (1-q)^2)$ and values x_j. Then $p_j x_j = \tau g_j$ with*

$$g = \big(q(c + sd),\ (1-q)c - s\, q\, d,\ -q\, c + s(1-q)d,\ -(1-q)(c + sd)\big), \tag{2.3}$$

and

$$\mathbb{E}|X| = 2\tau \max\{c,\ d,\ [s = 1]\,(1-q)(c+d)\}$$

(the last entry is present only for $s = 1$). If moreover $q \leq q_0$, then $\mathbb{E}|X| \leq T\sqrt{c^2 + d^2}$, and for $(c, d) \neq 0$ equality holds if and only if $s = 1$ and $c = d$, or $q = q_0$ and $cd = 0$.

Proof. The identities $p_j x_j = \tau g_j$ follow from (2.1); for example $q(1-q)(cu - sdv) = (1-q)\tau c - q\tau sd$. Since $\mathbb{E}X = 0$, $\mathbb{E}|X| = 2\mathbb{E}X_+ = 2\tau \sum_j (g_j)_+$. For $s = 1$: $g_1 \geq 0 \geq g_4$, so $\mathbb{E}X_+/\tau = q(c+d) + ((1-q)c - qd)_+ + ((1-q)d - qc)_+$. If both middle terms are nonnegative this equals $(1-q)(c+d)$, and then $(1-q)(c+d) - c = (1-q)d - qc \geq 0$ and similarly $\geq d$. If only the first is nonnegative it equals $q(c+d) + (1-q)c - qd = c$, and $(1-q)(c+d) - c = (1-q)d - qc < 0$, while $c \geq d$ (otherwise $(1-q)d - qc \geq (1-2q)c \geq 0$). The case where only the second is nonnegative is symmetric. Both negative would give $(1-q)(c+d) < q(c+d)$, impossible for $q \leq \frac{1}{2}$ unless $c = d = 0$. In all cases $\mathbb{E}X_+/\tau = \max\{c, d, (1-q)(c+d)\}$. For $s = -1$: $g_2 \geq 0 \geq g_3$. If $c \geq d$ then $g_1 \geq 0 \geq g_4$ and $\mathbb{E}X_+/\tau = q(c-d) + (1-q)c + qd = c$. If $c < d$ then $g_1 < 0 < g_4$ and $\mathbb{E}X_+/\tau = (1-q)c + qd + (1-q)(d-c) = d$. So $\mathbb{E}X_+/\tau = \max(c, d)$.

For the bound let $\rho = \sqrt{c^2 + d^2} > 0$. Then $\max(c, d) \leq \rho$ with equality iff $cd = 0$, and $2\tau\rho \leq T\rho$ iff $\sqrt{2}(1-q) \geq 1$ iff $q \leq q_0$, with equality iff $q = q_0$. Also $(1-q)(c+d) \leq \sqrt{2}(1-q)\rho$ with equality iff $c = d$. This gives the bound and the equality cases. □

2.3.2 Three coordinates

For $f : \{0,1\}^3 \to [-1,1]$ and $x_i = \mathbf{1}\{\chi_i = u\}$ put $\Delta_i(f) = \mathbb{E}[f \mid x_i = 1] - \mathbb{E}[f \mid x_i = 0]$, a polynomial in q. Then, by (2.1),

$$\mathbb{E}[f\chi_i] = qu\,\mathbb{E}[f \mid x_i = 1] - (1-q)v\,\mathbb{E}[f \mid x_i = 0] = \tau\,\Delta_i(f). \tag{2.4}$$

Lemma 2.6 (three-bit lemma)**.** *Let $q \in [q_3, q_0]$ and $c \in \mathbb{R}^3$. Then*

$$G_3(c) := \mathbb{E}|c_1\chi_1 + c_2\chi_2 + c_3\chi_3| \le T\,|c|.$$

For $c \neq 0$ equality holds if and only if c is a positive multiple of one of: $\pm(e_i + e_j)$ $(i \neq j)$; $\pm(e_1+e_2+e_3)$, and then $q = q_3$; $\pm e_i$, and then $q = q_0$.

Proof. Let $X = c \cdot \chi$ and $f^* = \operatorname{sgn} X$ (with $\operatorname{sgn} 0 = 1$), a function of (x_1, x_2, x_3) with values ± 1. By (2.4) and Cauchy–Schwarz,

$$G_3(c) = \mathbb{E}[f^* X] = \tau \sum_i c_i \Delta_i(f^*) \le \tau|c|\,|\Delta(f^*)|.$$

Claim: for each of the $2^8 = 256$ functions $f : \{0,1\}^3 \to \{-1,1\}$, the polynomial $P_f(q) = 8(1-q)^2 - \sum_{i=1}^3 \Delta_i(f)^2$ is ≥ 0 on $[q_3, q_0]$. Moreover $P_f \equiv 0$ exactly for $f = \pm(2 \cdot \mathbf{1}\{x_i \vee x_j\} - 1)$ (six functions); $P_f(q_3) = 0 \neq P_f$ exactly for $f = \pm(2 \cdot \mathbf{1}\{x_1 \vee x_2 \vee x_3\} - 1)$; and $P_f(q_0) = 0 \neq P_f$ exactly for $f = \pm(2x_i - 1)$. Given the claim, $G_3(c) \le \tau|c|\sqrt{8}(1-q) = T|c|$.

The claim is a finite exact computation (Section 2.9, part G). For each f, P_f is computed symbolically as a polynomial with rational coefficients (degree ≤ 4). Let $\mu_3(q) = 3q^2 - 6q + 1$ and $\mu_0(q) = 2q^2 - 4q + 1$; these are the minimal polynomials of q_3 and q_0 (irreducible over $\mathbb{Q}$, since 24 and 8 are not squares). Their other roots $1 + \sqrt{2/3}$ and $1 + 1/\sqrt{2}$ lie above 1, so $\mu_3 \le 0$ on $[q_3, 1]$ and $\mu_0 \ge 0$ on $[0, q_0]$. Take rational enclosures $q_3 \in [q_3^-, q_3^+]$ and $q_0 \in [q_0^-, q_0^+]$ of width 10^{-15}. The signs of μ_3, μ_0 at the enclosure endpoints are asserted. Then: (i) by Sturm sequences, P_f has no root in $[q_3^+, q_0^-]$, and $P_f(q_3^+) > 0$; (ii) near q_3: if $\mu_3 \mid P_f$, write $P_f = \mu_3 Q$; then Q has no root in $[q_3^-, q_3^+]$ and $Q(q_3^+) < 0$, so $P_f \ge 0$ on $[q_3, q_3^+]$; otherwise P_f has no root in $[q_3^-, q_3^+]$ and $P_f(q_3^+) > 0$; (iii) near q_0, in the same way with μ_0 and $Q(q_0^-) > 0$. The six functions with $P_f \equiv 0$ are $\pm$ the OR of two bits, by Lemma 2.4 ($\Delta(f) = 2(1-q)(e_i + e_j)$).

Equality. Suppose $G_3(c) = T|c|$ with $c \neq 0$. Then $|\Delta(f^*)|^2 = 8(1-q)^2$, so $P_{f^*}(q) = 0$, and c is a positive multiple of $\Delta(f^*)$. By the claim, f^* is $\pm$OR of two bits, with $\Delta = \pm 2(1-q)(e_i + e_j)$; or $q = q_3$ and $f^* = \pm\mathrm{OR}_3$, with $\Delta = \pm 2(1-q)^2(1,1,1)$; or $q = q_0$ and $f^* = \pm(2x_i - 1)$, with $\Delta = \pm 2e_i$. Conversely, these c attain $T|c|$ by Lemmas 2.4 and 2.5. □

Remark 2.7. Lemma 2.6 is the case $n = 3$ of RQ-C's result C6: for $n \le 7$ and all $q \in (0,1)$, $R_n(q) = 2\tau\sqrt{\max_{k \le n} k(1-\bar{q})^{2k-2}}$ with $\bar{q} = \min(q, 1-q)$, with only OR_k extremal. RQ-AUD audited C6 VALID (A.5 for $n \le 6$, A.5b for $n = 7$). Our check is independent of it.

2.4 Moments of the remainder

Lemma 2.8. *The cumulants of χ are $\kappa_1 = 0$, $\kappa_2 = 1$, and, with $w = u^2 + v^2$, $\kappa_3 = u - v$, $\kappa_4 = w - 4$, $\kappa_5 = (u-v)(w-10)$, $\kappa_6 = w^2 - 26w + 64$.*

Proof. By (2.1), $m_k = \mathbb{E}\chi^k = (u^k + (-1)^k u^{2-k})/(1+u^2)$, which gives $m_3 = u - v$, $m_4 = w - 1$, $m_5 = (u-v)w$ and $m_6 = w^2 - w - 1$. (Use $u^4 - 1 = (u^2+1)(u^2-1)$, $u^6 + 1 = (u^2+1)(u^4 - u^2 + 1)$, $u^8 - 1 = (u^2+1)(u^2-1)(u^4+1)$ and $u^{10} + 1 = (u^2+1)(u^8 - u^6 + u^4 - u^2 + 1)$.) For a centred variable with unit variance, $\kappa_3 = m_3$, $\kappa_4 = m_4 - 3$, $\kappa_5 = m_5 - 10m_3$ and $\kappa_6 = m_6 - 15m_4 - 10m_3^2 + 30$. Using $(u-v)^2 = w - 2$ gives the formulas. (Verified symbolically in `verify_all.py`, part A1.) □

Lemma 2.9. *Let $M = \sum \beta_i \chi_i$ (finite sum) with $\sum \beta_i^2 = 1$ and power sums $p_j = \sum_i \beta_i^j$. Then $\mathbb{E}M = 0$, $\mathbb{E}M^2 = 1$, and*

$$\mathbb{E}M^3 = \kappa_3 p_3, \quad \mathbb{E}M^4 = 3 + \kappa_4 p_4, \quad \mathbb{E}M^5 = \kappa_5 p_5 + 10\kappa_3 p_3, \quad \mathbb{E}M^6 = 15 + 15\kappa_4 p_4 + 10\kappa_3^2 p_3^2 + \kappa_6 p_6.$$

Proof. Cumulants of independent sums add and are homogeneous, so M has cumulants $K_1 = 0$, $K_2 = 1$ and $K_j = \kappa_j p_j$. For a centred variable, $m_3 = K_3$, $m_4 = K_4 + 3K_2^2$, $m_5 = K_5 + 10K_3K_2$ and $m_6 = K_6 + 15K_4K_2 + 10K_3^2 + 15K_2^3$. □

Lemma 2.10. *If $\sum \beta_i^2 = 1$ and $\max|\beta_i| \le m \le 1$, then $p_3^2 \le p_4 \le m^2$, $p_4^2 \le p_6 \le m^2 p_4$, $|p_5| \le m p_4$ and $0 \le p_4 \le 1$.*

Proof. Cauchy–Schwarz gives $p_3^2 = (\sum \beta_i \beta_i^2)^2 \le \sum \beta_i^2 \sum \beta_i^4 = p_4$ and $p_4^2 = (\sum \beta_i \beta_i^3)^2 \le p_2 p_6 = p_6$. Also $p_4 \le m^2 \sum \beta_i^2 = m^2$, $p_6 \le m^2 p_4$ and $|p_5| \le \sum |\beta_i| \beta_i^4 \le m p_4$. □

Lemma 2.11 (sign information)**.** *Let $\sum \beta_i^2 = 1$, $m = \max|\beta_i|$, and suppose $\beta_{i_0} = -m$ for some i_0. If $m \ge m_c \in (0,1]$, then $p_3 \le \varphi(m_c) := -m_c^3 + (1 - m_c^2)^{3/2}$.*

Proof. For $i \ne i_0$, $|\beta_i| \le (\sum_{i \ne i_0} \beta_i^2)^{1/2} = \sqrt{1 - m^2}$. Hence $p_3 = -m^3 + \sum_{i \ne i_0} \beta_i^3 \le -m^3 + \sqrt{1-m^2} \sum_{i \ne i_0} \beta_i^2 = -m^3 + (1-m^2)^{3/2}$. Finally $\frac{d}{dm}\big(-m^3 + (1-m^2)^{3/2}\big) = -3m^2 - 3m\sqrt{1-m^2} \le 0$. □

Cumulant enclosures. For $1 \le u_1 \le u \le u_2$: $\kappa_3 = u - 1/u$ and $w = u^2 + u^{-2}$ are increasing, so $\kappa_3 \in [k_3^-, k_3^+] = [u_1 - \frac{1}{u_1}, u_2 - \frac{1}{u_2}]$ and $w \in [w^-, w^+]$. We require $w^+ < 13$ (here $w^+ < 4.7$). Then $\kappa_4 \in [w^- - 4, w^+ - 4]$, $\kappa_6 \in [f_6(w^+), f_6(w^-)]$ with $f_6(x) = x^2 - 26x + 64$ (decreasing for $x < 13$), and $|\kappa_5| \le k_5^+ := k_3^+ \max(|w^- - 10|, |w^+ - 10|)$.

Definition 2.12 (objective bound)**.** For $c = (c_0, \dots, c_6)$, an interval $[u_1, u_2]$ with $u_1 > 1$, a number $m^* \in (0,1]$, an optional number $p^* < 0$, and a target Θ, put

$$\begin{aligned} A &= c_0 + c_2 + 3c_4 + 15c_6, & \bar{B} &= k_3^+ |c_3 + 10c_5|, \\ C^+ &= \max_{\kappa_4 \in [w^- - 4, w^+ - 4]} \kappa_4 (c_4 + 15c_6), & \bar{D} &= k_5^+ |c_5|, \\ E^+ &= \max\{f_6(w^-)c_6, f_6(w^+)c_6\}, & F^+ &= \max\{0, 10(k_3^-)^2 c_6, 10(k_3^+)^2 c_6\}, \end{aligned}$$

$\Gamma = C^+ + \bar{D} m^* + F^+ + \max(E^+, 0) m^{*2}$ and $\varepsilon = \min(E^+, 0)$. If p^* is given and $c_3 + 10c_5 \ge 0$, replace A by $A + k_3^-(c_3 + 10c_5)p^*$ and $\bar{B}$ by 0. We say that c *satisfies the objective bound for* $(u_1, u_2, m^*, p^*, \Theta)$ if $h(\rho) = \Theta - A - \bar{B}\rho - \Gamma\rho^2 - \varepsilon\rho^4 > 0$ for all $\rho \in [0, m^*]$.

Lemma 2.13 (expectation bound)**.** *Suppose c satisfies the objective bound for $(u_1, u_2, m^*, p^*, \Theta)$, and let $P(y) = \sum_k c_k y^k$. Then $\mathbb{E}P(M) < \Theta$ for every $u \in [u_1, u_2]$ and every $M = \sum \beta_i \chi_i$ with $\sum \beta_i^2 = 1$ and $\max|\beta_i| \le m^*$, and, if p^* is given, $p_3 \le p^*$.*

Proof. By Lemma 2.9, $\mathbb{E}P(M) = A + \kappa_3(c_3 + 10c_5)p_3 + \kappa_4(c_4 + 15c_6)p_4 + \kappa_5 c_5 p_5 + \kappa_6 c_6 p_6 + 10\kappa_3^2 c_6 p_3^2$, with A the unmodified value. Put $\rho = \sqrt{p_4} \in [0, m^*]$ (Lemma 2.10). Then $\kappa_3(c_3 + 10c_5)p_3 \le \bar{B}\rho$ since $|p_3| \le \rho$. If p^* is given and $c_3 + 10c_5 \ge 0$, then instead $\kappa_3(c_3 + 10c_5)p_3 \le \kappa_3(c_3 + 10c_5)p^* \le k_3^-(c_3 + 10c_5)p^*$, using $\kappa_3 \ge k_3^- > 0$ and $p^* < 0$. Next, $\kappa_4(c_4 + 15c_6)p_4 \le C^+\rho^2$ (linear in κ_4, $p_4 \ge 0$); $\kappa_5 c_5 p_5 \le \bar{D} m^* \rho^2$; $10\kappa_3^2 c_6 p_3^2 \le F^+\rho^2$; and $\kappa_6 c_6 p_6 \le E^+ p_6$, which is $\le E^+ m^{*2}\rho^2$ if $E^+ \ge 0$ and $\le E^+\rho^4$ if $E^+ < 0$ (Lemma 2.10). Summing, $\mathbb{E}P(M) \le \Theta - h(\rho) < \Theta$. □

2.5 The one-coordinate route ($a_1 \le \frac{9}{20}$)

Here we split off only $a = a_1$: $L = a\chi_1 + b_1 M_1$ with $b_1 = \sqrt{1-a^2}$, $M_1 = \sum_{i\ge 2}(\alpha_i/b_1)\chi_i$, whose coefficients are at most $\min(1, a/b_1)$ in absolute value. By BF3, Lemma 9.4 (Lemma 3 of `MAIN_RESULT`; audited VALID in A.0 and A.3),

$$\mathbb{E}|L| = 2\tau a + 2\mathbb{E}R_a(b_1 M_1), \qquad R_a(y) = \max\{0, (1-q)(y-av),\, q(-y-au)\},$$

so $\mathbb{E}|L| < T$ iff $\mathbb{E}R_a(b_1M_1) < \tau(\sqrt{2}(1-q) - a)$.

A *cell* is $[u_1, u_2] \times [a_1, a_2]$ with rationals $1 < u_1 < u_2$, $0 \le a_1 < a_2 \le \frac{9}{20}$. Put $\bar b = \lceil \sqrt{1-a_1^2} \rceil_{15}$, $\bar m = \min\{1, a_2/\lfloor \sqrt{1-a_2^2} \rfloor_{15}\}$, and

$$\bar\ell_1(y) = \frac{u_2^2}{1+u_2^2}\Big(\bar b y - \frac{a_1}{u_2}\Big), \quad \bar\ell_2(y) = \frac{1}{1+u_1^2}\big(-\bar b y - a_1 u_1\big), \quad \Theta_1 = \tau(u_2)\Big(S_2\frac{u_1^2}{1+u_1^2} - a_2\Big).$$

A *cell certificate* is $c \in \mathbb{Q}^7$ with $P(y) = \sum c_k y^k$ such that (V1) $P > 0$, (V2) $P > \bar\ell_1$, (V3) $P > \bar\ell_2$ on $\mathbb{R}$, and (V4) c satisfies the objective bound for $(u_1, u_2, \bar m, -, \Theta_1)$.

Lemma 2.14. *If a cell has a certificate, then $\mathbb{E}|L| < T$ for every $u \in [u_1, u_2]$ and every unit α with $a_1 \le \max|\alpha_i| \le a_2$.*

Proof. For $u \in [u_1, u_2]$, $a \in [a_1, a_2]$, $b_1 = \sqrt{1-a^2}$, we have $R_a(b_1 y) \le \max\{0, \bar\ell_1, \bar\ell_2\}(y)$. This is Lemma 7 of `MAIN_RESULT`, audited VALID in A.6. We recall the proof: $R_a(b_1y) = \max\{0, \ell_1, \ell_2\}$ with $\ell_1 = \frac{u^2}{1+u^2}(b_1 y - \frac{a}{u})$ and $\ell_2 = \frac{1}{1+u^2}(-b_1 y - au)$. If $\ell_1(y) > 0$ then $y > 0$ and $0 < b_1 y - \frac{a}{u} \le \bar b y - \frac{a_1}{u_2}$, and $\frac{u^2}{1+u^2} \le \frac{u_2^2}{1+u_2^2}$. If $\ell_2(y) > 0$ then $y < 0$ and $0 < -b_1 y - au \le -\bar b y - a_1 u_1$, and $\frac{1}{1+u^2} \le \frac{1}{1+u_1^2}$. So by (V1)–(V3), $\mathbb{E}R_a(b_1M_1) \le \mathbb{E}P(M_1)$. Since $a/\sqrt{1-a^2}$ is increasing, the coefficients of M_1 are at most $\bar m$. By Lemma 2.13, $\mathbb{E}P(M_1) < \Theta_1$. Finally $\Theta_1 \le \tau(u)(\sqrt{2}(1-q) - a)$, because $\tau(u) \ge \tau(u_2)$, $1 - q \ge \frac{u_1^2}{1+u_1^2}$, $S_2 < \sqrt{2}$, $a \le a_2$, and the bracket is positive: $S_2\frac{u_1^2}{1+u_1^2} \ge 1.414 \cdot 0.707 > \frac{9}{20} \ge a_2$. □

2.6 The two-coordinate route: box certificates

A *box* is $B = [u_1, u_2] \times [t_1, t_2] \times [r_1, r_2]$ with rationals $1 < u_1 < u_2$, $0 \le t_1 < t_2 \le 1$, $0 \le r_1 < r_2 \le 1$, together with a sign s. For a point of B, $a_1 = rc(t)$, $a_2 = rd(t)$ and $b = \sqrt{1-r^2}$, as in Section 2.2.3.

Lemma 2.15 (conditional expectation)**.** *For a point of B with $r < 1$, $\mathbb{E}|L| = \mathbb{E}F(M)$, where*

$$F(y) = \sum_{j=1}^{4} p_j |x_j + by| = \sum_{j=1}^{4} \big|p_j x_j + p_j b\, y\big|,$$

x_j and p_j are the atoms and probabilities of $a_1\chi_1 + sa_2\chi_2$, and $p_j x_j = r\tau g_j$ with g as in (2.3) *(with $c = c(t)$, $d = d(t)$).*

Proof. Condition on (χ_1, χ_2) (independent of M), and use Lemma 2.5 for $(a_1, a_2) = r(c, d)$. □

Box enclosures. On B: $q \in [\frac{1}{1+u_2^2}, \frac{1}{1+u_1^2}]$, $1-q \in [\frac{u_1^2}{1+u_1^2}, \frac{u_2^2}{1+u_2^2}]$, $\tau \in [\tau(u_2), \tau(u_1)]$, $c \in [c(t_2), c(t_1)]$, $d \in [d(t_1), d(t_2)]$, $r \in [r_1, r_2]$ and $b \in [b^-, b^+]$ with $b^- = \lfloor \sqrt{1-r_2^2} \rfloor_{15}$ ($b^- = 0$ if $r_2 = 1$) and $b^+ = \lceil \sqrt{1-r_1^2} \rceil_{15}$. Interval arithmetic then gives rational enclosures $p_j x_j \in [\pi_j^-, \pi_j^+]$ and $p_j b \in [\beta_j^-, \beta_j^+]$ with $\beta_j^- \ge 0$. We define $\bar m(B) = 1$ if $b^- = 0$ or $r_2 d(t_2) \ge b^-$, and otherwise $\bar m(B)$ is a rational with $\bar m(B) \ge r_2 d(t_2)/b^-$. Then $m \le \min(1, a_2/b) \le \min(1, \bar m(B))$ at every point of B with $r < 1$.

Definition 2.16 (box envelope)**.** $F_B(y) = \sum_j \max(\pi_j^+ + \beta_j^+ y,\ -\pi_j^- - \beta_j^- y)$ for $y \geq 0$, and $F_B(y) = \sum_j \max(\pi_j^+ + \beta_j^- y,\ -\pi_j^- - \beta_j^+ y)$ for $y < 0$.

Lemma 2.17 (envelope)**.** *$F(y) \leq F_B(y)$ for all $y \in \mathbb{R}$ and all points of B with $r < 1$. On each half-line, F_B is the maximum of the 2^4 affine functions obtained by choosing one of the two lines in each summand.*

Proof. $|p_j x_j + p_j b y| = \max(p_j x_j + p_j b y,\ -p_j x_j - p_j b y)$. For $y \geq 0$: $p_j x_j + p_j b y \leq \pi_j^+ + \beta_j^+ y$ and $-p_j x_j - p_j b y \leq -\pi_j^- - \beta_j^- y$. For $y < 0$: $p_j b y \leq \beta_j^- y$ and $-p_j b y \leq -\beta_j^+ y$. A sum of maxima is the maximum over all choices. □

Definition 2.18 (box certificate)**.** Let $m^* \in (0, \min(1, \bar{m}(B))]$ and let $p^* < 0$ be optional. A *box certificate for* (B, s, m^*, p^*) is $c \in \mathbb{Q}^7$ with $P(y) = \sum c_k y^k$ such that (W1) $P(y) > F_B(y)$ for all $y \in \mathbb{R}$, and (W2) c satisfies the objective bound for $(u_1, u_2, m^*, p^*, T^-(u_1, u_2))$.

Lemma 2.19 (box certificate lemma)**.** *If c is a box certificate for (B, s, m^*, p^*), then $\mathbb{E}|L| < T(u)$ at every point of B with $r < 1$ and every remainder M with $m \leq m^*$ and, if p^* is given, $p_3 \leq p^*$.*

Proof. By Lemmas 2.15 and 2.17 and (W1), $\mathbb{E}|L| = \mathbb{E}F(M) \leq \mathbb{E}P(M)$. By Lemma 2.13 and (W2), $\mathbb{E}P(M) < T^-(u_1, u_2) \leq T(u)$, using (2.2). □

With $m^* = \min(1, \bar{m}(B))$ and no p^*, Lemma 2.19 covers every remainder. These are the boxes of kind lp.

2.7 Near the extremiser: the near-circle lemma

Lemma 2.20 (tail bound)**.** *Let $y \in \mathbb{R}$, $b \geq 0$ and let Z be a random variable with $\mathbb{E}Z = 0$ and $\mathbb{E}Z^4 < \infty$. Then*

$$\mathbb{E}|y + bZ| \leq |y| + \min\Big(b\,\mathbb{E}|Z|,\ \frac{27}{128}\,\frac{b^4 \mathbb{E}Z^4}{|y|^3}\Big),$$

where for $y = 0$ the minimum is read as its first entry. The same convention is used below whenever this bound is applied at a point where $y = 0$.

Proof. The first bound is the triangle inequality. For the second (only needed for $y \neq 0$), $|y + z| - |y| - \operatorname{sgn}(y) z = 2(-\operatorname{sgn}(y) z - |y|)_+ \leq 2(|z| - |y|)_+$, and $\mathbb{E}[\operatorname{sgn}(y) bZ] = 0$. For $x \geq 0$ and $\eta > 0$, $(x - \eta)_+ \leq \frac{27}{256} x^4/\eta^3$: the maximum of $(x - \eta)/x^4$ over $x > \eta$ is at $x = \frac{4}{3}\eta$ and equals $\frac{27}{256}\eta^{-3}$. Hence $\mathbb{E}|y + bZ| - |y| \leq 2 \cdot \frac{27}{256}\, b^4 \mathbb{E}Z^4/|y|^3$. □

Lemma 2.21 (near-circle tests)**.** *Let B be a box with $r_1 > 0$. Let y_j $(j = 1, \dots, 4)$ be the atoms of $c\chi_1 + sd\chi_2$, so that the atoms of $a_1\chi_1 + sa_2\chi_2$ are ry_j. Let $\eta_j \geq 0$ be a lower bound of $|y_j|$ on B, p_j^+ an upper bound of p_j, and $E_4 = 3 + \max(0, w^+ - 4)\ \min(1, \bar{m}(B))^2$. Let $T^- = T^-(u_1, u_2)$.*

(A) If all $\eta_j > 0$ and $\frac{27}{128} E_4 (b^+)^2 \frac{1 + r_2}{r_1^3} \sum_j p_j^+ \eta_j^{-3} < T^-$, then at every point of B with $u \geq u_0$: $\mathbb{E}|L| < T$ if $r < 1$, and $\mathbb{E}|L| \leq T$ if $r = 1$, with equality only in the cases of Lemma 2.5.

(B) Let G^+ be an upper bound of $\mathbb{E}|c\chi_1 + sd\chi_2| = \tau \sum_j |g_j|$ on B with $G^+ \leq T^-$, and $e_j^+ = \min\big(b^+, \frac{27}{128}(b^+)^4 E_4/(r_1^3 \eta_j^3)\big)$ $(e_j^+ = b^+$ if $\eta_j = 0)$. If $\sum_j p_j^+ e_j^+ < T^-(1 - r_2) + r_1(T^- - G^+)$, then $\mathbb{E}|L| < T$ at every point of B.

Proof. At a point of B with $r<1$, condition on (χ_1,χ_2) and apply Lemma 2.20 with $Z=M$. Here $\mathbb{E}M^4=3+\kappa_4 p_4\le E_4$, by Lemma 2.9, since $p_4\le m^2\le\min(1,\bar m)^2$. This gives $\mathbb{E}|L|\le rG+\sum_j p_j e_j$, where $G=\mathbb{E}|c\chi_1+sd\chi_2|$ and $e_j=\min(b,\frac{27}{128}b^4E_4/(r^3|y_j|^3))$; also $\mathbb{E}|M|\le 1$. If $r=1$ then $\mathbb{E}|L|=G$. (A) By Lemma 2.5 ($q\le q_0$), $G\le T$. Since $1-r=b^2/(1+r)$, $\sum_j p_j e_j\le\frac{27}{128}\frac{b^4E_4}{r^3}\sum_j\frac{p_j}{|y_j|^3}\le b^2\cdot\frac{27}{128}E_4(b^+)^2\frac{1}{r_1^3}\sum_j\frac{p_j^+}{\eta_j^3}<\frac{b^2T^-}{1+r_2}\le T(1-r)$ when $b>0$. So $\mathbb{E}|L|<rT+T(1-r)=T$. For $r=1$ use Lemma 2.5. (B) $\mathbb{E}|L|\le rG^+ +\sum_j p_j^+e_j^+ < rG^+ +T^-(1-r_2)+r_1(T^- -G^+)\le rG^+ +T^-(1-r)+r(T^- -G^+)=T^-\le T$, using $r_1\le r\le r_2$ and $T^- -G^+\ge 0$. □

These are the boxes of kind ncA and ncB.

2.8 Near the triple point: the m-split

At $u=u_3$ the vector $(e_1+e_2+e_3)/\sqrt{3}$ also attains T. In our coordinates it is the point $a_1=a_2=b=1/\sqrt{3}$ with $M=\chi_3$, so $m=1$ and $p_3=1$. There the six-moment relaxation is exact, and no box certificate can work near it. We split according to $m=\max_{i\ge3}|\beta_i|$ and the sign of a largest remaining coefficient.

Lemma 2.22 (three-coordinate near-sphere bound)**.** *Consider a point with $r<1$ and suppose $\beta_{i_0}=+m$ for some $i_0\ge3$. Put $a_3=bm$, $b'=b\sqrt{1-m^2}$, $Y=a_1\chi_1+sa_2\chi_2+a_3\chi_{i_0}$ with atoms y_j and probabilities p_j ($j=1,\dots,8$), $r'=\sqrt{a_1^2+a_2^2+a_3^2}=\sqrt{1-b'^2}$ and $E_4'=3+\max(0,\kappa_4)$. Then*

$$\mathbb{E}|L|\le\mathbb{E}|Y|+\sum_j p_j\min\Big(b',\ \frac{27}{128}\frac{b'^4E_4'}{|y_j|^3}\Big).$$

If moreover $q\in[q_3,q_0]$, all $y_j\ne0$ and $\frac{27}{128}E_4'\,b'^2(1+r')\sum_j p_j|y_j|^{-3}<T$, then $\mathbb{E}|L|<T$ if $b'>0$, and if $b'=0$ then $\mathbb{E}|L|=G_3(a_1,sa_2,a_3)\le T$.

Proof. If $m=1$ then $b'=0$ and $L=Y$. Otherwise $L=Y+b'M'$, where $M'=\sum_{i\ge3,\,i\ne i_0}\beta_i'\chi_i$ with $\beta_i'=\beta_i/\sqrt{1-m^2}$. Then M' is independent of Y, $\sum\beta_i'^2=1$ and $\sum\beta_i'^4\le1$, so $\mathbb{E}M'^4=3+\kappa_4\sum\beta_i'^4\le E_4'$ by Lemma 2.9. Conditioning on $(\chi_1,\chi_2,\chi_{i_0})$ and applying Lemma 2.20 with $Z=M'$ (and $\mathbb{E}|M'|\le1$) gives the first bound. By Lemma 2.6, $\mathbb{E}|Y|=G_3(a_1,sa_2,a_3)\le Tr'$. If $b'>0$, the hypothesis and $1-r'=b'^2/(1+r')$ give $\sum_j p_j\frac{27}{128}\frac{b'^4E_4'}{|y_j|^3}<T\frac{b'^2}{1+r'}=T(1-r')$, hence $\mathbb{E}|L|<Tr'+T(1-r')=T$. □

Piece tests. Let B be a box with $b^->0$, and $[m_1,m_2]\subset(0,1]$. On $B\times[m_1,m_2]$ we enclose $a_3\in[b^-m_1,b^+m_2]$, $b'^2\le(b'^2)^+:=(b^+)^2(1-m_1^2)$, $b'\le b'^+$ with b'^+ an upper bound of $\sqrt{(b'^2)^+}$, and $r'\le r'^+$ with r'^+ an upper bound of $\min\big(1,\sqrt{1-(b^-)^2(1-m_2^2)}\big)$ (recall $r'^2=1-b^2(1-m^2)$). The atoms $y_j=a_1x_{j1}+sa_2x_{j2}+a_3x_{j3}$ ($x\in\{u,-v\}^3$) and the products $p_jy_j=\tau\sum_i(\pm a_i)\prod_{k\ne i}\Pr[x_{jk}]$ (by $qu=(1-q)v=\tau$) are enclosed in interval arithmetic. Let η_j be a lower bound of $|y_j|$, p_j^+ an upper bound of p_j, and $E_4'=3+\max(0,w^+-4)$. The piece passes

- test (A3) if all $\eta_j>0$ and $\frac{27}{128}E_4'(b'^2)^+(1+r'^+)\sum_j p_j^+\eta_j^{-3}<T^-(u_1,u_2)$;
- test (B3) if $\sum_j\big(|p_jy_j|^+ +p_j^+\min\big(b'^+,\frac{27}{128}((b'^2)^+)^2E_4'/\eta_j^3\big)\big)<T^-(u_1,u_2)$, where $|p_jy_j|^+$ is an upper bound of $|p_jy_j|$ (the second entry of the minimum is omitted if $\eta_j=0$).

By Lemma 2.22, if a piece passes (A3), then at every point of B with $u \in [u_0, u_3]$ and every remainder with $\beta_{i_0} = +m$, $m \in [m_1, m_2]$, we have $\mathbb{E}|L| < T$ if $b' > 0$ and $\mathbb{E}|L| \le T$ if $b' = 0$. If it passes (B3), then $\mathbb{E}|L| < T$ by the first bound of Lemma 2.22 alone.

Definition 2.23 (m-split box)**.** An m-split box is a box B with sign s and $b^- > 0$, together with: a rational $m_c \in (0, 1]$ and a rational p^* with $\varphi(m_c) \le p^* < 0$ (this forces $2m_c^2 > 1$, because $\varphi(m) < 0$ iff $(1 - m^2)^{3/2} < m^3$ iff $2m^2 > 1$; the verifier also checks $2m_c^2 > 1$ directly); a box certificate $c^{(1)}$ for $(B, s, \min(m_c, \bar{m}(B)), -)$; a box certificate $c^{(2)}$ for $(B, s, \min(1, \bar{m}(B)), p^*)$; and pieces $[m_1, m_2]$, each passing (A3) or (B3), whose union contains $[m_c, \min(1, \bar{m}(B))]$.

Lemma 2.24 (m-split lemma)**.** *Let B be an m-split box. At every point of B with $r < 1$ and $u \in [u_0, u_3]$ we have $\mathbb{E}|L| \le T$. Equality forces $m = 1$, $\beta_{i_0} = +1$ for some i_0 (that is, $\alpha = a_1 e_1 + s a_2 e_2 + b e_{i_0}$), and $G_3(a_1, s a_2, b) = T$.*

Proof. Recall $m \le \min(1, \bar{m}(B))$. If $m \le m_c$, use $c^{(1)}$ and Lemma 2.19: $\mathbb{E}|L| < T$. If $m \ge m_c$ and $\beta_{i_0} = -m$ for some i_0, then $p_3 \le \varphi(m_c) \le p^*$ by Lemma 2.11; use $c^{(2)}$ and Lemma 2.19: $\mathbb{E}|L| < T$. Otherwise $\beta_{i_0} = +m$ for some i_0, and $m \in [m_c, \min(1, \bar{m}(B))]$ lies in a piece. The piece tests give $\mathbb{E}|L| < T$ unless $b' = 0$, i.e. $m = 1$, and then $\mathbb{E}|L| = G_3(a_1, s a_2, b) \le T$. □

2.9 Computer verification

All scripts and outputs are in the repository (`scripts/`, `outputs/`). Floating point (HiGHS linear programming via scipy) is used only to *find* certificates. Every *verification* is exact or uses outward-rounded interval arithmetic.

2.9.1 Data

- One-coordinate cells: `outputs/cover_k2/one_A.json` (450 cells, $u \in [U_-, 2]$) and `one_B.json` (334 cells, $u \in [2, U_+]$), all with $a \in [0, \frac{9}{20}]$.
- Two-coordinate boxes: 114 files `outputs/cover2c/s*.json` and `b*.json`, listed in `outputs/k2_manifest.json`. For each sign they cover $[U_-, U_+] \times [0, T_8] \times [\frac{9}{20}, 1]$. Each box record has its kind and data: lp (certificate c), ncA/ncB, small (boxes with $r_2 c(t_1) \le \frac{9}{20}$, i.e. $a_1 \le \frac{9}{20}$ on the whole box, which are left to the one-coordinate route), and ms (m_c, p^*, $c^{(1)}$, $c^{(2)}$ and the pieces).

sign	lp	ncA	ncB	ms	small	total
$s = +1$	33 479	1 680	1 909	1 189	374	38 631
$s = -1$	15 331	288	958	0	307	16 884

Table 2.1: Two-coordinate boxes. Widths range from $1.25 \cdot 10^{-3}$ to 0.01 in u, from $8.1 \cdot 10^{-4}$ to 0.052 in t and from $1.6 \cdot 10^{-3}$ to 0.05 in r. All ms boxes have $u \ge 2.09$; they carry 1 669 pieces (1 659 of type (A3), 10 of type (B3)), with $m_c \in \{\frac{31}{40}, \frac{4}{5}, \frac{33}{40}, \frac{17}{20}, \frac{7}{8}, \frac{9}{10}\}$.

2.9.2 Generation

`cover2c.py` bisects $[u_1, u_2] \times [0, T_8] \times [\frac{9}{20}, 1]$ adaptively (8 initial t-intervals, 11 r-intervals). On each box it tries, in order: small; the near-circle tests (`nearcircle.py`, exact rationals); a box certificate (`cert2c.py`); the m-split (`cover2c.try_msplit`, `nsphere3.py`). The certificates come from a discretised six-moment linear program (dual multipliers of the moment rows), rounded to rationals and repaired; (W1) is checked exactly on every linear piece of F_B by real-root counting, and (W2) exactly by bisection. One-coordinate cells come from `cover_k2.py` (the pipeline of `MAIN_RESULT` with target Θ_1). No box or cell failed.

2.9.3 Independent verification

`verify_k2.py` re-checks everything. It shares no code with the generators; it reuses only the Sturm-sequence, integer-square-root and tiling helpers of `verify_all.py` (the verifier of Theorem 1, audited in A.6). Its parts:

A. Symbolic identities (sympy): $p_j x_j = r\tau g_j$ for both signs, $\sum p_j = 1$, mean 0, the two-coordinate values, the half-angle formulas, the constant $27/256$, and the unimodality of $\tilde{T}$.

B. Coverage (exact). The one-coordinate cells tile $[U_-, U_+] \times [0, \frac{9}{20}]$. For each sign the boxes tile $[U_-, U_+] \times [0, T_8] \times [\frac{9}{20}, 1]$: they lie in the region, have pairwise disjoint interiors and total volume equal to the volume of the region. A closed subset of full measure is dense, so it is the whole region. Also $U_- < u_0$, $U_+ \geq u_3$, $T_8 \geq \sqrt{2} - 1$, and every small box has $r_2 c(t_1) \leq \frac{9}{20}$.

C. One-coordinate cells: (V1)–(V3) by Sturm sequences; (V4) strictly by Sturm on $[0, \bar{m}]$.

D. Box certificates (lp, and both certificates of each ms box): (W1) by writing F_B on each half-line as the maximum of the 16 sign-pattern lines and checking by Sturm counting that P minus each line is positive on that half-line; (W2) strictly; for ms boxes also $0 < m_c \leq 1$, $2m_c^2 > 1$, $p^* < 0$, $p^* \geq \varphi(m_c)$ (as $(p^* + m_c^3)^2 \geq (1 - m_c^2)^3$ with $p^* + m_c^3 \geq 0$), and $m^* = \min(m_c, \bar{m})$ for $c^{(1)}$. The verifier recomputes $\bar{m}$ as the exact quotient $r_2 d(t_2)/b^-$.

E. Near-circle boxes: mpmath interval arithmetic (120 bits), tests (A)/(B) strictly.

F. m-split pieces: the pieces with $s_3 = +1$ cover $[m_c, \min(1, \bar{m})]$; each passes (A3) or (B3) in mpmath interval arithmetic (120 bits); the box has $u_1 \geq 2$.

G. The three-bit claim of Lemma 2.6, for all 256 functions, by exact Sturm sequences as described there, including the list of equality cases.

The output is `outputs/verify_k2_ABCDEFG.txt` (all parts pass).

Negative tests. `break_tests_k2.py` corrupts random samples of records and runs the check functions of `verify_k2.py` on them (output `outputs/break_tests_k2.txt`). On 40 ms boxes, each of the following is rejected 40 times out of 40: lowering m_c by $\frac{1}{10}$ (the pieces no longer reach m_c); removing or halving the top piece; lowering p^* by $\frac{1}{100}$ (below $\varphi(m_c)$); lowering the constant term of $c^{(2)}$ by 10^{-3}; multiplying the constant term of $c^{(1)}$ by $\frac{99}{100}$; widening the r- or the t-interval downwards by $\frac{1}{20}$. Raising m_c by $\frac{1}{10}$ is rejected 38/40 times; in the other two cases $c^{(1)}$ still satisfies the objective bound with the larger cap, so the modified record is still a valid proof. The pair $(-m_c,\, 1 + m_c^3)$ satisfies the φ inequality $(p^* + m^3)^2 \geq (1 - m^2)^3$, $p^* + m^3 \geq 0$ for $m = -m_c$; the check rejects it in 40/40 cases because it also requires $0 < m_c \leq 1$ and $p^* < 0$. On 60 lp

boxes, lowering c_0 by $10^{-3}|c_0|$, lowering c_6 by $10^{-1}|c_6|$, or widening the r-interval by $\frac{1}{10}$ is rejected 60/60 times; on 60 near-circle boxes, widening the r-interval by $\frac{1}{10}$ is rejected 60/60 times; on 40 one-coordinate cells, lowering c_0 by $10^{-3}|c_0|$ is rejected 40/40 times. The claim of Lemma 2.6 fails at $q_3 - 10^{-3}$ (for OR_3) and at $q_0 + 10^{-3}$ (for a dictator).

Two corruptions are *not* detected, as expected. Shifting an ms box by $+\frac{1}{20}$ in u (beyond u_3) passes part F (it is rejected by part D in 40/40 cases), and moving a near-circle box to $u \le \frac{3}{2} < u_0$ passes part E in 29/60 cases. The piece test (A3) and the near-circle test (A) only bound the error term; the main term is bounded by Lemma 2.6 (valid only for $q \ge q_3$) and by Lemma 2.5 (valid only for $q \le q_0$). This is why Lemma 2.21(A) is stated only for $u \ge u_0$ and Lemma 2.24 only for $u \in [u_0, u_3]$, and why the theorem stops at u_0 and u_3.

2.9.4 Reproducing

```
pip install numpy scipy sympy mpmath
cd scripts
python3 verify_k2.py          # parts A-G, about 5 minutes on 8 cores
python3 break_tests_k2.py     # negative tests, about 15 seconds
# regeneration of one slab, e.g. the last one (m-split near u3):
python3 cover2c.py 421/200 1054691/500000 1 \
        ../outputs/cover2c/b10b_p.json 1 8 11 18 ms
```

2.10 Proof of Theorem 2.1

(a) By Lemma 2.3 let $q \in [q_3, q_0]$, i.e. $u \in [u_0, u_3] \subset [U_-, U_+]$. Reduce α as in Section 2.2.3.

(1) $a_1 = 1$: $\alpha = e_1$ and $\mathbb{E}|L| = 2\tau \le T$ (Lemma 2.4), with equality iff $q = q_0$.

(2) $a_1 \le \frac{9}{20}$: (u, a_1) lies in a cell, and Lemma 2.14 gives $\mathbb{E}|L| < T$.

(3) $a_1 > \frac{9}{20}$ and $r = 1$: $L = a_1\chi_1 + sa_2\chi_2$, and Lemma 2.5 gives $\mathbb{E}|L| \le T$, with equality iff $s = 1$ and $a_1 = a_2$, or $q = q_0$ and $a_2 = 0$.

(4) $a_1 > \frac{9}{20}$ and $r < 1$: (u, t, r) lies in a box of the cover for the sign s (part B), and the box is not small, because $a_1 > \frac{9}{20}$. If it is lp, Lemma 2.19 with $m^* = \min(1, \bar{m}(B)) \ge m$ gives $\mathbb{E}|L| < T$. If it is ncA or ncB, Lemma 2.21 gives $\mathbb{E}|L| < T$ (here $u \ge u_0$). If it is ms, Lemma 2.24 gives $\mathbb{E}|L| \le T$ (here $u \le u_3$).

So $\mathbb{E}|L| \le T$ always, and $(e_1 + e_2)/\sqrt{2}$ attains T (Lemma 2.4). Hence $R(q) = T(q)$. For $q \in [1 - q_0, 1 - q_3]$ use Lemma 2.3: $R(q) = R(1 - q) = 2\sqrt{2}\, q\, \tau$.

(b) Equality can occur only in cases (1), (3) and the ms case of (4). Case (1) gives $\alpha = \pm e_j$ at $q = q_0$. Case (3) gives $\alpha = \pm(e_i + e_j)/\sqrt{2}$, or $\alpha = \pm e_j$ at $q = q_0$. In the ms case, Lemma 2.24 gives $\alpha = a_1 e_1 + sa_2 e_2 + be_{i_0}$ (after the reduction) with $G_3(a_1, sa_2, b) = T$ and $a_1, b > 0$, $a_2 \ge |\alpha_{i_0}| = b > 0$. By Lemma 2.6, (a_1, sa_2, b) is a positive multiple of $\pm(e_i + e_j)$, of $\pm e_i$ or of $\pm(1, 1, 1)$. Only the last has three nonzero entries, so $q = q_3$, $s = 1$ and $a_1 = a_2 = b$, i.e. $\alpha = (e_1 + e_2 + e_{i_0})/\sqrt{3}$. Undoing the reduction (global sign and permutation) gives the list in (b). Conversely, each listed vector attains T at the stated q (Lemma 2.4). For $q \ge \frac{1}{2}$ use Lemma 2.3.

(c) For $q < q_3 < \frac{1}{3}$, Lemma 2.4 with $k = 3$ gives $R(q) \ge 2\sqrt{3}(1 - q)^2\tau > T$. For $q \in (q_0, \frac{1}{2}]$, $R(q) \ge \mathbb{E}|\chi_1| = 2\tau > T$. Together with (a) this gives $\{q \le \frac{1}{2} : R(q) = T(q)\} = [q_3, q_0]$. □

2.11 Remarks

1. **Why two coordinates.** In the one-coordinate split of `MAIN_RESULT` the $k = 2$ extremiser is an interior point of the parameter region where the target is attained by $M = \chi_2$. In the two-coordinate split it is the boundary point $b = 0$, where Lemma 2.21(A) has slack $T(1 - r) = Tb^2/(1 + r)$ against an error of order b^4.

2. **The triple point.** At u_3 the vector $(e_1 + e_2 + e_3)/\sqrt{3}$ ties. In the two-coordinate split it is an interior point with $m = 1$, $p_3 = 1$, where the six-moment relaxation is exact. The m-split removes it: $m \le m_c$ excludes it; a negative largest coefficient forces $p_3 \le \varphi(m_c) < 0$; and a positive one is the boundary point $b' = 0$ of a three-coordinate split, where Lemma 2.22 again has slack of order b'^2 against an error of order b'^4, thanks to the exact three-bit lemma. Numerically, near the triple point the capped certificate has margin about 0.015 for $m_c = 0.8$, the sign-constrained one about 0.03, and the (A3) ratio is about 0.8–0.9.

3. **Beyond q_3.** For $q < q_3$ the extremiser should be $(e_1 + e_2 + e_3)/\sqrt{3}$ up to $q_4 = 1 - \sqrt{3/4}$ (RQ-C, numerical, and proved for $n \le 7$). The present method would need a three-coordinate split. It also needs more than six moments for small coefficients: the six-moment Gaussian value 0.888074 exceeds $2\sqrt{3}(1 - q_4)^2\tau(q_4) \approx 0.8854$.

4. **Relation to RQ-C's C11.** RQ-C proved $R(q) = T(q)$ on $[\frac{256}{985}, q_0]$ by a different method (audited VALID as A.9). Theorem 2.1 extends this to the whole interval $[q_3, q_0]$, which is the largest possible by part (c).

5. **Status.** Rated VALID by RQ-AUD (A.11, 2026-10-22 08:52 UTC) with no mathematical fix; the two cosmetic points of that report are applied in this version (Lemma 2.20 for $y = 0$, Definition 2.23). Refereed VALID by RQ-REF1 (2026-10-22 15:38 UTC), with no fixes; after that report only this item was changed. The computer steps have been run twice (generator and independent verifier), the verifier rejects corrupted data (negative tests above), and the referee re-did every computer step with its own exact programs.

Chapter 3

The $k = 3$ regime of $R(q)$: $R(q) = 2\sqrt{3}\,(1-q)^2\sqrt{q(1-q)}$ for $\frac{25}{169} \le q \le 1 - \sqrt{2/3}$

Source: RQ-A, `MAIN_RESULT_K3.tex` (md5 `00720a0c083de2020282ed4635e00c0c`), by "RQ-A (R(q) attack)", dated 22 October 2026. Its main result is Theorem 3 (claim MAIN-3), which keeps this name.

Refereed version: md5 `9f20afc71aadef43fc877694bca3755c`, the file in commit `6ecd564`. The source differs from it only in the status item of the closing remarks, which now records the audit and referee verdicts.

Audit: A.14, VALID and NEW, no fix (22 October, 10:37 UTC).

Referee: RQ-REF1, VALID, no fixes (report `REFEREE.md`, md5 `369c1cfb...`, mirrored at 15:38 UTC on 22 October).

Use in the Main Theorem: Step 1, through Corollary 5.2.

Transcription: the whole paper, with the mechanical changes of Appendix C: labels prefixed by `ch03:`, numbers n become $3.n$, the title becomes the chapter title, no table of contents, the abstract as a quoted block. No editorial footnotes.

Abstract of the source paper. For $q \in (0,1)$ let $\chi_1, \chi_2, \dots$ be i.i.d. normalised q-biased bits and let $R(q)$ be the supremum of $\mathbb{E}|\sum \alpha_i \chi_i|$ over unit vectors α. We prove that $R(q) = 2\sqrt{3}\,(1-q)^2\sqrt{q(1-q)}$, the value of $(e_1+e_2+e_3)/\sqrt{3}$, for every $q \in [\frac{25}{169}, 1-\sqrt{2/3}] \approx [0.1479, 0.1835]$ (and the mirror statement on $[1-\sqrt{2/3}, \frac{144}{169}]$), and we determine all extremisers. These are the first exact values of $R(q)$ in the regime where three equal coefficients are optimal. The upper end is sharp: above $q_3 = 1-\sqrt{2/3}$ the vector $(e_1+e_2)/\sqrt{2}$ is better. The conjectured lower end is $q_4 = 1-\sqrt{3}/2 \approx 0.1340$, below which $(e_1+\cdots+e_4)/2$ is better. Together with our Theorems 1 and 2 (`MAIN_RESULT`, `MAIN_RESULT_K2`), this gives $R(q) = 2\sqrt{q(1-q)}\max\{1, \sqrt{2}\,\hat{q}, \sqrt{3}\,\hat{q}^2\}$, $\hat{q} = \max(q, 1-q)$, for all $q \in [\frac{25}{169}, \frac{144}{169}]$. The proof uses the method of Theorem 2 with a new target. We split off the two largest coefficients and bound the conditional expectation by degree-six polynomials, whose expectations depend only on six moments of the remainder. A fourth-moment tail bound handles the neighbourhood of $(e_1+e_2)/\sqrt{2}$. The extremiser $(e_1+e_2+e_3)/\sqrt{3}$ is handled by splitting off a third coordinate, using an exact $k=3$ three-bit lemma. The computer-assisted steps (81 975 boxes and 2 704 cells) use exact rational arithmetic and certified interval arithmetic, and all of them were repeated by an independent program.

3.1 Statement

Fix $q \in (0,1)$ and put

$$u = \sqrt{\tfrac{1-q}{q}}, \qquad v = \frac{1}{u}, \qquad \tau = \sqrt{q(1-q)}.$$

Let $\chi, \chi_1, \chi_2, \dots$ be i.i.d. with $\Pr[\chi = u] = q$ and $\Pr[\chi = -v] = 1-q$, so that $\mathbb{E}\chi = 0$, $\mathbb{E}\chi^2 = 1$ and $\mathbb{E}|\chi| = 2\tau$. Let

$$R(q) = \sup_{n \ge 1} \sup_{\alpha \in \mathbb{R}^n \setminus \{0\}} \frac{\mathbb{E}|\sum_{i=1}^n \alpha_i \chi_i|}{|\alpha|_2}.$$

Put

$$q_3 = 1 - \sqrt{2/3} \approx 0.183503, \qquad q_4 = 1 - \tfrac{\sqrt{3}}{2} \approx 0.133975, \qquad q_L = \tfrac{25}{169} \approx 0.147929,$$

$$T(q) = 2\sqrt{3}\,(1-q)^2\,\tau, \qquad T_2(q) = 2\sqrt{2}\,(1-q)\,\tau.$$

Theorem 3. *(a) For every $q \in [q_L, q_3]$, every $n \ge 1$ and every $\alpha \in \mathbb{R}^n$ with $|\alpha|_2 = 1$,*

$$\mathbb{E}\Big|\sum_{i=1}^n \alpha_i \chi_i\Big| \le 2\sqrt{3}\,(1-q)^2 \sqrt{q(1-q)}.$$

For $q \in [1-q_3, 1-q_L]$ the same holds with $1-q$ replaced by q. Consequently $R(q) = 2\sqrt{3}\max(q,1-q)^2\sqrt{q(1-q)}$ for $q \in [q_L, q_3] \cup [1-q_3, 1-q_L]$.

(b) (Extremisers.) Let $q \in [q_L, q_3] \cup [1-q_3, 1-q_L]$. Equality in (a) holds if and only if $\alpha = \pm\frac{1}{\sqrt{3}}(e_i + e_j + e_k)$ with i, j, k distinct, or $q \in \{q_3, 1-q_3\}$ and $\alpha = \pm\frac{1}{\sqrt{2}}(e_i + e_j)$ with $i \ne j$.

(c) (Sharpness.) For $q \in (q_3, \frac{1}{2}]$, $R(q) \ge T_2(q) > T(q)$. For $q \in (0, q_4)$, $R(q) \ge 4(1-q)^3\tau > T(q)$. Hence $[q_L, q_3] \subseteq \{q \in (0, \frac{1}{2}] : R(q) = T(q)\} \subseteq [q_4, q_3]$.

Corollary 3.1. *With Theorem 1 of `MAIN_RESULT` ($R(q) = 2\tau$ on $[q_0, 1-q_0]$, $q_0 = 1 - 1/\sqrt{2}$) and Theorem 2 (the main theorem of `MAIN_RESULT_K2`: $R(q) = T_2(q)$ on $[q_3, q_0]$, mirrored on $[1-q_0, 1-q_3]$):*

$$R(q) = 2\sqrt{q(1-q)}\,\max\{1,\ \sqrt{2}\,\hat{q},\ \sqrt{3}\,\hat{q}^{\,2}\}, \qquad \hat{q} = \max(q, 1-q), \qquad \text{for all } q \in [\tfrac{25}{169}, \tfrac{144}{169}].$$

Proof. For $q \le \frac{1}{2}$, $\hat{q} = 1-q$, and $\max\{1, \sqrt{2}(1-q), \sqrt{3}(1-q)^2\}$ equals $\sqrt{3}(1-q)^2$ on $[q_L, q_3]$, $\sqrt{2}(1-q)$ on $[q_3, q_0]$ and 1 on $[q_0, \frac{1}{2}]$: indeed $\sqrt{3}(1-q)^2 \ge \sqrt{2}(1-q)$ iff $1-q \ge \sqrt{2/3}$, $\sqrt{2}(1-q) \ge 1$ iff $1-q \ge 1/\sqrt{2}$, and $\sqrt{3}(1-q)^2 \ge 1$ for $q \le q_3$. For $q \ge \frac{1}{2}$ use Lemma 3.2. □

Part (c) and the lower bound $R \ge T$ in (a) are elementary (Lemma 3.3). The content is the upper bound in (a), and (b).

Relation to Theorem 2. Theorem 2 is the main theorem of `MAIN_RESULT_K2` (labelled Theorem 1 there). The proof of Theorem 3 follows `MAIN_RESULT_K2` step by step. Sections 3.4, 3.6 and the generic parts of Sections 3.7–3.8 are unchanged. The changes are: the target T and its lower bound (3.2); the range $u \in [u_3, \frac{12}{5}]$; the threshold $A_S = \frac{2}{5}$; the target Θ_1 of the one-coordinate route; the $k = 3$ three-bit lemma (Lemma 3.5), used in the m-split; and the main-term bounds in Lemmas 3.4 and 3.20(A), which now use $T_2 \le T$ for $q \le q_3$. We give the full proof so that the document can be read on its own.

Conventions. $x_+ = \max(x,0)$. All polynomials in the computer-assisted parts have rational coefficients. "Verified" means verified in exact rational arithmetic or in outward-rounded interval arithmetic, as specified in Section 3.9. For a rational $x \ge 0$ we write $\lfloor\sqrt{x}\rfloor_{15} = \lfloor 10^{15}\sqrt{x}\rfloor/10^{15}$ and $\lceil\sqrt{x}\rceil_{15} = (\lfloor 10^{15}\sqrt{x}\rfloor + 1)/10^{15}$ (integer square roots).

3.2 Reductions

3.2.1 Symmetry and parametrisation

Lemma 3.2. *The law of $-\chi^{(q)}$ is the law of $\chi^{(1-q)}$. Hence $\mathbb{E}|\sum \alpha_i\chi_i^{(q)}| = \mathbb{E}|\sum \alpha_i\chi_i^{(1-q)}|$, $R(q) = R(1-q)$, and the extremisers for q and $1-q$ coincide.*

Proof. $-\chi^{(q)}$ takes the value $-u_q$ with probability q and v_q with probability $1-q$; since $u_{1-q} = v_q$ and $v_{1-q} = u_q$, this is the law of $\chi^{(1-q)}$. Finally $|\sum \alpha_i(-\chi_i)| = |\sum \alpha_i\chi_i|$. □

From now on $q \le \frac{1}{2}$, i.e. $u \ge 1$, and

$$q = \frac{1}{1+u^2}, \quad 1-q = \frac{u^2}{1+u^2}, \quad v = \frac{1}{u}, \quad \tau = \frac{u}{1+u^2}, \quad qu = (1-q)v = \tau. \tag{3.1}$$

On $u \ge 1$, τ and q are decreasing and $1-q$ is increasing in u. The target is

$$T = 2\sqrt{3}(1-q)^2\tau = \sqrt{3}\,\tilde{T}(u), \qquad \tilde{T}(u) = \frac{2u^5}{(1+u^2)^3}, \qquad \frac{d}{du}\frac{u^5}{(1+u^2)^3} = \frac{u^4(5-u^2)}{(1+u^2)^4},$$

so $\tilde{T}$ is increasing on $[1,\sqrt{5}]$ and decreasing on $[\sqrt{5},\infty)$. In particular, for $1 \le u_1 < u_2$ and $u \in [u_1,u_2]$,

$$T(u) \;\ge\; T^-(u_1,u_2) := S_3 \min\{\tilde{T}(u_1),\tilde{T}(u_2)\}, \qquad S_3 = \lfloor\sqrt{3}\rfloor_{15} < \sqrt{3}. \tag{3.2}$$

The range $q \in [q_L, q_3]$ corresponds to $u \in [u_3, \frac{12}{5}]$ with

$$u_3 = \sqrt{2+\sqrt{6}} \approx 2.1093814,$$

because $(1-q_3)/q_3 = \sqrt{2}/(\sqrt{3}-\sqrt{2}) = 2+\sqrt{6}$ and $1/(1+(12/5)^2) = \frac{25}{169}$. We fix the rationals

$$U_- = \frac{2109381}{1000000} < u_3, \qquad U_+ = \frac{12}{5} < u_4 := \sqrt{3+2\sqrt{3}} \approx 2.5425,$$

(indeed $U_-^2 > 2$ with $(U_-^2-2)^2 < 6$, and $U_+^2 = 5.76 < 3+2\sqrt{3}$; u_4 corresponds to q_4). The computations cover $u \in [U_-, U_+]$; the theorem uses only $u \in [u_3, U_+]$.

3.2.2 Values of a few vectors

Lemma 3.3. *Let $k \ge 1$ and $q < 1/k$. Then $\mathbb{E}|\chi_1+\cdots+\chi_k|/\sqrt{k} = 2\sqrt{k}\,(1-q)^{k-1}\tau$. In particular $\mathbb{E}|\chi_1| = 2\tau$, $\mathbb{E}|\chi_1+\chi_2|/\sqrt{2} = T_2$ (for $q < \frac{1}{2}$; also at $q = \frac{1}{2}$ by continuity), $\mathbb{E}|\chi_1+\chi_2+\chi_3|/\sqrt{3} = T$ for $q < \frac{1}{3}$, and $\mathbb{E}|\chi_1+\cdots+\chi_4|/2 = 4(1-q)^3\tau$ for $q < \frac{1}{4}$. Moreover:*

(i) for $q \le \frac{1}{2}$: $T_2 \le T$ iff $q \le q_3$, with equality iff $q = q_3$;

(ii) for $q \le q_3$: $2\tau < T$;

(iii) for $q < \frac{1}{4}$: $4(1-q)^3\tau > T$ iff $q < q_4$.

Proof. Let $S = \chi_1 + \cdots + \chi_k$ and let $x_i = \mathbf{1}\{\chi_i = u\}$. If some $x_i = 1$ then $S \geq u - (k-1)v > 0$, because $u^2 > k-1$ is equivalent to $q < 1/k$. If all $x_i = 0$ then $S = -kv < 0$. So $|S| = fS$ with $f = 2 \cdot \mathbf{1}\{\exists i : x_i = 1\} - 1 = 1 - 2 \cdot \mathbf{1}\{\text{all } x_i = 0\}$. Since $\mathbb{E}\chi_i = 0$, $\mathbb{E}[f\chi_i] = -2\mathbb{E}[\chi_i \mathbf{1}\{\text{all } x = 0\}] = -2(1-q)^k(-v) = 2(1-q)^{k-1}(1-q)v = 2(1-q)^{k-1}\tau$. Summing over i gives $\mathbb{E}|S| = 2k(1-q)^{k-1}\tau$. The comparisons: (i) $2\sqrt{2}(1-q)\tau \leq 2\sqrt{3}(1-q)^2\tau$ iff $1 - q \geq \sqrt{2/3}$; (ii) for $q \leq q_3$, $\sqrt{3}(1-q)^2 \geq \sqrt{3} \cdot \frac{2}{3} = \frac{2}{\sqrt{3}} > 1$; (iii) $4(1-q)^3 > 2\sqrt{3}(1-q)^2$ iff $1 - q > \frac{\sqrt{3}}{2}$. □

3.2.3 Splitting off the two largest coefficients

Let $|\alpha|_2 = 1$ and $L = \sum \alpha_i \chi_i$. Changing the sign of α and permuting coordinates does not change $\mathbb{E}|L|$. So we may assume

$$a_1 := \alpha_1 = \max_i |\alpha_i| > 0, \qquad a_2 := |\alpha_2| = \max_{i \geq 2} |\alpha_i|, \qquad |\alpha_3| \geq |\alpha_4| \geq \cdots,$$

and we put $s = \operatorname{sgn} \alpha_2 \in \{1, -1\}$ ($s = 1$ if $\alpha_2 = 0$),

$$r = \sqrt{a_1^2 + a_2^2} \in (0, 1], \qquad b = \sqrt{1 - r^2}.$$

If $r < 1$, let $\beta_i = \alpha_i / b$ for $i \geq 3$ and $M = \sum_{i \geq 3} \beta_i \chi_i$. Then

$$L = a_1\chi_1 + s\, a_2\chi_2 + bM, \qquad \sum_{i \geq 3} \beta_i^2 = 1, \qquad m := \max_{i \geq 3} |\beta_i| = \frac{|\alpha_3|}{b} \leq \min\Big(1, \frac{a_2}{b}\Big),$$

and M is independent of (χ_1, χ_2). We use half-angle coordinates for (a_1, a_2):

$$a_1 = r\, c(t), \quad a_2 = r\, d(t), \qquad c(t) = \frac{1 - t^2}{1 + t^2}, \quad d(t) = \frac{2t}{1 + t^2}, \qquad t = \frac{a_2}{r + a_1}.$$

Since $0 \leq a_2 \leq a_1$, the angle θ with $\tan\theta = a_2/a_1$ is in $[0, \pi/4]$ and $t = \tan(\theta/2) \in [0, \sqrt{2} - 1]$. We fix $T_8 = \frac{20711}{50000} = 0.41422 \geq \sqrt{2} - 1$ (indeed $(T_8 + 1)^2 \geq 2$). On $[0, 1]$, c is decreasing and d is increasing in t, and $c^2 + d^2 = 1$. Thus every unit α gives a point

$$(u, t, r, s) \in [U_-, U_+] \times [0, T_8] \times (0, 1] \times \{1, -1\} \qquad (u \in [u_3, U_+]).$$

We put $A_S = \frac{2}{5}$. If $a_1 \leq A_S$ we use the one-coordinate route of Section 3.5; otherwise $r \geq a_1 > A_S$ and we use the two-coordinate route of Sections 3.6–3.8.

3.3 Exact evaluations

3.3.1 Two coordinates

Lemma 3.4 (two-coordinate value)**.** *Let $q \leq \frac{1}{2}$, $c, d \geq 0$, $s \in \{1, -1\}$, and $X = c\chi_1 + s\, d\chi_2$. List the atoms of X as $(\chi_1, \chi_2) = (u, u), (u, -v), (-v, u), (-v, -v)$, with probabilities $p = (q^2,\ q(1-q),\ q(1-q),\ (1-q)^2)$ and values x_j. Then $p_j x_j = \tau g_j$ with*

$$g = \big(q(c + sd),\ (1-q)c - s\, q\, d,\ -q\, c + s(1-q)d,\ -(1-q)(c + sd)\big), \tag{3.3}$$

and

$$\mathbb{E}|X| = 2\tau \max\{c,\ d,\ [s = 1]\,(1-q)(c + d)\}$$

(the last entry is present only for $s = 1$). If $q \leq q_0 = 1 - 1/\sqrt{2}$, then $\mathbb{E}|X| \leq T_2\sqrt{c^2 + d^2}$. If $q \leq q_3$, then $\mathbb{E}|X| \leq T\sqrt{c^2 + d^2}$, and for $(c, d) \neq 0$ equality holds if and only if $q = q_3$, $s = 1$ and $c = d$.

Proof. The identities $p_j x_j = \tau g_j$ follow from (3.1); for example $q(1-q)(cu - sdv) = (1-q)\tau c - q\tau sd$. Since $\mathbb{E}X = 0$, $\mathbb{E}|X| = 2\mathbb{E}X_+ = 2\tau\sum_j (g_j)_+$. For $s = 1$: $g_1 \geq 0 \geq g_4$, so $\mathbb{E}X_+/\tau = q(c+d) + ((1-q)c - qd)_+ + ((1-q)d - qc)_+$. If both middle terms are nonnegative this equals $(1-q)(c+d)$, and then $(1-q)(c+d) - c = (1-q)d - qc \geq 0$ and similarly $\geq d$. If only the first is nonnegative it equals $q(c+d) + (1-q)c - qd = c$, and $(1-q)(c+d) - c = (1-q)d - qc < 0$, while $c \geq d$ (otherwise $(1-q)d - qc \geq (1-2q)c \geq 0$). The case where only the second is nonnegative is symmetric. Both negative would give $(1-q)(c+d) < q(c+d)$, impossible for $q \leq \frac{1}{2}$ unless $c = d = 0$. In all cases $\mathbb{E}X_+/\tau = \max\{c, d, (1-q)(c+d)\}$. For $s = -1$: $g_2 \geq 0 \geq g_3$. If $c \geq d$ then $g_1 \geq 0 \geq g_4$ and $\mathbb{E}X_+/\tau = q(c-d) + (1-q)c + qd = c$. If $c < d$ then $g_1 < 0 < g_4$ and $\mathbb{E}X_+/\tau = (1-q)c + qd + (1-q)(d-c) = d$. So $\mathbb{E}X_+/\tau = \max(c, d)$.

For the bounds let $\rho = \sqrt{c^2 + d^2} > 0$. Then $\max(c, d) \leq \rho$, and $2\tau\rho \leq T_2\rho$ iff $\sqrt{2}(1-q) \geq 1$ iff $q \leq q_0$. Also $(1-q)(c+d) \leq \sqrt{2}(1-q)\rho$ with equality iff $c = d$. This gives $\mathbb{E}|X| \leq T_2\rho$ for $q \leq q_0$. Now let $q \leq q_3$ ($< q_0$). Then $2\tau\max(c, d) \leq 2\tau\rho < T\rho$ by Lemma 3.3(ii), and $2\tau(1-q)(c+d) \leq T_2\rho \leq T\rho$ by Lemma 3.3(i), with equality iff $c = d$ and $q = q_3$. Since the third entry is present only for $s = 1$, this gives the claim. □

3.3.2 Three coordinates

For $f : \{0,1\}^3 \to [-1, 1]$ and $x_i = \mathbf{1}\{\chi_i = u\}$ put $\Delta_i(f) = \mathbb{E}[f \mid x_i = 1] - \mathbb{E}[f \mid x_i = 0]$, a polynomial in q. Then, by (3.1),

$$\mathbb{E}[f\chi_i] = qu\,\mathbb{E}[f \mid x_i = 1] - (1-q)v\,\mathbb{E}[f \mid x_i = 0] = \tau\,\Delta_i(f). \tag{3.4}$$

Lemma 3.5 (three-bit lemma, $k = 3$)**.** *Let $q \in [q_L, q_3]$ and $c \in \mathbb{R}^3$. Then*

$$G_3(c) := \mathbb{E}|c_1\chi_1 + c_2\chi_2 + c_3\chi_3| \leq T\,|c|.$$

For $c \neq 0$ equality holds if and only if c is a positive multiple of $\pm(e_1 + e_2 + e_3)$, or $q = q_3$ and c is a positive multiple of $\pm(e_i + e_j)$ for some $i \neq j$.

Proof. Let $X = c \cdot \chi$ and $f^* = \operatorname{sgn} X$ (with $\operatorname{sgn} 0 = 1$), a function of (x_1, x_2, x_3) with values ± 1. By (3.4) and Cauchy–Schwarz,

$$G_3(c) = \mathbb{E}[f^* X] = \tau \sum_i c_i \Delta_i(f^*) \leq \tau|c|\,|\Delta(f^*)|.$$

Claim: for each of the $2^8 = 256$ functions $f : \{0,1\}^3 \to \{-1, 1\}$, the polynomial $P_f(q) = 12(1-q)^4 - \sum_{i=1}^3 \Delta_i(f)^2$ is ≥ 0 on $[q_L, q_3]$. Moreover $P_f \equiv 0$ exactly for $f = \pm(2 \cdot \mathbf{1}\{x_1 \vee x_2 \vee x_3\} - 1)$ (two functions); $P_f(q_3) = 0 \neq P_f$ exactly for $f = \pm(2 \cdot \mathbf{1}\{x_i \vee x_j\} - 1)$ (six functions); and no $P_f \not\equiv 0$ has a zero in $[q_L, q_3)$. Given the claim, $G_3(c) \leq \tau|c|\sqrt{12}(1-q)^2 = T|c|$.

The claim is a finite exact computation (Section 3.9, part G). For each f, P_f is computed symbolically as a polynomial with rational coefficients (degree ≤ 4). Let $\mu_3(q) = 3q^2 - 6q + 1$, the minimal polynomial of q_3 (irreducible over $\mathbb{Q}$, since 24 is not a square). Its other root $1 + \sqrt{2/3}$ lies above 1, so $\mu_3 > 0$ on $[0, q_3)$. Take a rational enclosure $q_3 \in [q_3^-, q_3^+]$ of width 10^{-15}; the signs $\mu_3(q_3^-) > 0 > \mu_3(q_3^+)$ and $q_L < q_3^-$ are asserted. Then: (i) by Sturm sequences, P_f has no root in $[q_L, q_3^-]$, and $P_f(q_L) > 0$; (ii) near q_3: if $\mu_3 \mid P_f$, write $P_f = \mu_3 Q$; then Q has no root in $[q_3^-, q_3^+]$ and $Q(q_3^-) > 0$, so $P_f > 0$ on $[q_3^-, q_3)$ and $P_f(q_3) = 0$; otherwise P_f has no root in $[q_3^-, q_3^+]$ and $P_f(q_3^-) > 0$. Since μ_3 is irreducible, $P_f(q_3) = 0$ iff $\mu_3 \mid P_f$. The two functions with $P_f \equiv 0$ are $\pm\mathrm{OR}_3$, by the computation in Lemma 3.3 ($\Delta(\mathrm{OR}_3) = 2(1-q)^2(e_1 + e_2 + e_3)$); and $\Delta(\mathrm{OR}_{ij}) = 2(1-q)(e_i + e_j)$ gives $P = 12(1-q)^4 - 8(1-q)^2 = 4(1-q)^2\mu_3(q)$ for the OR of two bits.

Equality. Suppose $G_3(c) = T|c|$ with $c \neq 0$. Then $|\Delta(f^*)|^2 = 12(1-q)^4$, so $P_{f^*}(q) = 0$, and c is a positive multiple of $\Delta(f^*)$. By the claim, $f^* = \pm\mathrm{OR}_3$, with $\Delta = \pm 2(1-q)^2(1,1,1)$; or $q = q_3$ and f^* is $\pm$ the OR of two bits, with $\Delta = \pm 2(1-q)(e_i + e_j)$. Conversely, these c attain $T|c|$ by Lemmas 3.3 and 3.4 (at $q = q_3$, $T_2 = T$). □

Remark 3.6. Lemma 3.5 is contained in the case $n = 3$ of RQ-C's result C6: for $n \leq 7$ and all $q \in (0,1)$, $R_n(q) = 2\tau\sqrt{\max_{k\leq n} k(1-\bar{q})^{2k-2}}$ with $\bar{q} = \min(q, 1-q)$, with only OR_k extremal. RQ-AUD audited C6 VALID (A.5 for $n \leq 6$, A.5b for $n = 7$). Our check is independent of it. Unlike the $k = 2$ lemma of Theorem 2, the $k = 3$ claim has no lower end of validity coming from three bits (the OR of four bits needs a fourth coordinate). The range of Theorem 3 is limited by the rest of the argument, not by Lemma 3.5.

3.4 Moments of the remainder

Lemma 3.7. *The cumulants of χ are $\kappa_1 = 0$, $\kappa_2 = 1$, and, with $w = u^2+v^2$, $\kappa_3 = u-v$, $\kappa_4 = w-4$, $\kappa_5 = (u-v)(w-10)$, $\kappa_6 = w^2 - 26w + 64$.*

Proof. By (3.1), $m_k = \mathbb{E}\chi^k = (u^k + (-1)^k u^{2-k})/(1+u^2)$, which gives $m_3 = u - v$, $m_4 = w - 1$, $m_5 = (u-v)w$ and $m_6 = w^2 - w - 1$. (Use $u^4 - 1 = (u^2+1)(u^2-1)$, $u^6+1 = (u^2+1)(u^4-u^2+1)$, $u^8-1 = (u^2+1)(u^2-1)(u^4+1)$ and $u^{10}+1 = (u^2+1)(u^8-u^6+u^4-u^2+1)$.) For a centred variable with unit variance, $\kappa_3 = m_3$, $\kappa_4 = m_4 - 3$, $\kappa_5 = m_5 - 10m_3$ and $\kappa_6 = m_6 - 15m_4 - 10m_3^2 + 30$. Using $(u-v)^2 = w - 2$ gives the formulas. (Verified symbolically in `verify_all.py`, part A1.) □

Lemma 3.8. *Let $M = \sum \beta_i \chi_i$ (finite sum) with $\sum \beta_i^2 = 1$ and power sums $p_j = \sum_i \beta_i^j$. Then $\mathbb{E}M = 0$, $\mathbb{E}M^2 = 1$, and*

$$\mathbb{E}M^3 = \kappa_3 p_3, \quad \mathbb{E}M^4 = 3 + \kappa_4 p_4, \quad \mathbb{E}M^5 = \kappa_5 p_5 + 10\kappa_3 p_3, \quad \mathbb{E}M^6 = 15 + 15\kappa_4 p_4 + 10\kappa_3^2 p_3^2 + \kappa_6 p_6.$$

Proof. Cumulants of independent sums add and are homogeneous, so M has cumulants $K_1 = 0$, $K_2 = 1$ and $K_j = \kappa_j p_j$. For a centred variable, $m_3 = K_3$, $m_4 = K_4 + 3K_2^2$, $m_5 = K_5 + 10K_3K_2$ and $m_6 = K_6 + 15K_4K_2 + 10K_3^2 + 15K_2^3$. □

Lemma 3.9. *If $\sum \beta_i^2 = 1$ and $\max|\beta_i| \leq m \leq 1$, then $p_3^2 \leq p_4 \leq m^2$, $p_4^2 \leq p_6 \leq m^2 p_4$, $|p_5| \leq m p_4$ and $0 \leq p_4 \leq 1$.*

Proof. Cauchy–Schwarz gives $p_3^2 = (\sum \beta_i \beta_i^2)^2 \leq \sum \beta_i^2 \sum \beta_i^4 = p_4$ and $p_4^2 = (\sum \beta_i \beta_i^3)^2 \leq p_2 p_6 = p_6$. Also $p_4 \leq m^2 \sum \beta_i^2 = m^2$, $p_6 \leq m^2 p_4$ and $|p_5| \leq \sum |\beta_i| \beta_i^4 \leq m p_4$. □

Lemma 3.10 (sign information)**.** *Let $\sum \beta_i^2 = 1$, $m = \max|\beta_i|$, and suppose $\beta_{i_0} = -m$ for some i_0. If $m \geq m_c \in (0,1]$, then $p_3 \leq \varphi(m_c) := -m_c^3 + (1-m_c^2)^{3/2}$.*

Proof. For $i \neq i_0$, $|\beta_i| \leq (\sum_{i\neq i_0} \beta_i^2)^{1/2} = \sqrt{1-m^2}$. Hence $p_3 = -m^3 + \sum_{i\neq i_0} \beta_i^3 \leq -m^3 + \sqrt{1-m^2} \sum_{i\neq i_0} \beta_i^2 = -m^3 + (1-m^2)^{3/2}$. Finally $\frac{d}{dm}\big(-m^3 + (1-m^2)^{3/2}\big) = -3m^2 - 3m\sqrt{1-m^2} \leq 0$. □

Cumulant enclosures. For $1 \leq u_1 \leq u \leq u_2$: $\kappa_3 = u - 1/u$ and $w = u^2 + u^{-2}$ are increasing, so $\kappa_3 \in [k_3^-, k_3^+] = [u_1 - \frac{1}{u_1}, u_2 - \frac{1}{u_2}]$ and $w \in [w^-, w^+]$. We require $w^+ < 13$ (here $w^+ < 6$). Then $\kappa_4 \in [w^- - 4, w^+ - 4]$, $\kappa_6 \in [f_6(w^+), f_6(w^-)]$ with $f_6(x) = x^2 - 26x + 64$ (decreasing for $x < 13$), and $|\kappa_5| \leq k_5^+ := k_3^+ \max(|w^- - 10|, |w^+ - 10|)$.

Definition 3.11 (objective bound)**.** For $c = (c_0, \dots, c_6)$, an interval $[u_1, u_2]$ with $u_1 > 1$, a number $m^* \in (0, 1]$, an optional number $p^* < 0$, and a target Θ, put

$$A = c_0 + c_2 + 3c_4 + 15c_6, \qquad \bar{B} = k_3^+|c_3 + 10c_5|,$$
$$C^+ = \max_{\kappa_4 \in [w^- - 4, w^+ - 4]} \kappa_4(c_4 + 15c_6), \qquad \bar{D} = k_5^+|c_5|,$$
$$E^+ = \max\{f_6(w^-)c_6, f_6(w^+)c_6\}, \qquad F^+ = \max\{0, 10(k_3^-)^2 c_6, 10(k_3^+)^2 c_6\},$$

$\Gamma = C^+ + \bar{D}m^* + F^+ + \max(E^+, 0)m^{*2}$ and $\varepsilon = \min(E^+, 0)$. If p^* is given and $c_3 + 10c_5 \geq 0$, replace A by $A + k_3^-(c_3 + 10c_5)p^*$ and $\bar{B}$ by 0. We say that c *satisfies the objective bound for* $(u_1, u_2, m^*, p^*, \Theta)$ if $h(\rho) = \Theta - A - \bar{B}\rho - \Gamma\rho^2 - \varepsilon\rho^4 > 0$ for all $\rho \in [0, m^*]$.

Lemma 3.12 (expectation bound)**.** *Suppose c satisfies the objective bound for $(u_1, u_2, m^*, p^*, \Theta)$, and let $P(y) = \sum_k c_k y^k$. Then $\mathbb{E}P(M) < \Theta$ for every $u \in [u_1, u_2]$ and every $M = \sum \beta_i \chi_i$ with $\sum \beta_i^2 = 1$ and $\max|\beta_i| \leq m^*$, and, if p^* is given, $p_3 \leq p^*$.*

Proof. By Lemma 3.8, $\mathbb{E}P(M) = A + \kappa_3(c_3 + 10c_5)p_3 + \kappa_4(c_4 + 15c_6)p_4 + \kappa_5 c_5 p_5 + \kappa_6 c_6 p_6 + 10\kappa_3^2 c_6 p_3^2$, with A the unmodified value. Put $\rho = \sqrt{p_4} \in [0, m^*]$ (Lemma 3.9). Then $\kappa_3(c_3 + 10c_5)p_3 \leq \bar{B}\rho$ since $|p_3| \leq \rho$. If p^* is given and $c_3 + 10c_5 \geq 0$, then instead $\kappa_3(c_3 + 10c_5)p_3 \leq \kappa_3(c_3 + 10c_5)p^* \leq k_3^-(c_3 + 10c_5)p^*$, using $\kappa_3 \geq k_3^- > 0$ and $p^* < 0$. Next, $\kappa_4(c_4 + 15c_6)p_4 \leq C^+\rho^2$ (linear in κ_4, $p_4 \geq 0$); $\kappa_5 c_5 p_5 \leq \bar{D}m^*\rho^2$; $10\kappa_3^2 c_6 p_3^2 \leq F^+\rho^2$; and $\kappa_6 c_6 p_6 \leq E^+ p_6$, which is $\leq E^+ m^{*2}\rho^2$ if $E^+ \geq 0$ and $\leq E^+\rho^4$ if $E^+ < 0$ (Lemma 3.9). Summing, $\mathbb{E}P(M) \leq \Theta - h(\rho) < \Theta$. □

3.5 The one-coordinate route ($a_1 \leq \frac{2}{5}$)

Here we split off only $a = a_1$: $L = a\chi_1 + b_1 M_1$ with $b_1 = \sqrt{1 - a^2}$, $M_1 = \sum_{i \geq 2}(\alpha_i / b_1)\chi_i$, whose coefficients are at most $\min(1, a/b_1)$ in absolute value. By BF3, Lemma 9.4 (Lemma 3 of `MAIN_RESULT`; audited VALID in A.0 and A.3),

$$\mathbb{E}|L| = 2\tau a + 2\mathbb{E}R_a(b_1 M_1), \qquad R_a(y) = \max\{0, (1 - q)(y - av), q(-y - au)\},$$

so $\mathbb{E}|L| < T$ iff $\mathbb{E}R_a(b_1 M_1) < \tau(\sqrt{3}(1 - q)^2 - a)$.

A *cell* is $[u_1, u_2] \times [a_1, a_2]$ with rationals $1 < u_1 < u_2$, $0 \leq a_1 < a_2 \leq \frac{2}{5}$. Put $\bar{b} = \lceil \sqrt{1 - a_1^2} \rceil_{15}$, $\bar{m} = \min\{1, a_2 / \lfloor \sqrt{1 - a_2^2} \rfloor_{15}\}$, and

$$\bar{\ell}_1(y) = \frac{u_2^2}{1 + u_2^2}\Big(\bar{b}y - \frac{a_1}{u_2}\Big), \quad \bar{\ell}_2(y) = \frac{1}{1 + u_1^2}\big(-\bar{b}y - a_1 u_1\big), \quad \Theta_1 = \tau(u_2)\Big(S_3\Big(\frac{u_1^2}{1 + u_1^2}\Big)^2 - a_2\Big).$$

A *cell certificate* is $c \in \mathbb{Q}^7$ with $P(y) = \sum c_k y^k$ such that (V1) $P > 0$, (V2) $P > \bar{\ell}_1$, (V3) $P > \bar{\ell}_2$ on $\mathbb{R}$, and (V4) c satisfies the objective bound for $(u_1, u_2, \bar{m}, -, \Theta_1)$.

Lemma 3.13. *If a cell with $u_1 \geq U_-$ has a certificate, then $\mathbb{E}|L| < T$ for every $u \in [u_1, u_2]$ and every unit α with $a_1 \leq \max|\alpha_i| \leq a_2$.*

Proof. For $u \in [u_1, u_2]$, $a \in [a_1, a_2]$, $b_1 = \sqrt{1 - a^2}$, we have $R_a(b_1 y) \leq \max\{0, \bar{\ell}_1, \bar{\ell}_2\}(y)$. This is Lemma 7 of `MAIN_RESULT`, audited VALID in A.6. We recall the proof: $R_a(b_1 y) = \max\{0, \ell_1, \ell_2\}$ with $\ell_1 = \frac{u^2}{1+u^2}(b_1 y - \frac{a}{u})$ and $\ell_2 = \frac{1}{1+u^2}(-b_1 y - au)$. If $\ell_1(y) > 0$ then $y > 0$ and $0 < b_1 y - \frac{a}{u} \leq \bar{b}y - \frac{a_1}{u_2}$, and $\frac{u^2}{1+u^2} \leq \frac{u_2^2}{1+u_2^2}$. If $\ell_2(y) > 0$ then $y < 0$ and $0 < -b_1 y - au \leq -\bar{b}y - a_1 u_1$, and $\frac{1}{1+u^2} \leq \frac{1}{1+u_1^2}$. So by (V1)–(V3), $\mathbb{E}R_a(b_1 M_1) \leq \mathbb{E}P(M_1)$. Since $a/\sqrt{1 - a^2}$ is increasing, the coefficients of M_1 are at most $\bar{m}$. By Lemma 3.12, $\mathbb{E}P(M_1) < \Theta_1$. Finally $\Theta_1 \leq \tau(u)(\sqrt{3}(1 - q)^2 - a)$, because $\tau(u) \geq \tau(u_2)$, $(1 - q)^2 \geq (\frac{u_1^2}{1+u_1^2})^2$, $S_3 < \sqrt{3}$, $a \leq a_2$, and the bracket is positive: $S_3(\frac{u_1^2}{1+u_1^2})^2 \geq S_3(\frac{U_-^2}{1+U_-^2})^2 > 1.15 > \frac{2}{5} \geq a_2$ (the verifier also asserts $\Theta_1 > 0$ for every cell). □

3.6 The two-coordinate route: box certificates

A *box* is $B = [u_1, u_2] \times [t_1, t_2] \times [r_1, r_2]$ with rationals $1 < u_1 < u_2$, $0 \le t_1 < t_2 \le 1$, $0 \le r_1 < r_2 \le 1$, together with a sign s. For a point of B, $a_1 = rc(t)$, $a_2 = rd(t)$ and $b = \sqrt{1 - r^2}$, as in Section 3.2.3.

Lemma 3.14 (conditional expectation)**.** *For a point of B with $r < 1$, $\mathbb{E}|L| = \mathbb{E}F(M)$, where*

$$F(y) = \sum_{j=1}^{4} p_j |x_j + by| = \sum_{j=1}^{4} \left| p_j x_j + p_j b\, y \right|,$$

x_j and p_j are the atoms and probabilities of $a_1\chi_1 + sa_2\chi_2$, and $p_j x_j = r\tau g_j$ with g as in (3.3) *(with $c = c(t)$, $d = d(t)$).*

Proof. Condition on (χ_1, χ_2) (independent of M), and use Lemma 3.4 for $(a_1, a_2) = r(c, d)$. □

Box enclosures. On B: $q \in [\frac{1}{1+u_2^2}, \frac{1}{1+u_1^2}]$, $1-q \in [\frac{u_1^2}{1+u_1^2}, \frac{u_2^2}{1+u_2^2}]$, $\tau \in [\tau(u_2), \tau(u_1)]$, $c \in [c(t_2), c(t_1)]$, $d \in [d(t_1), d(t_2)]$, $r \in [r_1, r_2]$ and $b \in [b^-, b^+]$ with $b^- = \lfloor \sqrt{1 - r_2^2} \rfloor_{15}$ ($b^- = 0$ if $r_2 = 1$) and $b^+ = \lceil \sqrt{1 - r_1^2} \rceil_{15}$. Interval arithmetic then gives rational enclosures $p_j x_j \in [\pi_j^-, \pi_j^+]$ and $p_j b \in [\beta_j^-, \beta_j^+]$ with $\beta_j^- \ge 0$. We define $\bar{m}(B) = 1$ if $b^- = 0$ or $r_2 d(t_2) \ge b^-$, and otherwise $\bar{m}(B)$ is a rational with $\bar{m}(B) \ge r_2 d(t_2)/b^-$. Then $m \le \min(1, a_2/b) \le \min(1, \bar{m}(B))$ at every point of B with $r < 1$.

Definition 3.15 (box envelope)**.** $F_B(y) = \sum_j \max(\pi_j^+ + \beta_j^+ y,\ -\pi_j^- - \beta_j^- y)$ for $y \ge 0$, and $F_B(y) = \sum_j \max(\pi_j^+ + \beta_j^- y,\ -\pi_j^- - \beta_j^+ y)$ for $y < 0$.

Lemma 3.16 (envelope)**.** *$F(y) \le F_B(y)$ for all $y \in \mathbb{R}$ and all points of B with $r < 1$. On each half-line, F_B is the maximum of the 2^4 affine functions obtained by choosing one of the two lines in each summand.*

Proof. $|p_j x_j + p_j b y| = \max(p_j x_j + p_j b y,\ -p_j x_j - p_j b y)$. For $y \ge 0$: $p_j x_j + p_j b y \le \pi_j^+ + \beta_j^+ y$ and $-p_j x_j - p_j b y \le -\pi_j^- - \beta_j^- y$. For $y < 0$: $p_j b y \le \beta_j^- y$ and $-p_j b y \le -\beta_j^+ y$. A sum of maxima is the maximum over all choices. □

Definition 3.17 (box certificate)**.** Let $m^* \in (0, \min(1, \bar{m}(B))]$ and let $p^* < 0$ be optional. A *box certificate for* (B, s, m^*, p^*) is $c \in \mathbb{Q}^7$ with $P(y) = \sum c_k y^k$ such that (W1) $P(y) > F_B(y)$ for all $y \in \mathbb{R}$, and (W2) c satisfies the objective bound for $(u_1, u_2, m^*, p^*, T^-(u_1, u_2))$, with T^- as in (3.2).

Lemma 3.18 (box certificate lemma)**.** *If c is a box certificate for (B, s, m^*, p^*), then $\mathbb{E}|L| < T(u)$ at every point of B with $r < 1$ and every remainder M with $m \le m^*$ and, if p^* is given, $p_3 \le p^*$.*

Proof. By Lemmas 3.14 and 3.16 and (W1), $\mathbb{E}|L| = \mathbb{E}F(M) \le \mathbb{E}P(M)$. By Lemma 3.12 and (W2), $\mathbb{E}P(M) < T^-(u_1, u_2) \le T(u)$, using (3.2). □

With $m^* = \min(1, \bar{m}(B))$ and no p^*, Lemma 3.18 covers every remainder. These are the boxes of kind lp.

3.7 Near $(e_1+e_2)/\sqrt{2}$: the near-circle lemma

Lemma 3.19 (tail bound). *Let $y \in \mathbb{R}$, $b \geq 0$ and let Z be a random variable with $\mathbb{E}Z = 0$ and $\mathbb{E}Z^4 < \infty$. Then*

$$\mathbb{E}|y + bZ| \leq |y| + \min\Big(b\,\mathbb{E}|Z|,\ \frac{27}{128}\,\frac{b^4\mathbb{E}Z^4}{|y|^3}\Big),$$

where for $y = 0$ the minimum is read as its first entry. The same convention is used below whenever this bound is applied at a point where $y = 0$.

Proof. The first bound is the triangle inequality. For the second (only needed for $y \neq 0$), $|y+z| - |y| - \operatorname{sgn}(y)z = 2(-\operatorname{sgn}(y)z - |y|)_+ \leq 2(|z| - |y|)_+$, and $\mathbb{E}[\operatorname{sgn}(y)bZ] = 0$. For $x \geq 0$ and $\eta > 0$, $(x-\eta)_+ \leq \frac{27}{256}x^4/\eta^3$: the maximum of $(x-\eta)/x^4$ over $x > \eta$ is at $x = \frac{4}{3}\eta$ and equals $\frac{27}{256}\eta^{-3}$. Hence $\mathbb{E}|y+bZ| - |y| \leq 2 \cdot \frac{27}{256}\, b^4\mathbb{E}Z^4/|y|^3$. □

Lemma 3.20 (near-circle tests). *Let B be a box with $r_1 > 0$. Let y_j $(j = 1, \dots, 4)$ be the atoms of $c\chi_1 + sd\chi_2$, so that the atoms of $a_1\chi_1 + sa_2\chi_2$ are ry_j. Let $\eta_j \geq 0$ be a lower bound of $|y_j|$ on B, p_j^+ an upper bound of p_j, and $E_4 = 3 + \max(0, w^+ - 4)\,\min(1, \bar{m}(B))^2$. Let $T^- = T^-(u_1, u_2)$.*

(A) If all $\eta_j > 0$ and $\frac{27}{128}E_4(b^+)^2\frac{1+r_2}{r_1^3}\sum_j p_j^+\eta_j^{-3} < T^-$, then at every point of B with $u \geq u_3$: $\mathbb{E}|L| < T$ if $r < 1$, and $\mathbb{E}|L| \leq T$ if $r = 1$, with equality only in the case of Lemma 3.4 $(q = q_3,\ s = 1,\ a_1 = a_2)$.

(B) Let G^+ be an upper bound of $\mathbb{E}|c\chi_1 + sd\chi_2| = \tau\sum_j |g_j|$ on B with $G^+ \leq T^-$, and $e_j^+ = \min\big(b^+, \frac{27}{128}(b^+)^4E_4/(r_1^3\eta_j^3)\big)$ $(e_j^+ = b^+$ if $\eta_j = 0)$. If $\sum_j p_j^+e_j^+ < T^-(1-r_2) + r_1(T^- - G^+)$, then $\mathbb{E}|L| < T$ at every point of B.

Proof. At a point of B with $r < 1$, condition on (χ_1, χ_2) and apply Lemma 3.19 with $Z = M$. Here $\mathbb{E}M^4 = 3 + \kappa_4 p_4 \leq E_4$, by Lemma 3.8, since $p_4 \leq m^2 \leq \min(1, \bar{m})^2$. This gives $\mathbb{E}|L| \leq rG + \sum_j p_j e_j$, where $G = \mathbb{E}|c\chi_1 + sd\chi_2|$ and $e_j = \min(b, \frac{27}{128}b^4E_4/(r^3|y_j|^3))$; also $\mathbb{E}|M| \leq 1$. If $r = 1$ then $\mathbb{E}|L| = G$. (A) By Lemma 3.4 ($q \leq q_3$, since $u \geq u_3$), $G \leq T$. Since $1 - r = b^2/(1+r)$, $\sum_j p_j e_j \leq \frac{27}{128}\frac{b^4E_4}{r^3}\sum_j \frac{p_j}{|y_j|^3} \leq b^2 \cdot \frac{27}{128}E_4(b^+)^2\frac{1}{r_1^3}\sum_j \frac{p_j^+}{\eta_j^3} < \frac{b^2T^-}{1+r_2} \leq T(1-r)$ when $b > 0$. So $\mathbb{E}|L| < rT + T(1-r) = T$. For $r = 1$ use Lemma 3.4. (B) $\mathbb{E}|L| \leq rG^+ + \sum_j p_j^+e_j^+ < rG^+ + T^-(1-r_2) + r_1(T^- - G^+) \leq rG^+ + T^-(1-r) + r(T^- - G^+) = T^- \leq T$, using $r_1 \leq r \leq r_2$ and $T^- - G^+ \geq 0$. □

These are the boxes of kind ncA and ncB.

3.8 Near the extremiser $(e_1+e_2+e_3)/\sqrt{3}$: the m-split

The extremiser $(e_1+e_2+e_3)/\sqrt{3}$ is, in our coordinates, the point $a_1 = a_2 = b = 1/\sqrt{3}$ with $M = \chi_3$, so $m = 1$ and $p_3 = 1$. It is an interior point of the parameter region, and there the six-moment relaxation is exact, so no box certificate can work near it. In Theorem 2 this happened only at the endpoint u_3; here it happens for every u in the range. As in Theorem 2, we split according to $m = \max_{i \geq 3}|\beta_i|$ and the sign of a largest remaining coefficient.

Lemma 3.21 (three-coordinate near-sphere bound). *Consider a point with $r < 1$ and suppose $\beta_{i_0} = +m$ for some $i_0 \geq 3$. Put $a_3 = bm$, $b' = b\sqrt{1-m^2}$, $Y = a_1\chi_1 + sa_2\chi_2 + a_3\chi_{i_0}$ with atoms y_j*

and probabilities p_j $(j = 1, \dots, 8)$, $r' = \sqrt{a_1^2 + a_2^2 + a_3^2} = \sqrt{1 - b'^2}$ *and* $E_4' = 3 + \max(0, \kappa_4)$. *Then*

$$\mathbb{E}|L| \le \mathbb{E}|Y| + \sum_j p_j \min\Big(b',\ \frac{27}{128}\frac{b'^4 E_4'}{|y_j|^3}\Big).$$

If moreover $q \in [q_L, q_3]$, *all* $y_j \neq 0$ *and* $\frac{27}{128} E_4' b'^2 (1 + r') \sum_j p_j |y_j|^{-3} < T$, *then* $\mathbb{E}|L| < T$ *if* $b' > 0$, *and if* $b' = 0$ *then* $\mathbb{E}|L| = G_3(a_1, sa_2, a_3) \le T$.

Proof. If $m = 1$ then $b' = 0$ and $L = Y$. Otherwise $L = Y + b'M'$, where $M' = \sum_{i \ge 3,\, i \neq i_0} \beta_i' \chi_i$ with $\beta_i' = \beta_i / \sqrt{1 - m^2}$. Then M' is independent of Y, $\sum \beta_i'^2 = 1$ and $\sum \beta_i'^4 \le 1$, so $\mathbb{E}M'^4 = 3 + \kappa_4 \sum \beta_i'^4 \le E_4'$ by Lemma 3.8. Conditioning on $(\chi_1, \chi_2, \chi_{i_0})$ and applying Lemma 3.19 with $Z = M'$ (and $\mathbb{E}|M'| \le 1$) gives the first bound. By Lemma 3.5, $\mathbb{E}|Y| = G_3(a_1, sa_2, a_3) \le Tr'$. If $b' > 0$, the hypothesis and $1 - r' = b'^2/(1 + r')$ give $\sum_j p_j \frac{27}{128} \frac{b'^4 E_4'}{|y_j|^3} < T \frac{b'^2}{1 + r'} = T(1 - r')$, hence $\mathbb{E}|L| < Tr' + T(1 - r') = T$. □

Piece tests. Let B be a box with $b^- > 0$, and $[m_1, m_2] \subset (0, 1]$. On $B \times [m_1, m_2]$ we enclose $a_3 \in [b^- m_1, b^+ m_2]$, $b'^2 \le (b'^2)^+ := (b^+)^2(1 - m_1^2)$, $b' \le b'^+$ with b'^+ an upper bound of $\sqrt{(b'^2)^+}$, and $r' \le r'^+$ with r'^+ an upper bound of $\min\big(1, \sqrt{1 - (b^-)^2(1 - m_2^2)}\big)$ (recall $r'^2 = 1 - b^2(1 - m^2)$). The atoms $y_j = a_1 x_{j1} + sa_2 x_{j2} + a_3 x_{j3}$ ($x \in \{u, -v\}^3$) and the products $p_j y_j = \tau \sum_i (\pm a_i) \prod_{k \neq i} \Pr[x_{jk}]$ (by $qu = (1 - q)v = \tau$) are enclosed in interval arithmetic. Let η_j be a lower bound of $|y_j|$, p_j^+ an upper bound of p_j, and $E_4' = 3 + \max(0, w^+ - 4)$. The piece passes

- test (A3) if all $\eta_j > 0$ and $\frac{27}{128} E_4' (b'^2)^+ (1 + r'^+) \sum_j p_j^+ \eta_j^{-3} < T^-(u_1, u_2)$;
- test (B3) if $\sum_j \big(|p_j y_j|^+ + p_j^+ \min\big(b'^+, \frac{27}{128}((b'^2)^+)^2 E_4' / \eta_j^3\big)\big) < T^-(u_1, u_2)$, where $|p_j y_j|^+$ is an upper bound of $|p_j y_j|$ (the second entry of the minimum is omitted if $\eta_j = 0$).

By Lemma 3.21, if a piece passes (A3), then at every point of B with $u \in [u_3, U_+]$ and every remainder with $\beta_{i_0} = +m$, $m \in [m_1, m_2]$, we have $\mathbb{E}|L| < T$ if $b' > 0$ and $\mathbb{E}|L| \le T$ if $b' = 0$. If it passes (B3), then $\mathbb{E}|L| < T$ by the first bound of Lemma 3.21 alone.

Definition 3.22 (m-split box)**.** An m-split box is a box B with sign s and $b^- > 0$, together with: a rational $m_c \in (0, 1]$ and a rational p^* with $\varphi(m_c) \le p^* < 0$ (this forces $2m_c^2 > 1$, because $\varphi(m) < 0$ iff $(1 - m^2)^{3/2} < m^3$ iff $2m^2 > 1$; the verifier also checks $2m_c^2 > 1$ directly); a box certificate $c^{(1)}$ for $(B, s, \min(m_c, \bar{m}(B)), -)$; a box certificate $c^{(2)}$ for $(B, s, \min(1, \bar{m}(B)), p^*)$; and pieces $[m_1, m_2]$, each passing (A3) or (B3), whose union contains $[m_c, \min(1, \bar{m}(B))]$.

Lemma 3.23 (m-split lemma)**.** *Let* B *be an* m*-split box. At every point of* B *with* $r < 1$ *and* $u \in [u_3, U_+]$ *we have* $\mathbb{E}|L| \le T$. *Equality forces* $m = 1$, $\beta_{i_0} = +1$ *for some* i_0 *(that is,* $\alpha = a_1 e_1 + sa_2 e_2 + b e_{i_0}$*), and* $G_3(a_1, sa_2, b) = T$.

Proof. Recall $m \le \min(1, \bar{m}(B))$. If $m \le m_c$, use $c^{(1)}$ and Lemma 3.18: $\mathbb{E}|L| < T$. If $m \ge m_c$ and $\beta_{i_0} = -m$ for some i_0, then $p_3 \le \varphi(m_c) \le p^*$ by Lemma 3.10; use $c^{(2)}$ and Lemma 3.18: $\mathbb{E}|L| < T$. Otherwise $\beta_{i_0} = +m$ for some i_0, and $m \in [m_c, \min(1, \bar{m}(B))]$ lies in a piece. The piece tests give $\mathbb{E}|L| < T$ unless $b' = 0$, i.e. $m = 1$, and then $\mathbb{E}|L| = G_3(a_1, sa_2, b) \le T$. □

3.9 Computer verification

All scripts and outputs are in the repository (`scripts/`, `outputs/`). Floating point (HiGHS linear programming via scipy) is used only to *find* certificates. Every *verification* is exact or uses outward-rounded interval arithmetic. The programs are those of Theorem 2, run with the environment variable `RQ_K=3`, which selects the target T (in the generators `cert2c.py`, `nearcircle.py`, `nsphere3.py` and in the verifier `verify_k2.py`) and, in the verifier, the data list `outputs/k3_manifest.json`, the target Θ_1 and the $k = 3$ three-bit claim.

3.9.1 Data

- One-coordinate cells: 10 files `outputs/k3/one/o00.json`, ..., `o09.json` (2 704 cells), covering $u \in [U_-, U_+]$ and $a \in [0, \frac{2}{5}]$.
- Two-coordinate boxes: 58 files `outputs/k3/cover2c/p00.json`, ..., `p57.json` ($s = +1$, u-slabs of width 0.005, the first one $[U_-, \frac{423}{200}]$) and 29 files `m00.json`, ..., `m28.json` ($s = -1$, width 0.01, the first one $[U_-, \frac{53}{25}]$). For each sign they cover $[U_-, U_+] \times [0, T_8] \times [\frac{2}{5}, 1]$. Each file records $K = 3$ and $A_S = \frac{2}{5}$. Each box record has its kind and data: lp (certificate c), ncA/ncB, small (boxes with $r_2 c(t_1) \le \frac{2}{5}$, i.e. $a_1 \le \frac{2}{5}$ on the whole box, which are left to the one-coordinate route), and ms (m_c, p^*, $c^{(1)}$, $c^{(2)}$ and the pieces).

sign	lp	ncA	ncB	ms	small	total
$s = +1$	45 720	1 097	1 205	21 232	617	69 871
$s = -1$	11 613	0	232	0	259	12 104

Table 3.1: Two-coordinate boxes for Theorem 3. Widths range from $2.5 \cdot 10^{-3}$ to 0.0106 in u, from $1.6 \cdot 10^{-3}$ to 0.052 in t and from $3.1 \cdot 10^{-3}$ to 0.05 in r. The ms boxes carry 32 932 pieces (32 386 of type (A3), 546 of type (B3)), with $m_c \in \{\frac{3}{4}, \frac{31}{40}, \frac{4}{5}, \frac{33}{40}, \frac{17}{20}, \frac{7}{8}, \frac{9}{10}\}$.

3.9.2 Generation

`scripts/run_k3.sh` runs the 97 jobs of `outputs/k3/jobs.txt`. A two-coordinate job is `RQ_K=3 RQ_AS=2/5 python3 cover2c.py u1 u2 s out.json 1 8 12 18 ms`: it bisects $[u_1, u_2] \times [0, T_8] \times [\frac{2}{5}, 1]$ adaptively (8 initial t-intervals, 12 r-intervals, depth ≤ 18) and on each box tries, in order: small; the near-circle tests (`nearcircle.py`, exact rationals); a box certificate (`cert2c.py`); the m-split (`cover2c.try_msplit`, `nsphere3.py`). The certificates come from a discretised six-moment linear program (dual multipliers of the moment rows), rounded to rationals and repaired; (W1) is checked exactly on every linear piece of F_B by real-root counting, and (W2) exactly by bisection. One-coordinate cells come from `cover_k3.py` (the pipeline of `MAIN_RESULT` with target Θ_1). No box or cell failed.

3.9.3 Independent verification

`RQ_K=3 python3 verify_k2.py` re-checks everything. The verifier shares no code with the generators; it reuses only the Sturm-sequence, integer-square-root and tiling helpers of `verify_all.py` (the verifier of Theorem 1, audited in A.6). Its parts:

A. Symbolic identities (sympy): $p_j x_j = r\tau g_j$ for both signs, $\sum p_j = 1$, mean 0, the two-coordinate values, the half-angle formulas, the constant $27/256$, the identity $T = \sqrt{3}\,\tilde{T}(u)$ and the derivative of $u^5/(1+u^2)^3$.

B. Coverage (exact). The one-coordinate cells tile $[U_-, U_+] \times [0, \frac{2}{5}]$. For each sign the boxes tile $[U_-, U_+] \times [0, T_8] \times [\frac{2}{5}, 1]$: they lie in the region, have pairwise disjoint interiors and total volume equal to the volume of the region. A closed subset of full measure is dense, so it is the whole region. Also $U_- < u_3$, $U_+ < u_4$, $T_8 \geq \sqrt{2} - 1$, every file has $K = 3$ and $A_S = \frac{2}{5}$, and every small box has $r_2 c(t_1) \leq \frac{2}{5}$.

C. One-coordinate cells: (V1)–(V3) by Sturm sequences; $\Theta_1 > 0$; (V4) strictly by Sturm on $[0, \bar{m}]$.

D. Box certificates (lp, and both certificates of each ms box): (W1) by writing F_B on each half-line as the maximum of the 16 sign-pattern lines and checking by Sturm counting that P minus each line is positive on that half-line; (W2) strictly, with the target $T^-(u_1, u_2)$ of (3.2); for ms boxes also $0 < m_c \leq 1$, $2m_c^2 > 1$, $p^* < 0$, $p^* \geq \varphi(m_c)$ (as $(p^* + m_c^3)^2 \geq (1 - m_c^2)^3$ with $p^* + m_c^3 \geq 0$), and $m^* = \min(m_c, \bar{m})$ for $c^{(1)}$. The verifier recomputes $\bar{m}$ as the exact quotient $r_2 d(t_2)/b^-$.

E. Near-circle boxes: mpmath interval arithmetic (120 bits), tests (A)/(B) strictly, with T^- computed from an interval enclosure of $\sqrt{3}$.

F. m-split pieces: the pieces with $s_3 = +1$ cover $[m_c, \min(1, \bar{m})]$; each passes (A3) or (B3) in mpmath interval arithmetic (120 bits); the box has $u_1 \geq 2$.

G. The three-bit claim of Lemma 3.5, for all 256 functions, by exact Sturm sequences as described there, on $[q_L, q_3]$ with $q_L = 1/(1 + U_+^2)$, including the list of equality cases.

The output is `outputs/verify_k3_ABCDEFG.txt` (all parts pass).

Negative tests. `RQ_K=3 python3 break_tests_k2.py` corrupts random samples of records and runs the check functions of `verify_k2.py` on them (output `outputs/break_tests_k3.txt`). A corruption is counted only if it changes the record. On 40 ms boxes, each of the following is rejected 40 times out of 40: lowering m_c by $\frac{1}{10}$ (the pieces no longer reach m_c); removing or halving the top piece; lowering p^* by $\frac{1}{100}$ (below $\varphi(m_c)$); lowering the constant term of $c^{(2)}$ by 10^{-3}; multiplying the constant term of $c^{(1)}$ by $\frac{99}{100}$; widening the r- or the t-interval downwards by $\frac{1}{20}$. Raising m_c by $\frac{1}{10}$ is rejected 37/40 times; in the other three cases $c^{(1)}$ still satisfies the objective bound with the larger cap, the pieces still cover $[m_c, 1]$ and φ is decreasing, so the modified record is still a valid proof. The pair $(-m_c,\, 1 + m_c^3)$ satisfies the φ inequality $(p^* + m^3)^2 \geq (1 - m^2)^3$, $p^* + m^3 \geq 0$ for $m = -m_c$; the check rejects it in 40/40 cases because it also requires $0 < m_c \leq 1$ and $p^* < 0$. On 60 lp boxes, lowering c_0 by $10^{-3}|c_0|$ or c_6 by $10^{-1}|c_6|$ is rejected 60/60 times, and widening the r-interval downwards by $\frac{1}{10}$ (but not below $\frac{2}{5}$) is rejected in all 58 cases where it changes the box (two of the sampled boxes already start at $r = \frac{2}{5}$). On 60 near-circle boxes, widening the r-interval by $\frac{1}{10}$ is rejected 60/60 times; on 40 one-coordinate cells, lowering c_0 by $10^{-3}|c_0|$ is rejected 40/40 times. The claim of Lemma 3.5 fails at $q_3 + 10^{-3}$ (for the OR of two bits).

Two corruptions are *not* always detected, as expected. Shifting an ms box by $-\frac{1}{20}$ in u (below u_3) passes part F in 17/40 cases (it is rejected by part D in 40/40 cases), and moving a near-circle box to $u \leq 2 < u_3$ passes part E in 43/60 cases. The piece test (A3) and the near-circle test (A) only bound the error term. The main term is bounded by Lemma 3.5 and by Lemma 3.4 with

$T_2 \le T$, and both hold only for $q \le q_3$. This is why Lemma 3.20(A) and Lemma 3.23 are stated only for $u \ge u_3$, and why the theorem stops at u_3.

3.9.4 Reproducing

```
pip install numpy scipy sympy mpmath
cd scripts
RQ_K=3 python3 verify_k2.py        # parts A-G
RQ_K=3 python3 break_tests_k2.py   # negative tests
# regeneration of one slab, e.g. the first one (s = +1, next to u3):
RQ_K=3 RQ_AS=2/5 python3 cover2c.py 2109381/1000000 423/200 1 \
        ../outputs/k3/cover2c/p00.json 1 8 12 18 ms
```

3.10 Proof of Theorem 3

(a) By Lemma 3.2 let $q \in [q_L, q_3]$, i.e. $u \in [u_3, U_+] \subset [U_-, U_+]$. Reduce α as in Section 3.2.3.

(1) $a_1 = 1$: $\alpha = e_1$ and $\mathbb{E}|L| = 2\tau < T$ (Lemma 3.3(ii)).

(2) $a_1 \le \frac{2}{5}$: (u, a_1) lies in a cell, and Lemma 3.13 gives $\mathbb{E}|L| < T$.

(3) $a_1 > \frac{2}{5}$ and $r = 1$: $L = a_1\chi_1 + sa_2\chi_2$, and Lemma 3.4 ($q \le q_3$) gives $\mathbb{E}|L| \le T$, with equality iff $q = q_3$, $s = 1$ and $a_1 = a_2$.

(4) $a_1 > \frac{2}{5}$ and $r < 1$: (u, t, r) lies in a box of the cover for the sign s (part B), and the box is not small, because $a_1 > \frac{2}{5}$. If it is lp, Lemma 3.18 with $m^* = \min(1, \bar{m}(B)) \ge m$ gives $\mathbb{E}|L| < T$. If it is ncA or ncB, Lemma 3.20 gives $\mathbb{E}|L| < T$ (here $u \ge u_3$). If it is ms, Lemma 3.23 gives $\mathbb{E}|L| \le T$ (here $u \in [u_3, U_+]$).

So $\mathbb{E}|L| \le T$ always, and $(e_1 + e_2 + e_3)/\sqrt{3}$ attains T (Lemma 3.3, $q < \frac{1}{3}$). Hence $R(q) = T(q)$. For $q \in [1 - q_3, 1 - q_L]$ use Lemma 3.2: $R(q) = R(1 - q) = 2\sqrt{3}\, q^2\tau$.

(b) Equality can occur only in case (3) and in the ms case of (4). Case (3) gives $q = q_3$ and $\alpha = \pm(e_i + e_j)/\sqrt{2}$. In the ms case, Lemma 3.23 gives $\alpha = a_1e_1 + sa_2e_2 + be_{i_0}$ (after the reduction) with $G_3(a_1, sa_2, b) = T$ and $a_1, b > 0$, $a_2 \ge |\alpha_{i_0}| = b > 0$. By Lemma 3.5, (a_1, sa_2, b) is a positive multiple of $\pm(1, 1, 1)$, or $q = q_3$ and it is a positive multiple of $\pm(e_i + e_j)$. The second is impossible because all three entries are nonzero. So $s = 1$ and $a_1 = a_2 = b$, i.e. $\alpha = (e_1 + e_2 + e_{i_0})/\sqrt{3}$. Undoing the reduction (global sign and permutation) gives the list in (b). Conversely, each listed vector attains T at the stated q (Lemma 3.3; at q_3, $T_2 = T$). For $q \ge \frac{1}{2}$ use Lemma 3.2.

(c) For $q \in (q_3, \frac{1}{2}]$, $R(q) \ge T_2(q) > T(q)$ by Lemma 3.3 and (i). For $q < q_4 < \frac{1}{4}$, $R(q) \ge \mathbb{E}|\chi_1 + \cdots + \chi_4|/2 = 4(1 - q)^3\tau > T(q)$ by Lemma 3.3 and (iii). Together with (a) this gives $[q_L, q_3] \subseteq \{q \le \frac{1}{2} : R(q) = T(q)\} \subseteq [q_4, q_3]$. □

3.11 Remarks

1. **What changed from Theorem 2.** Only the target, the range, A_S, Θ_1 and the three-bit lemma. The near-circle lemma now treats a point that is *not* an extremiser for $q < q_3$: at $(e_1 + e_2)/\sqrt{2}$ we have $\mathbb{E}|L| = T_2 < T$. The m-split, which in Theorem 2 was needed only for $u \ge 2.09$, is now needed throughout $[u_3, U_+]$ (it is used in 21 232 of the 69 871 of the $s = +1$ boxes).

2. **Why the range stops at $\frac{25}{169}$.** Two parts of the method lose their margin below $q \approx 0.14$ (`outputs/k3/scan_one.txt`, `scan_two.txt`; floating point, evidence only). (i) The one-coordinate route: as $a_1 \to 0$ the remainder becomes Gaussian, and the best six-moment bound tends to the six-moment Gaussian value $\sup\{\mathbb{E}|X| : \mathbb{E}X^j = \mathbb{E}G^j,\ j \le 6\} \approx 0.888074$. The scanned ratio of the six-moment bound to T is 0.9937 at $q = 0.15$, 0.9990 at $q = 0.14$ and 1.0027 at $q = 0.135$, for small a. (ii) The two-coordinate route near $a_1 = a_2 \approx 0.57$: the plain certificate already fails at $q = 0.145$ (margin $-5 \cdot 10^{-4}$, so the m-split is needed there), and at $q = 0.14$ the scan has points where every tried m_c fails (the capped certificate or the piece test (A3)).

3. **The gap $[q_4, \frac{25}{169})$.** We conjecture $R = T$ on $[q_4, q_3]$; this is the case $k = 3$ of the conjecture $R(q) = \max_k 2\sqrt{k}(1-q)^{k-1}\tau$ for $q \le \frac{1}{2}$ (BF3, Stone; RQ-C's Conjecture S). Six moments cannot reach q_4: $0.888074 > T(q_4) \approx 0.884970$. Eight moments do not help either, since the eight-moment Gaussian value is ≈ 0.886410. Ten moments give ≈ 0.856068, below $\sqrt{2/e} \approx 0.857764 = \lim_{q\to 0} R(q)$ (these values come from a floating-point linear program over polynomial majorants of $|y|$; numerical). At q_4 the vector $(e_1 + \cdots + e_4)/2$ also attains T. In our coordinates it has $M = (\chi_3 + \chi_4)/\sqrt{2}$ with two equal largest coefficients, which the m-split does not handle.

4. **Status.** Audited VALID by RQ-AUD (A.14, 2026-10-22 10:37 UTC), with no fix, and refereed VALID by RQ-REF1 (2026-10-22 15:38 UTC), with no fixes; after the referee's report only this item was changed. The computer steps have been run twice (generator and independent verifier), the verifier rejects corrupted data (negative tests above), and the referee re-did every computer step with its own exact programs.

Chapter 4

The $k = 3$ regime of $R(q)$, lower part: $R(q) = 2\sqrt{3}\,(1-q)^2\sqrt{q(1-q)}$ for $1 - \frac{\sqrt{3}}{2} \le q \le \frac{25}{169}$, and hence on the whole $k = 3$ regime $[1 - \frac{\sqrt{3}}{2},\, 1 - \sqrt{2/3}]$

Source: RQ-A, `MAIN_RESULT_K3B.tex` (md5 `efa33947fa2293a078c7aa805b4d1ab2`), by "RQ-A (R(q) attack)", dated 22 October 2026. Its main result is Theorem 4 (claim MAIN-4), which keeps this name.

Refereed version: md5 `53aa11d14ea1f70b944843aaff8de1ce`, the file in commit `6ecd564`. The source differs from it only in the status item of the closing remarks, which now records the audit and referee verdicts.

Audit: A.18, VALID and NEW, no fix (22 October, 12:41 UTC).

Referee: RQ-REF1, VALID, no fixes (report `REFEREE.md`, md5 `369c1cfb...`, mirrored at 15:38 UTC on 22 October).

Use in the Main Theorem: Step 1, through Corollary 5.2.

Transcription: the whole paper, with the mechanical changes of Appendix C: labels prefixed by `ch04:`, numbers n become $4.n$, the title becomes the chapter title, no table of contents, the abstract as a quoted block. No editorial footnotes.

Abstract of the source paper. For $q \in (0,1)$ let $\chi_1, \chi_2, \dots$ be i.i.d. normalised q-biased bits and let $R(q)$ be the supremum of $\mathbb{E}|\sum \alpha_i \chi_i|$ over unit vectors α. We prove that $R(q) = 2\sqrt{3}\,(1-q)^2\sqrt{q(1-q)}$ for every $q \in [q_4, \frac{25}{169}]$, where $q_4 = 1 - \sqrt{3}/2 \approx 0.13397$ (and the mirror statement on $[\frac{144}{169}, 1 - q_4]$), and we determine all extremisers: $(e_i + e_j + e_k)/\sqrt{3}$, and at $q = q_4$ also $(e_i + e_j + e_k + e_l)/2$. Together with our Theorem 3 (`MAIN_RESULT_K3`, audited VALID), this determines R on the whole regime where three equal coefficients are optimal: $R(q) = 2\sqrt{3}\,(1-q)^2\sqrt{q(1-q)}$ exactly for $q \in [q_4, q_3]$, $q_3 = 1 - \sqrt{2/3}$, and this interval is exactly the set of $q \le \frac{1}{2}$ where this formula holds. With our Theorems 1 and 2 we obtain $R(q) = 2\sqrt{q(1-q)}\,\max_{k \ge 1} \sqrt{k}\,\hat{q}^{\,k-1}$, $\hat{q} = \max(q, 1-q)$, for all $q \in [q_4, 1 - q_4]$. The proof follows Theorem 3 with three new ingredients: polynomial certificates of degree up to ten with a ten-moment bound; *vertex certificates*, which use convexity and homogeneity of $x \mapsto \mathbb{E}|x \cdot (\chi_1, \chi_2, y)|$ to replace interval envelopes over a box by one certificate per vertex of a polytope whose cone contains the parameter patch; and a four-coordinate near-sphere bound based on an exact four-bit lemma, which handles the second extremiser at q_4. The computer-assisted steps (1 421 boxes

with 2 845 sets of vertex certificates, 288 cells, and the bit lemmas) use exact rational arithmetic and certified interval arithmetic, and all of them were repeated by an independent program.

4.1 Statement

Fix $q \in (0,1)$ and put

$$u = \sqrt{\tfrac{1-q}{q}}, \qquad v = \frac{1}{u}, \qquad \tau = \sqrt{q(1-q)}.$$

Let $\chi, \chi_1, \chi_2, \dots$ be i.i.d. with $\Pr[\chi = u] = q$ and $\Pr[\chi = -v] = 1-q$, so that $\mathbb{E}\chi = 0$, $\mathbb{E}\chi^2 = 1$ and $\mathbb{E}|\chi| = 2\tau$. Let

$$R(q) = \sup_{n \ge 1} \sup_{\alpha \in \mathbb{R}^n \setminus \{0\}} \frac{\mathbb{E}\left|\sum_{i=1}^n \alpha_i \chi_i\right|}{|\alpha|_2}.$$

Put

$$q_3 = 1 - \sqrt{2/3} \approx 0.183503, \qquad q_4 = 1 - \tfrac{\sqrt{3}}{2} \approx 0.133975, \qquad q_L = \tfrac{25}{169} \approx 0.147929,$$

$$T(q) = 2\sqrt{3}\,(1-q)^2\,\tau, \qquad T_2(q) = 2\sqrt{2}\,(1-q)\,\tau, \qquad T_4(q) = 4(1-q)^3\tau.$$

Theorem 4. *(a) For every $q \in [q_4, q_L]$, every $n \ge 1$ and every $\alpha \in \mathbb{R}^n$ with $|\alpha|_2 = 1$,*

$$\mathbb{E}\Big|\sum_{i=1}^n \alpha_i \chi_i\Big| \le 2\sqrt{3}\,(1-q)^2\sqrt{q(1-q)}.$$

For $q \in [1-q_L, 1-q_4]$ the same holds with $1-q$ replaced by q. Consequently $R(q) = 2\sqrt{3}\max(q,1-q)^2\sqrt{q(1-q)}$ for $q \in [q_4, q_L] \cup [1-q_L, 1-q_4]$.

(b) (Extremisers.) Let $q \in [q_4, q_L] \cup [1-q_L, 1-q_4]$. Equality in (a) holds if and only if $\alpha = \pm\frac{1}{\sqrt{3}}(e_i + e_j + e_k)$ with i, j, k distinct, or $q \in \{q_4, 1-q_4\}$ and $\alpha = \pm\frac{1}{2}(e_i + e_j + e_k + e_l)$ with i, j, k, l distinct.

(c) (Sharpness.) For $q \in (0, q_4)$, $R(q) \ge T_4(q) > T(q)$.

Corollary 4.1 (the whole $k = 3$ regime)**.** *With Theorem 3 of `MAIN_RESULT_K3` ($R = T$ on $[q_L, q_3]$, audited VALID by RQ-AUD as A.14): $R(q) = T(q)$ for every $q \in [q_4, q_3]$, and*

$$\{q \in (0, \tfrac{1}{2}] : \ R(q) = T(q)\} = [q_4, q_3].$$

For $q \in [q_4, q_3]$ the extremisers are the vectors $\pm(e_i + e_j + e_k)/\sqrt{3}$, together with $\pm(e_i + e_j)/\sqrt{2}$ when $q = q_3$ and $\pm(e_i + e_j + e_k + e_l)/2$ when $q = q_4$. The mirror statements hold on $[1-q_3, 1-q_4]$.

Proof. On $[q_L, q_3]$ this is Theorem 3(a),(b); on $[q_4, q_L]$ it is Theorem 4(a),(b). For $q \in (q_3, \frac{1}{2}]$, $R(q) \ge T_2(q) > T(q)$ (Theorem 3(c), or Lemma 4.4(i) below), and for $q < q_4$, $R(q) \ge T_4(q) > T(q)$ (Theorem 4(c)). □

Corollary 4.2. *With Theorem 1 of `MAIN_RESULT` ($R(q) = 2\tau$ on $[q_0, 1-q_0]$, $q_0 = 1 - 1/\sqrt{2}$; audited VALID as A.6) and Theorem 2 of `MAIN_RESULT_K2` ($R(q) = T_2(q)$ on $[q_3, q_0]$, mirrored on $[1-q_0, 1-q_3]$; audited VALID as A.11):*

$$R(q) = 2\sqrt{q(1-q)}\,\max\{1,\ \sqrt{2}\,\hat{q},\ \sqrt{3}\,\hat{q}^{\,2}\} = 2\sqrt{q(1-q)}\,\max_{k \ge 1} \sqrt{k}\,\hat{q}^{\,k-1}, \qquad \hat{q} = \max(q, 1-q),$$

for all $q \in [q_4, 1-q_4] = [1 - \frac{\sqrt{3}}{2}, \frac{\sqrt{3}}{2}]$.

Proof. By symmetry (Lemma 4.3) let $q \le \frac{1}{2}$, so $\hat{q} = 1-q$. The maximum of $\{1, \sqrt{2}(1-q), \sqrt{3}(1-q)^2\}$ is $\sqrt{3}(1-q)^2$ on $[q_4, q_3]$, $\sqrt{2}(1-q)$ on $[q_3, q_0]$ and 1 on $[q_0, \frac{1}{2}]$: indeed $\sqrt{3}(1-q)^2 \ge \sqrt{2}(1-q)$ iff $1-q \ge \sqrt{2/3}$, $\sqrt{2}(1-q) \ge 1$ iff $1-q \ge 1/\sqrt{2}$, and $\sqrt{3}(1-q)^2 \ge 1$ for $q \le q_3$. So the first formula follows from Corollary 4.1 and Theorems 1 and 2. For the second, let $k \ge 4$ and $1-q \le \frac{\sqrt{3}}{2}$ (i.e. $q \ge q_4$). Then $\sqrt{k}(1-q)^{k-1} \le \sqrt{3}(1-q)^2$ iff $\sqrt{k/3}\,(1-q)^{k-3} \le 1$, and $\sqrt{k/3}\,(1-q)^{k-3} \le (\frac{k}{3}(\frac{3}{4})^{k-3})^{1/2}$. The sequence $\frac{k}{3}(\frac{3}{4})^{k-3}$ equals 1 at $k=4$ and decreases for $k \ge 4$, since $\frac{k+1}{k} \cdot \frac{3}{4} \le \frac{5}{4} \cdot \frac{3}{4} < 1$. So the terms with $k \ge 4$ never exceed the term with $k=3$ on $[q_4, \frac{1}{2}]$. □

Part (c) and the lower bound $R \ge T$ in (a) are elementary (Lemma 4.4). The content is the upper bound in (a), and (b).

Relation to Theorem 3. The proof follows `MAIN_RESULT_K3` (Theorem 3) step by step. The new ingredients are:

(i) the range $u \in [\frac{12}{5}, u_4]$ and the threshold $A_S = \frac{7}{20}$ of the one-coordinate route;

(ii) polynomial certificates of degree up to ten, with an expectation bound that uses ten moments of the remainder (Section 4.4). Six moments cannot reach q_4 (Remark 3 of `MAIN_RESULT_K3`); the one-coordinate cells here have degree ten;

(iii) *vertex certificates* (Section 4.6), which replace the box certificates of Theorem 3. They are needed because near q_4 the slack of the certificates is small and the first-order loss of the interval envelope over a box is too large;

(iv) in the m-split near $(e_1+e_2+e_3)/\sqrt{3}$ (Section 4.8): vertex certificates for the patch with three split coordinates, a second m-split inside them, and a four-coordinate near-sphere bound based on an exact four-bit lemma (Lemma 4.7). This handles the second extremiser $(e_1 + e_2 + e_3 + e_4)/2$, which ties with $(e_1+e_2+e_3)/\sqrt{3}$ at q_4.

The lemmas that are unchanged from Theorem 3 are proved again here, so that the document can be read on its own.

Conventions. $x_+ = \max(x, 0)$. All polynomials in the computer-assisted parts have rational coefficients. "Verified" means verified in exact rational arithmetic or in outward-rounded interval arithmetic, as specified in Section 4.9. For a rational $x \ge 0$ and an integer $N \ge 1$, *rational lower and upper bounds of* $\sqrt{x}$ are $\lfloor N\sqrt{x} \rfloor / N$ and $(\lfloor N\sqrt{x} \rfloor + 1)/N$ computed with integer square roots (the verifier uses $N = 10^{15}$ for the box parameters and $N = 10^{12}$ for the patch enclosures).

4.2 Reductions

4.2.1 Symmetry and parametrisation

Lemma 4.3. *The law of $-\chi^{(q)}$ is the law of $\chi^{(1-q)}$. Hence $\mathbb{E}|\sum \alpha_i \chi_i^{(q)}| = \mathbb{E}|\sum \alpha_i \chi_i^{(1-q)}|$, $R(q) = R(1-q)$, and the extremisers for q and $1-q$ coincide.*

Proof. $-\chi^{(q)}$ takes the value $-u_q$ with probability q and v_q with probability $1-q$; since $u_{1-q} = v_q$ and $v_{1-q} = u_q$, this is the law of $\chi^{(1-q)}$. Finally $|\sum \alpha_i(-\chi_i)| = |\sum \alpha_i \chi_i|$. □

From now on $q \le \frac{1}{2}$, i.e. $u \ge 1$, and

$$q = \frac{1}{1+u^2}, \quad 1-q = \frac{u^2}{1+u^2}, \quad v = \frac{1}{u}, \quad \tau = \frac{u}{1+u^2}, \quad qu = (1-q)v = \tau. \tag{4.1}$$

On $u \ge 1$, τ and q are decreasing and $1-q$ is increasing in u. The target is

$$T = 2\sqrt{3}(1-q)^2\tau = \sqrt{3}\,\tilde{T}(u), \qquad \tilde{T}(u) = \frac{2u^5}{(1+u^2)^3}, \qquad \frac{d}{du}\frac{u^5}{(1+u^2)^3} = \frac{u^4(5-u^2)}{(1+u^2)^4},$$

so $\tilde{T}$ is increasing on $[1, \sqrt{5}]$ and decreasing on $[\sqrt{5}, \infty)$. In particular, for $1 \le u_1 < u_2$ and $u \in [u_1, u_2]$,

$$T(u) \;\ge\; T^-(u_1, u_2) := S_3 \min\{\tilde{T}(u_1), \tilde{T}(u_2)\}, \tag{4.2}$$

where $S_3 < \sqrt{3}$ is a rational lower bound of $\sqrt{3}$ (the verifier uses a lower bound with $N = 10^{15}$ in exact arithmetic, and an outward-rounded interval enclosure of $\sqrt{3}$ in its interval-arithmetic parts). The range $q \in [q_4, q_L]$ corresponds to $u \in [\frac{12}{5}, u_4]$ with

$$u_4 = \sqrt{3 + 2\sqrt{3}} \approx 2.5424597,$$

because $(1-q_4)/q_4 = \frac{\sqrt{3}/2}{1-\sqrt{3}/2} = \frac{\sqrt{3}}{2-\sqrt{3}} = \sqrt{3}(2+\sqrt{3}) = 3 + 2\sqrt{3}$ and $1/(1+(12/5)^2) = \frac{25}{169}$. We fix the rationals

$$U_- = \frac{12}{5}, \qquad U_+ = \frac{127123}{50000} = 2.54246 \;\ge u_4$$

(indeed $U_+^2 > 3$ and $(U_+^2 - 3)^2 \ge 12$, so $U_+^2 \ge 3 + 2\sqrt{3}$), and put $q_U = 1/(1+U_+^2) \le q_4$. Also $U_-^2 = 5.76 > 5$, so $\tilde{T}$ is decreasing on $[U_-, U_+]$; we do not need this, since (4.2) takes the minimum over both endpoints. The computations cover $u \in [U_-, U_+]$; the theorem uses only $u \in [U_-, u_4]$. Since $u_3 = \sqrt{2+\sqrt{6}} \approx 2.1094 < U_-$, every q in the range satisfies $q < q_3$.

4.2.2 Values of a few vectors

Lemma 4.4. *Let $k \ge 1$ and $q < 1/k$. Then $\mathbb{E}|\chi_1 + \cdots + \chi_k|/\sqrt{k} = 2\sqrt{k}\,(1-q)^{k-1}\tau$. In particular $\mathbb{E}|\chi_1| = 2\tau$, $\mathbb{E}|\chi_1+\chi_2|/\sqrt{2} = T_2$ for $q < \frac{1}{2}$, $\mathbb{E}|\chi_1+\chi_2+\chi_3|/\sqrt{3} = T$ for $q < \frac{1}{3}$, and $\mathbb{E}|\chi_1+\cdots+\chi_4|/2 = T_4$ for $q < \frac{1}{4}$. Moreover:*

(i) for $q \le \frac{1}{2}$: $T_2 \le T$ iff $q \le q_3$, with equality iff $q = q_3$;

(ii) for $q \le q_3$: $2\tau < T$;

(iii) for $q < \frac{1}{4}$: $T_4 \ge T$ iff $q \le q_4$, with equality iff $q = q_4$.

Proof. Let $S = \chi_1 + \cdots + \chi_k$ and let $x_i = \mathbf{1}\{\chi_i = u\}$. If some $x_i = 1$ then $S \ge u - (k-1)v > 0$, because $u^2 > k-1$ is equivalent to $q < 1/k$. If all $x_i = 0$ then $S = -kv < 0$. So $|S| = fS$ with $f = 1 - 2 \cdot \mathbf{1}\{\text{all } x_i = 0\}$. Since $\mathbb{E}\chi_i = 0$, $\mathbb{E}[f\chi_i] = -2\mathbb{E}[\chi_i \mathbf{1}\{\text{all } x = 0\}] = -2(1-q)^k(-v) = 2(1-q)^{k-1}(1-q)v = 2(1-q)^{k-1}\tau$. Summing over i gives $\mathbb{E}|S| = 2k(1-q)^{k-1}\tau$. The comparisons: (i) $2\sqrt{2}(1-q)\tau \le 2\sqrt{3}(1-q)^2\tau$ iff $1-q \ge \sqrt{2/3}$; (ii) for $q \le q_3$, $\sqrt{3}(1-q)^2 \ge \sqrt{3}\cdot\frac{2}{3} = \frac{2}{\sqrt{3}} > 1$; (iii) $4(1-q)^3 \ge 2\sqrt{3}(1-q)^2$ iff $1-q \ge \frac{\sqrt{3}}{2}$. □

4.2.3 Splitting off the two largest coefficients

Let $|\alpha|_2 = 1$ and $L = \sum \alpha_i \chi_i$. Changing the sign of α and permuting coordinates does not change $\mathbb{E}|L|$. So we may assume

$$a_1 := \alpha_1 = \max_i |\alpha_i| > 0, \qquad a_2 := |\alpha_2| = \max_{i \geq 2} |\alpha_i|, \qquad |\alpha_3| \geq |\alpha_4| \geq \cdots,$$

and we put $s = \operatorname{sgn} \alpha_2 \in \{1, -1\}$ ($s = 1$ if $\alpha_2 = 0$),

$$r = \sqrt{a_1^2 + a_2^2} \in (0, 1], \qquad b = \sqrt{1 - r^2}.$$

If $r < 1$, let $\beta_i = \alpha_i / b$ for $i \geq 3$ and $M = \sum_{i \geq 3} \beta_i \chi_i$. Then

$$L = a_1 \chi_1 + s\, a_2 \chi_2 + bM, \qquad \sum_{i \geq 3} \beta_i^2 = 1, \qquad m := \max_{i \geq 3} |\beta_i| = \frac{|\alpha_3|}{b} \leq \min\Big(1, \frac{a_2}{b}\Big),$$

and M is independent of (χ_1, χ_2). We use half-angle coordinates for (a_1, a_2):

$$a_1 = r\, c(t), \quad a_2 = r\, d(t), \qquad c(t) = \frac{1 - t^2}{1 + t^2}, \quad d(t) = \frac{2t}{1 + t^2}, \qquad t = \frac{a_2}{r + a_1}.$$

Since $0 \leq a_2 \leq a_1$, the angle θ with $\tan\theta = a_2/a_1$ is in $[0, \pi/4]$ and $t = \tan(\theta/2) \in [0, \sqrt{2} - 1]$. We fix $T_8 = \frac{20711}{50000} = 0.41422 \geq \sqrt{2} - 1$ (indeed $(T_8 + 1)^2 \geq 2$). On $[0, 1]$, c is decreasing and d is increasing in t, both are ≥ 0, and $c^2 + d^2 = 1$. Thus every unit α gives a point

$$(u, t, r, s) \in [U_-, U_+] \times [0, T_8] \times (0, 1] \times \{1, -1\} \qquad (u \in [U_-, u_4]).$$

We put $A_S = \frac{7}{20}$. If $a_1 \leq A_S$ we use the one-coordinate route of Section 4.5; otherwise $r \geq a_1 > A_S$ and we use the two-coordinate route of Sections 4.6–4.8.

4.3 Exact evaluations

4.3.1 Two coordinates

Lemma 4.5 (two-coordinate value)**.** *Let $q \leq \frac{1}{2}$, $c, d \geq 0$, $s \in \{1, -1\}$, and $X = c\chi_1 + s\, d\chi_2$. List the atoms of X as $(\chi_1, \chi_2) = (u, u), (u, -v), (-v, u), (-v, -v)$, with probabilities $p = (q^2,\ q(1-q),\ q(1-q),\ (1-q)^2)$ and values x_j. Then $p_j x_j = \tau g_j$ with*

$$g = \big(q(c + sd),\ (1 - q)c - s\, q\, d,\ -q\, c + s(1 - q)d,\ -(1 - q)(c + sd)\big), \tag{4.3}$$

and

$$\mathbb{E}|X| = 2\tau \max\{c,\ d,\ [s = 1]\,(1 - q)(c + d)\}$$

(the last entry is present only for $s = 1$). If $q \leq q_3$, then $\mathbb{E}|X| \leq T\sqrt{c^2 + d^2}$, and for $(c, d) \neq 0$ equality holds if and only if $q = q_3$, $s = 1$ and $c = d$. In particular $\mathbb{E}|X| < T\sqrt{c^2 + d^2}$ for $q < q_3$ and $(c, d) \neq 0$.

Proof. The identities $p_j x_j = \tau g_j$ follow from (4.1); for example $q(1-q)(cu - sdv) = (1-q)\tau c - q\tau sd$. Since $\mathbb{E}X = 0$, $\mathbb{E}|X| = 2\mathbb{E}X_+ = 2\tau \sum_j (g_j)_+$. For $s = 1$: $g_1 \geq 0 \geq g_4$, so $\mathbb{E}X_+/\tau = q(c + d) + ((1 - q)c - qd)_+ + ((1 - q)d - qc)_+$. If both middle terms are nonnegative this equals $(1 - q)(c + d)$, and then $(1 - q)(c + d) - c = (1 - q)d - qc \geq 0$ and similarly $\geq d$. If only the first is nonnegative

it equals $q(c+d)+(1-q)c-qd=c$, and $(1-q)(c+d)-c=(1-q)d-qc<0$, while $c\ge d$ (otherwise $(1-q)d-qc\ge(1-2q)c\ge 0$). The case where only the second is nonnegative is symmetric. Both negative would give $(1-q)(c+d)<q(c+d)$, impossible for $q\le\frac12$ unless $c=d=0$. In all cases $\mathbb{E}X_+/\tau=\max\{c,d,(1-q)(c+d)\}$. For $s=-1$: $g_2\ge 0\ge g_3$. If $c\ge d$ then $g_1\ge 0\ge g_4$ and $\mathbb{E}X_+/\tau=q(c-d)+(1-q)c+qd=c$. If $c<d$ then $g_1<0<g_4$ and $\mathbb{E}X_+/\tau=(1-q)c+qd+(1-q)(d-c)=d$. So $\mathbb{E}X_+/\tau=\max(c,d)$.

For the bound let $\rho=\sqrt{c^2+d^2}>0$ and $q\le q_3$. Then $2\tau\max(c,d)\le 2\tau\rho<T\rho$ by Lemma 4.4(ii), and, since $(1-q)(c+d)\le\sqrt{2}(1-q)\rho$ with equality iff $c=d$, $2\tau(1-q)(c+d)\le T_2\rho\le T\rho$ by Lemma 4.4(i), with equality iff $c=d$ and $q=q_3$. Since the third entry is present only for $s=1$, this gives the claim. □

4.3.2 Three and four coordinates

For $n\ge 1$, $f:\{0,1\}^n\to[-1,1]$ and $x_i=\mathbf{1}\{\chi_i=u\}$ put $\Delta_i(f)=\mathbb{E}[f\mid x_i=1]-\mathbb{E}[f\mid x_i=0]$, a polynomial in q. Then, by (4.1),

$$\mathbb{E}[f\chi_i]=qu\,\mathbb{E}[f\mid x_i=1]-(1-q)v\,\mathbb{E}[f\mid x_i=0]=\tau\,\Delta_i(f). \tag{4.4}$$

For $c\in\mathbb{R}^n$ write $G_n(c)=\mathbb{E}|c_1\chi_1+\cdots+c_n\chi_n|$. For a set $S\subseteq\{1,\dots,n\}$ let $\mathrm{OR}_S=2\cdot\mathbf{1}\{\exists i\in S: x_i=1\}-1$. By the computation in the proof of Lemma 4.4,

$$\Delta_i(\mathrm{OR}_S)=2(1-q)^{|S|-1}\ (i\in S),\qquad \Delta_i(\mathrm{OR}_S)=0\ (i\notin S). \tag{4.5}$$

Lemma 4.6 (three-bit lemma)**.** *Let $q\in[q_U,q_L]$ and $c\in\mathbb{R}^3$. Then $G_3(c)\le T\,|c|$. For $c\ne 0$ equality holds if and only if c is a positive multiple of $\pm(e_1+e_2+e_3)$.*

Lemma 4.7 (four-bit lemma)**.** *Let $q\in[q_4,q_L]$ and $c\in\mathbb{R}^4$. Then $G_4(c)\le T\,|c|$. For $c\ne 0$ equality holds if and only if c is a positive multiple of $\pm(e_i+e_j+e_k)$ for distinct i,j,k, or $q=q_4$ and c is a positive multiple of $\pm(e_1+e_2+e_3+e_4)$.*

Proof of Lemmas 4.6 and 4.7. Let $n\in\{3,4\}$, $X=c\cdot\chi$ and $f^*=\operatorname{sgn}X$ (with $\operatorname{sgn}0=1$), a function of $(x_1,\dots,x_n)$ with values ±1. By (4.4) and Cauchy–Schwarz,

$$G_n(c)=\mathbb{E}[f^*X]=\tau\sum_i c_i\Delta_i(f^*)\le\tau|c|\,|\Delta(f^*)|.$$

For $f:\{0,1\}^n\to\{-1,1\}$ put $H_f(q)=12(1-q)^4-\sum_{i=1}^n\Delta_i(f)^2$, a polynomial with integer coefficients. *Claims* (finite exact computations, Section 4.9, part G):

(C1) ($n=3$, all 2^8 functions) $H_f\ge 0$ on $[q_U,q_L]$; $H_f\equiv 0$ exactly for $f=\pm\mathrm{OR}_{\{1,2,3\}}$; every other H_f is >0 on $[q_U,q_L]$.

(C2) ($n=4$, all 2^{16} functions) $H_f\ge 0$ on $[q_4,q_L]$; $H_f\equiv 0$ exactly for the eight functions $f=\pm\mathrm{OR}_S$ with $|S|=3$; $H_f(q_4)=0\not\equiv H_f$ exactly for $f=\pm\mathrm{OR}_{\{1,2,3,4\}}$, and these two H_f are >0 on $(q_4,q_L]$; every other H_f is >0 on $[q_4,q_L]$.

Given the claims, $G_n(c)\le\tau|c|\sqrt{12}(1-q)^2=T|c|$ on the stated ranges. If equality holds with $c\ne0$, then $\Delta(f^*)\ne0$, c is a positive multiple of $\Delta(f^*)$, and $H_{f^*}(q)=0$. By the claims and (4.5): for $n=3$, $f^*=\pm\mathrm{OR}_{\{1,2,3\}}$ and $\Delta(f^*)=\pm2(1-q)^2(1,1,1)$; for $n=4$, either $f^*=\pm\mathrm{OR}_S$ with $|S|=3$ and $\Delta(f^*)=\pm2(1-q)^2\sum_{i\in S}e_i$, or $q=q_4$, $f^*=\pm\mathrm{OR}_{\{1,2,3,4\}}$ and $\Delta(f^*)=\pm2(1-q)^3(1,1,1,1)$. Conversely these vectors attain $T|c|$ by Lemma 4.4 (for $c=e_i+e_j+e_k$ the fourth coordinate does not contribute; at q_4, $T_4=T$).

How the claims are checked. For each f, $\Delta_i(f) = \sum_{x:x_i=1}(f(x) - f(x-e_i)) \prod_{l\neq i} q^{x_l}(1-q)^{1-x_l}$ is computed as an integer polynomial, and the distinct polynomials H_f are tested (39 for $n=3$, 1 630 for $n=4$). For $n=3$: $H_f \equiv 0$, or H_f has no real root in $[q_U, q_L]$ (Sturm) and $H_f(q_L) > 0$. For $n=4$, let $g_4(q) = 4q^2 - 8q + 1$, the minimal polynomial of q_4; it is irreducible over $\mathbb{Q}$ (its discriminant 48 is not a square), decreasing on $[0,1]$, and its other root $1+\sqrt{3}/2$ exceeds 1. Take rationals $q_4^- < q_4 < q_4^+$ with $g_4(q_4^-) > 0 > g_4(q_4^+)$ and $q_U < q_4^-$, $q_4^+ < q_L$ (from rational bounds of $\sqrt{3/4}$). Then for $H_f \not\equiv 0$: H_f has no root in $[q_4^+, q_L]$ and $H_f(q_L) > 0$; and either $g_4 \mid H_f$, $H_f = g_4 Q$, where Q has no root in $[q_4^-, q_4^+]$ and $Q(q_4^+) < 0$ (so $H_f = g_4 Q \geq 0$ on $[q_4, q_4^+]$ with equality only at q_4), or $g_4 \nmid H_f$, and H_f has no root in $[q_4^-, q_4^+]$ and $H_f(q_4^-) > 0$. Since g_4 is irreducible, $H_f(q_4) = 0$ iff $g_4 \mid H_f$. The lists of functions with $H_f \equiv 0$ and with $g_4 \mid H_f$ are compared with the truth tables of the OR functions. As a check of (4.5): $H_{\mathrm{OR}_{\{1,2,3,4\}}} = 12(1-q)^4 - 16(1-q)^6 = -4(1-q)^4 g_4(q)$. □

Remark 4.8. Lemma 4.6 on $[q_4, q_3]$ and Lemma 4.7 are the cases $n = 3, 4$ of RQ-C's result C6 ($R_n(q) = 2\tau\sqrt{\max_{k\leq n} k(1-\bar{q})^{2k-2}}$ for $n \leq 7$, audited VALID as A.5, A.5b). Our check is independent of it. Lemma 4.7 is false for $q < q_4$, where $(e_1 + \cdots + e_4)/2$ gives $T_4 > T$; this is the only place where the lower end q_4 of Theorem 4 enters the proof.

4.4 Moments of the remainder

Lemma 4.9 (cumulants)**.** *Let $w = u^2 + v^2$ and $d = u - v$. The cumulants of χ are $\kappa_1 = 0$, $\kappa_2 = 1$ and $\kappa_j = d^{[j \text{ odd}]} G_j(w)$ for $3 \leq j \leq 10$, where*

$$G_3 = 1, \qquad G_4 = w - 4,$$
$$G_5 = w - 10, \qquad G_6 = w^2 - 26w + 64,$$
$$G_7 = w^2 - 56w + 244, \qquad G_8 = w^3 - 120w^2 + 1188w - 2176,$$
$$G_9 = w^3 - 246w^2 + 4044w - 11080, \qquad G_{10} = w^4 - 502w^3 + 14604w^2 - 86728w + 126976.$$

Proof. By (4.1), $m_k = \mathbb{E}\chi^k = qu^k + (1-q)(-v)^k = (u^k + (-1)^k u^{2-k})/(1+u^2)$. The cumulants are determined by the recursion $\kappa_n = m_n - \sum_{k=1}^{n-1} \binom{n-1}{k-1} \kappa_k m_{n-k}$. For example $m_3 = u - v$, $m_4 = w - 1$, so $\kappa_3 = d$ and $\kappa_4 = m_4 - 3 = w - 4$. The identities for $j \leq 10$ are verified symbolically (sympy, part A1 of the verifier: the difference of the two sides simplifies to 0 as a rational function of u). □

Lemma 4.10 (moments from cumulants)**.** *Let $M = \sum \beta_i \chi_i$ (finite sum) with $\sum \beta_i^2 = 1$ and power sums $p_j = \sum_i \beta_i^j$. Then M has cumulants $K_1 = 0$, $K_2 = 1$, $K_j = \kappa_j p_j$, and $\mathbb{E}M^n = \mu_n(K_3, \ldots, K_n)$ for $n \leq 10$, where $\mu_0 = 1$ and*

$$\mu_n = \sum_{k=2}^{n} \binom{n-1}{k-1} K_k \, \mu_{n-k} \qquad (K_2 = 1).$$

Each μ_n is a polynomial in $K_3, \ldots, K_{10}$ with nonnegative integer coefficients; we write $\mu_n = \sum_e N_n(e) \prod_{j=3}^{10} K_j^{e_j}$ over exponent vectors $e = (e_3, \ldots, e_{10})$. The term with $e = 0$ is the Gaussian moment: $N_n(0) = (n-1)!!$ for even n and 0 for odd n.

Proof. Cumulants of independent sums add and $K_j(\beta\chi) = \beta^j \kappa_j$, so $K_j(M) = \kappa_j p_j$, with $K_1 = 0$ and $K_2 = \sum \beta_i^2 = 1$. The recursion is the moment–cumulant relation $m_n = \sum_{k=1}^{n} \binom{n-1}{k-1} K_k m_{n-k}$ with $K_1 = 0$. The value at $K_3 = \cdots = K_{10} = 0$ is the n-th moment of a standard Gaussian. (Part A2 of the verifier checks the recursion against the Gaussian moments and against $\mathbb{E}\chi^n$ at $u = \frac{5}{2}$ for $n \leq 10$.) □

Lemma 4.11 (power sums)**.** *Let* $\sum \beta_i^2 = 1$*,* $\max|\beta_i| \le m \le 1$ *and* $\rho = \sqrt{p_4}$*. Then* $0 \le \rho \le m$*,* $|p_3| \le \rho$*,* $|p_j| \le m^{j-4}\rho^2$ *for* $5 \le j \le 10$*, and* $p_j \ge \rho^{j-2}$ *for even* $j \ge 4$*.*

Proof. $p_4 \le m^2 \sum \beta_i^2 = m^2$. Cauchy–Schwarz gives $p_3^2 = (\sum \beta_i \beta_i^2)^2 \le p_2 p_4 = p_4$. For $j \ge 5$, $|p_j| \le \sum |\beta_i|^{j-4}\beta_i^4 \le m^{j-4} p_4$. For even $j \ge 4$, Jensen's inequality for the probability weights β_i^2 and the convex function $x \mapsto x^{(j-2)/2}$ gives $p_j = \sum \beta_i^2 (\beta_i^2)^{(j-2)/2} \ge (\sum \beta_i^2 \beta_i^2)^{(j-2)/2} = \rho^{j-2}$. □

Lemma 4.12 (sign information)**.** *Let* $\sum \beta_i^2 = 1$*,* $m = \max|\beta_i|$*, and suppose* $\beta_{i_0} = -m$ *for some* i_0*. If* $m \ge m_c \in (0,1]$*, then* $p_3 \le \varphi(m_c) := -m_c^3 + (1-m_c^2)^{3/2}$*. Moreover* $\varphi(m) < 0$ *iff* $2m^2 > 1$*.*

Proof. For $i \ne i_0$, $|\beta_i| \le (\sum_{i \ne i_0} \beta_i^2)^{1/2} = \sqrt{1-m^2}$. Hence $p_3 = -m^3 + \sum_{i \ne i_0} \beta_i^3 \le -m^3 + \sqrt{1-m^2} \sum_{i \ne i_0} \beta_i^2 = \varphi(m)$, and $\varphi'(m) = -3m^2 - 3m\sqrt{1-m^2} \le 0$. Finally $\varphi(m) < 0$ iff $(1-m^2)^{3/2} < m^3$ iff $1 - m^2 < m^2$. □

Cumulant enclosures. For $1 \le u_1 \le u \le u_2$: $d = u - 1/u$ and $w = u^2 + u^{-2}$ are increasing and $d \ge 0$, so $d \in [d^-, d^+] = [u_1 - \frac{1}{u_1}, u_2 - \frac{1}{u_2}]$ and $w \in [w^-, w^+] = [u_1^2 + u_1^{-2}, u_2^2 + u_2^{-2}]$. Let $[G_j^-, G_j^+]$ be the exact range of the polynomial G_j on $[w^-, w^+]$ (computed by isolating the real roots of G_j' by Sturm sequences and bisection). Then $\kappa_j \in [\kappa_j^-, \kappa_j^+]$, where this is $[G_j^-, G_j^+]$ for even j and the interval product $[d^-, d^+] \cdot [G_j^-, G_j^+]$ for odd j.

Definition 4.13 (objective bound)**.** Let $D \le 10$, $c = (c_0, \dots, c_D) \in \mathbb{Q}^{D+1}$, $1 < u_1 < u_2$ rationals, $m^* \in (0,1]$, $p^* < 0$ optional, and Θ a target. Put $L_e = \sum_n c_n N_n(e)$ and $A = L_0 = \sum_{n \text{ even}} c_n (n-1)!!$. For every $e \ne 0$ with $L_e \ne 0$ let $[C_e^-, C_e^+]$ be the interval product $L_e \prod_j [\kappa_j^-, \kappa_j^+]^{e_j}$, and put

$$u_e = e_3 + 2\sum_{j \ge 4} e_j, \qquad U_e = \prod_{j \ge 5} (m^*)^{(j-4)e_j}.$$

Call e *even* if e_j is even for every odd j. For even e let $(\ell_e, l_e) = (0,0)$ if $e_j > 0$ for some odd j, and $(\ell_e, l_e) = (1, \sum_{j \text{ even}} (j-2)e_j)$ otherwise. Define the term bounds

(T0) if p^* is given, $e = (1, 0, \dots, 0)$ (i.e. the monomial p_3) and $C_e^- \ge 0$: replace A by $A + C_e^- p^*$, and $b_e = 0$;

(T1) otherwise, if e is not even: $b_e(\rho) = \max(|C_e^-|, |C_e^+|)\, U_e\, \rho^{u_e}$;

(T2) if e is even and $C_e^+ \le 0$: $b_e(\rho) = C_e^+\, \ell_e\, \rho^{l_e}$;

(T3) if e is even and $C_e^+ > 0$: $b_e(\rho) = C_e^+\, U_e\, \rho^{u_e}$.

We say that c *satisfies the objective bound for* $(u_1, u_2, m^*, p^*, \Theta)$ if $h(\rho) = \Theta - A - \sum_e b_e(\rho) > 0$ for all $\rho \in [0, m^*]$.

Lemma 4.14 (expectation bound)**.** *Suppose* c *satisfies the objective bound for* $(u_1, u_2, m^*, p^*, \Theta)$ *and let* $P(y) = \sum_n c_n y^n$*. Then* $\mathbb{E}P(M) < \Theta$ *for every* $u \in [u_1, u_2]$ *and every* $M = \sum \beta_i \chi_i$ *with* $\sum \beta_i^2 = 1$*,* $\max|\beta_i| \le m^*$ *and, if* p^* *is given,* $p_3 \le p^*$*.*

Proof. By Lemma 4.10, $\mathbb{E}P(M) = \sum_n c_n \mu_n = L_0 + \sum_{e \ne 0} C_e p^e$ with $C_e = L_e \prod_j \kappa_j^{e_j} \in [C_e^-, C_e^+]$ and $p^e = \prod_j p_j^{e_j}$. Let $\rho = \sqrt{p_4} \in [0, m^*]$. By Lemma 4.11, $|p^e| \le \rho^{e_3} (\rho^2)^{e_4} \prod_{j \ge 5} (m^{*\,j-4} \rho^2)^{e_j} = U_e \rho^{u_e}$; if e is even then $p^e \ge 0$ (odd power sums appear to even powers, and $p_j \ge 0$ for even j); and if moreover $e_j = 0$ for all odd j, then $p^e \ge \prod_{j \text{ even}} \rho^{(j-2)e_j} = \rho^{l_e}$. Hence: in case (T0), $p_3 \le p^* < 0$ and $C_e \ge C_e^- \ge 0$ give $C_e p_3 \le C_e p^* \le C_e^- p^*$; in case (T1), $C_e p^e \le |C_e||p^e| \le b_e(\rho)$; in case (T2), $C_e \le C_e^+ \le 0$ and $p^e \ge \ell_e \rho^{l_e} \ge 0$ give $C_e p^e \le C_e^+ p^e \le C_e^+ \ell_e \rho^{l_e}$; in case (T3), $p^e \ge 0$ gives $C_e p^e \le C_e^+ p^e \le C_e^+ U_e \rho^{u_e}$. Summing, $\mathbb{E}P(M) \le \Theta - h(\rho) < \Theta$. □

4.5 The one-coordinate route ($a_1 \le \frac{7}{20}$)

Here we split off only $a = a_1$: $L = a\chi_1 + b_1 M_1$ with $b_1 = \sqrt{1-a^2}$ and $M_1 = \sum_{i\ge 2}(\alpha_i/b_1)\chi_i$, whose coefficients are at most $\min(1, a/b_1)$ in absolute value. For $y \in \mathbb{R}$,

$$\mathbb{E}|a\chi + y| = 2\tau a + 2R_a(y) - (1-2q)y, \qquad R_a(y) = \max\{0,\ (1-q)(y-av),\ q(-y-au)\}$$

(BF3, Lemma 9.4; Lemma 3 of `MAIN_RESULT`, audited VALID). Indeed $\mathbb{E}|a\chi+y| = q|au+y| + (1-q)|y-av|$ equals $2\tau a - (1-2q)y$ for $-au \le y \le av$ (using $qau = (1-q)av = \tau a$), y for $y > av$, and $-y$ for $y < -au$, and so does the right-hand side. Conditioning on M_1 and using $\mathbb{E}M_1 = 0$,

$$\mathbb{E}|L| = 2\tau a + 2\mathbb{E}R_a(b_1 M_1), \qquad \text{so} \qquad \mathbb{E}|L| < T \iff \mathbb{E}R_a(b_1 M_1) < \tau\big(\sqrt{3}(1-q)^2 - a\big).$$

A *cell* is $[u_1, u_2] \times [\underline{a}, \overline{a}]$ with rationals $1 < u_1 < u_2$ and $0 \le \underline{a} < \overline{a} \le A_S$. Let $\bar{b}$ be a rational upper bound of $\sqrt{1-\underline{a}^2}$, $\bar{m} = \min\{1, \overline{a}/\beta\}$ with β a rational lower bound of $\sqrt{1-\overline{a}^2}$, and

$$\bar{\ell}_1(y) = \frac{u_2^2}{1+u_2^2}\Big(\bar{b}y - \frac{\underline{a}}{u_2}\Big), \quad \bar{\ell}_2(y) = \frac{1}{1+u_1^2}\big(-\bar{b}y - \underline{a}u_1\big), \quad \Theta_1 = \tau(u_2)\Big(S_3\Big(\frac{u_1^2}{1+u_1^2}\Big)^2 - \overline{a}\Big).$$

A *cell certificate* is $c \in \mathbb{Q}^{D+1}$, $D \le 10$, with $P(y) = \sum c_n y^n$ such that (V1) $P > 0$, (V2) $P > \bar{\ell}_1$, (V3) $P > \bar{\ell}_2$ on $\mathbb{R}$, and (V4) c satisfies the objective bound for $(u_1, u_2, \bar{m}, -, \Theta_1)$.

Lemma 4.15. *If a cell with $u_1 \ge U_-$ has a certificate, then $\mathbb{E}|L| < T$ for every $u \in [u_1, u_2]$ and every unit α with $\underline{a} \le \max_i |\alpha_i| \le \overline{a}$.*

Proof. For $u \in [u_1, u_2]$, $a \in [\underline{a}, \overline{a}]$ and $b_1 = \sqrt{1-a^2}$ we have $R_a(b_1 y) = \max\{0, \ell_1, \ell_2\}$ with $\ell_1 = \frac{u^2}{1+u^2}(b_1 y - \frac{a}{u})$ and $\ell_2 = \frac{1}{1+u^2}(-b_1 y - au)$. If $\ell_1(y) > 0$ then $y > 0$ and $0 < b_1 y - \frac{a}{u} \le \bar{b}y - \frac{\underline{a}}{u_2}$, and $\frac{u^2}{1+u^2} \le \frac{u_2^2}{1+u_2^2}$, so $\ell_1(y) \le \bar{\ell}_1(y)$. If $\ell_2(y) > 0$ then $y < 0$ and $0 < -b_1 y - au \le -\bar{b}y - \underline{a}u_1$, and $\frac{1}{1+u^2} \le \frac{1}{1+u_1^2}$, so $\ell_2(y) \le \bar{\ell}_2(y)$. So by (V1)–(V3), $R_a(b_1 y) < P(y)$ for all y, and $\mathbb{E}R_a(b_1 M_1) \le \mathbb{E}P(M_1)$. Since $a/\sqrt{1-a^2}$ is increasing, the coefficients of M_1 are at most $\bar{m}$ in absolute value. By Lemma 4.14, $\mathbb{E}P(M_1) < \Theta_1$. Finally $\Theta_1 \le \tau(u)(\sqrt{3}(1-q)^2 - a)$, because $\tau(u) \ge \tau(u_2)$, $(1-q)^2 \ge (\frac{u_1^2}{1+u_1^2})^2$, $S_3 < \sqrt{3}$, $a \le \overline{a}$, and the bracket is positive: $S_3(\frac{u_1^2}{1+u_1^2})^2 \ge S_3(\frac{144}{169})^2 > 1.25 > \frac{7}{20} \ge \overline{a}$ (the verifier also asserts $\Theta_1 > 0$ for every cell). □

4.6 The two-coordinate route: vertex certificates

4.6.1 The functions F_x and the patches

Let $k \in \{2, 3\}$ and a sign vector $\sigma \in \{1, -1\}^k$ with $\sigma_1 = 1$. For $x \in \mathbb{R}^{k+1}$ and $y \in \mathbb{R}$ put

$$F_x(y) = \mathbb{E}\Big|\sum_{i=1}^{k} \sigma_i x_i \chi_i + x_{k+1}\, y\Big|,$$

where $\chi_1, \dots, \chi_k$ are i.i.d. normalised q-biased bits. We use $\sigma = (1, s)$ for $k = 2$ and $\sigma = (1, s, s_3)$ for $k = 3$.

Lemma 4.16. *For fixed q and y, the map $x \mapsto F_x(y)$ is convex and positively homogeneous of degree one. Consequently, if $x = \sum_l \nu_l V_l$ with $\nu_l \ge 0$, then $F_x(y) \le \sum_l \nu_l F_{V_l}(y)$.*

Proof. $F_x(y)$ is the expectation of the absolute value of a linear function of x, i.e. a seminorm of x. A seminorm N satisfies $N(\sum \nu_l V_l) \le \sum \nu_l N(V_l)$ for $\nu_l \ge 0$. □

The *patches* are the maps

$$p_2(t,r) = \big(rc(t),\, rd(t),\, \sqrt{1-r^2}\big), \qquad p_3(t,r,m) = \big(rc(t),\, rd(t),\, \sqrt{1-r^2}\,m,\, \sqrt{1-r^2}\sqrt{1-m^2}\big),$$

for $t \in [0,1]$, $r, m \in [0,1]$. Their values are unit vectors with nonnegative entries.

Lemma 4.17 (conditional expectation)**.** *At a point with $r < 1$, $\mathbb{E}|L| = \mathbb{E}F_{p_2(t,r)}(M)$ with $\sigma = (1, s)$, where the expectation on the right is over M (independent of χ_1, χ_2). If moreover $\beta_{i_0} = s_3 m$ with $m = \max|\beta_i| < 1$ and $s_3 \in \{1, -1\}$, let $M' = \sum_{i \ge 3,\, i \ne i_0} \beta'_i \chi_i$ with $\beta'_i = \beta_i/\sqrt{1-m^2}$. Then $\sum \beta'^2_i = 1$, $\max|\beta'_i| \le \min(1, m/\sqrt{1-m^2})$, M' is independent of $(\chi_1, \chi_2, \chi_{i_0})$ and $\mathbb{E}|L| = \mathbb{E}F_{p_3(t,r,m)}(M')$ with $\sigma = (1, s, s_3)$ (the third bit being χ_{i_0}). If $m = 1$, then $L = a_1\chi_1 + sa_2\chi_2 + s_3 b\chi_{i_0}$, and $F_{p_3(t,r,1)}(y) = \mathbb{E}|L|$ for every y.*

Proof. $L = a_1\chi_1 + sa_2\chi_2 + bM$ and $(a_1, a_2, b) = p_2(t,r)$; condition on M. In the second case $L = a_1\chi_1 + sa_2\chi_2 + s_3 bm\chi_{i_0} + b\sqrt{1-m^2}M'$ and $(a_1, a_2, bm, b\sqrt{1-m^2}) = p_3(t,r,m)$; $\sum_{i \ne i_0} \beta_i^2 = 1 - m^2$ and $|\beta_i| \le m$, and also $|\beta'_i| \le 1$. If $m = 1$ the last entry of p_3 is 0. □

4.6.2 Vertex sets and the cone lemma

Definition 4.18 (vertex set)**.** Let $X = \prod_{i=1}^k [\xi_i^-, \xi_i^+]$ be a box of patch parameters ((t,r) for $k = 2$, (t,r,m) for $k = 3$) and $p = p_k$. A *vertex set for X* is a vector $n_0 \in \mathbb{Q}^{k+1}$ and 2^k vectors $V_\epsilon \in \mathbb{Q}^{k+1}$, indexed by $\epsilon \in \{0,1\}^k$, such that:

(P1) $|n_0|^2 \ge 1$ and $V_\epsilon \cdot n_0 = |n_0|^2$ for all ϵ;

(P2) (parallelepiped) $V_\epsilon = V_0 + \sum_i \epsilon_i E_i$ with $E_i = V_{e_i} - V_0$;

(P3) (facets) for each i and $\delta \in \{0,1\}$ the 2^{k-1} vertices with $\epsilon_i = \delta$ span a linear subspace of dimension k; let $h_{i,\delta}$ be a normal vector of it, oriented so that $h_{i,\delta} \cdot \bar{c} > 0$ for the centre $\bar{c} = V_0 + \frac{1}{2}\sum_i E_i$ (and $h_{i,\delta} \cdot \bar{c} \ne 0$ is required);

(P4) (enclosure) $h_{i,\delta} \cdot p(\xi) \ge 0$ for all i, δ and all $\xi \in X$.

Lemma 4.19 (cone lemma)**.** *Let $(n_0, (V_\epsilon))$ be a vertex set for X. Then for every $\xi \in X$ there are $\nu_\epsilon \ge 0$ with $p(\xi) = \sum_\epsilon \nu_\epsilon V_\epsilon$ and $\sum_\epsilon \nu_\epsilon \le 1/|n_0| \le 1$.*

Proof. First, $V_0, E_1, \dots, E_k$ is a basis of $\mathbb{R}^{k+1}$. Indeed $E_i \cdot n_0 = 0$ by (P1) and $V_0 \cdot n_0 = |n_0|^2 \ne 0$, so $V_0 \notin \operatorname{span}\{E_i\}$. By (P2) the face $\{\epsilon_i = 0\}$ spans $S_i = \operatorname{span}(V_0, \{E_j\}_{j \ne i})$, which has dimension k by (P3); hence the k vectors $V_0, \{E_j\}_{j \ne i}$ are linearly independent. Moreover $\bar{c} - V_0 - \frac{1}{2}\sum_{j \ne i} E_j = \frac{1}{2}E_i$ and $h_{i,0} \cdot \bar{c} \ne 0$ with $h_{i,0} \perp S_i$, so $E_i \notin S_i$. Thus the $k+1$ vectors are independent.

Let $z \in \mathbb{R}^{k+1}$ with $h_{i,\delta} \cdot z \ge 0$ for all i, δ, and write $z = \lambda V_0 + \sum_i \mu_i E_i$. Since $h_{i,0} \perp S_i$, $h_{i,0} \cdot z = \mu_i\, h_{i,0} \cdot E_i$, and $h_{i,0} \cdot \bar{c} = \frac{1}{2} h_{i,0} \cdot E_i > 0$; so $\mu_i \ge 0$. The face $\{\epsilon_i = 1\}$ spans $\operatorname{span}(V_0 + E_i, \{E_j\}_{j \ne i})$, so $h_{i,1} \cdot E_j = 0$ ($j \ne i$) and $h_{i,1} \cdot V_0 = -h_{i,1} \cdot E_i$; then $h_{i,1} \cdot \bar{c} = -\frac{1}{2} h_{i,1} \cdot E_i > 0$, so $h_{i,1} \cdot V_0 > 0$, and $h_{i,1} \cdot z = (\lambda - \mu_i)\, h_{i,1} \cdot V_0$; so $\mu_i \le \lambda$. If $\lambda = 0$ then $z = 0$. Otherwise $z/\lambda = V_0 + \sum_i \theta_i E_i$ with $\theta_i = \mu_i/\lambda \in [0,1]$, which is a point of the parallelepiped $\operatorname{conv}\{V_\epsilon\}$, i.e. a convex combination $\sum \omega_\epsilon V_\epsilon$ (take $\omega_\epsilon = \prod_i \theta_i^{\epsilon_i}(1-\theta_i)^{1-\epsilon_i}$). So $z = \sum \nu_\epsilon V_\epsilon$ with $\nu = \lambda\omega \ge 0$ and $\sum \nu_\epsilon = \lambda$. Finally $z \cdot n_0 = \lambda |n_0|^2$, so $\lambda = z \cdot n_0/|n_0|^2 \le |z|/|n_0|$.

By (P4), $z = p(\xi)$ satisfies the hypothesis, and $|p(\xi)| = 1$. □

4.6.3 Vertex envelopes and vertex certificates

Fix a u-interval $[u_1, u_2]$ with $u_1 > 1$. For a vertex $V \in \mathbb{Q}^{k+1}$ let $\gamma = (\sigma_1 V_1, \dots, \sigma_k V_k)$ and $b_V = V_{k+1}$. The atoms of $\sum_i \gamma_i \chi_i$ are indexed by $\omega \in \{u, -v\}^k$, with probability $\pi_\omega = \prod_i q^{[\omega_i = u]}(1-q)^{[\omega_i = -v]}$ and value $y_\omega = \sum_i \gamma_i \omega_i$, and by (4.1)

$$\pi_\omega y_\omega = \tau \sum_i \gamma_i \, (\pm 1)_i \prod_{l \neq i} q^{[\omega_l = u]}(1-q)^{[\omega_l = -v]}, \qquad (\pm 1)_i = +1 \text{ if } \omega_i = u, \ -1 \text{ otherwise.}$$

Using $q \in [\frac{1}{1+u_2^2}, \frac{1}{1+u_1^2}]$, $1-q \in [\frac{u_1^2}{1+u_1^2}, \frac{u_2^2}{1+u_2^2}]$ and $\tau \in [\tau(u_2), \tau(u_1)]$, interval arithmetic gives rational enclosures $\pi_\omega y_\omega \in [\eta_\omega^-, \eta_\omega^+]$ and $\pi_\omega \in [\pi_\omega^-, \pi_\omega^+]$, valid for all $u \in [u_1, u_2]$. Put $[\beta_\omega^-, \beta_\omega^+] = [\min(\pi_\omega^- b_V, \pi_\omega^+ b_V), \max(\pi_\omega^- b_V, \pi_\omega^+ b_V)]$.

Definition 4.20 (vertex envelope)**.** $\Phi_V(y) = \sum_\omega \max(\eta_\omega^+ + \beta_\omega^+ y, \ -\eta_\omega^- - \beta_\omega^- y)$ for $y \geq 0$, and $\Phi_V(y) = \sum_\omega \max(\eta_\omega^+ + \beta_\omega^- y, \ -\eta_\omega^- - \beta_\omega^+ y)$ for $y < 0$.

Lemma 4.21 (envelope)**.** *$F_V(y) \leq \Phi_V(y)$ for all $y \in \mathbb{R}$ and all $u \in [u_1, u_2]$. On each closed half-line, Φ_V is continuous and piecewise linear, with breakpoints among the points where the two lines of one summand cross.*

Proof. $F_V(y) = \sum_\omega \pi_\omega |y_\omega + b_V y| = \sum_\omega |\pi_\omega y_\omega + \pi_\omega b_V \, y|$ and $|z| = \max(z, -z)$. For $y \geq 0$: $\pi_\omega y_\omega + \pi_\omega b_V y \leq \eta_\omega^+ + \beta_\omega^+ y$ and $-\pi_\omega y_\omega - \pi_\omega b_V y \leq -\eta_\omega^- - \beta_\omega^- y$, since $\pi_\omega b_V \in [\beta_\omega^-, \beta_\omega^+]$ (whatever the sign of b_V). For $y < 0$ the roles of $\beta^\pm$ are exchanged. □

Definition 4.22 (vertex certificate)**.** Let X be a parameter box, σ a sign vector, $[u_1, u_2]$ a u-interval, $m^* \in (0, 1]$ a cap, and $p^* < 0$ optional. A *vertex certificate for* $(X, \sigma, [u_1, u_2], m^*, p^*)$ is a vertex set $(n_0, (V_\epsilon))$ for X and coefficient vectors $c^{(\epsilon)} \in \mathbb{Q}^{D+1}$, $D \leq 10$, with $P_\epsilon(y) = \sum_n c_n^{(\epsilon)} y^n$, such that for every ϵ: (W1) $P_\epsilon(y) > \Phi_{V_\epsilon}(y)$ for all $y \in \mathbb{R}$; and (W2) $c^{(\epsilon)}$ satisfies the objective bound for $(u_1, u_2, m^*, p^*, T^-(u_1, u_2))$.

(W1) is checked as follows: on each half-line, Φ_V coincides on each interval between consecutive breakpoints with one line $\lambda_0 + \lambda_1 y$ (one choice of line per summand); for every such line, $P_\epsilon - \lambda_0 - \lambda_1 y$ is shown to be positive on all of $\mathbb{R}$ by Sturm sequences.

Lemma 4.23 (vertex certificate lemma)**.** *Let a vertex certificate for $(X, \sigma, [u_1, u_2], m^*, p^*)$ be given. Let $\mathcal{Z}$ be the class of random variables $Z = \sum \beta_i \chi_i'$ (finite sums of i.i.d. copies of χ, independent of $\chi_1, \dots, \chi_k$) with $\sum \beta_i^2 = 1$, $\max |\beta_i| \leq m^*$ and, if p^* is given, $p_3 \leq p^*$. Then for every $u \in [u_1, u_2]$, every $\xi \in X$ and every $Z \in \mathcal{Z}$,*

$$\mathbb{E} F_{p(\xi)}(Z) < T^-(u_1, u_2) \leq T(u).$$

Proof. By Lemma 4.19, $p(\xi) = \sum \nu_\epsilon V_\epsilon$ with $\nu \geq 0$ and $\sum \nu_\epsilon \leq 1$. By Lemmas 4.16 and 4.21 and (W1), for every y, $F_{p(\xi)}(y) \leq \sum_\epsilon \nu_\epsilon F_{V_\epsilon}(y) \leq \sum_\epsilon \nu_\epsilon P_\epsilon(y)$. Taking expectations over Z, $\mathbb{E} F_{p(\xi)}(Z) \leq \sum_\epsilon \nu_\epsilon \mathbb{E} P_\epsilon(Z)$. By (W1) and Lemma 4.21, $\mathbb{E} P_\epsilon(Z) > \mathbb{E} F_{V_\epsilon}(Z) \geq 0$, and by (W2) and Lemma 4.14, $\mathbb{E} P_\epsilon(Z) < T^-$. Since $\sum \nu_\epsilon \leq 1$ and $\max_\epsilon \mathbb{E} P_\epsilon(Z) \geq 0$, $\sum_\epsilon \nu_\epsilon \mathbb{E} P_\epsilon(Z) \leq \max_\epsilon \mathbb{E} P_\epsilon(Z) < T^-$. Finally $T^- \leq T(u)$ by (4.2). □

Remark 4.24. Compared with the box certificates of Theorem 3, the envelope here is taken only over u (the vertices are fixed vectors), and the parameters (t, r) enter only through the cone condition (P4). So the loss of the certificate is the variation of F over a polytope that hugs the patch, rather than a first-order interval overestimate in (t, r); in our runs this allowed boxes about eight times larger in t and r near q_4.

4.6.4 Boxes

A *box* is $B = [u_1, u_2] \times [t_1, t_2] \times [r_1, r_2]$ with rationals $1 < u_1 < u_2$, $0 \le t_1 < t_2 \le 1$, $0 \le r_1 < r_2 \le 1$, together with a sign s. Let b^- be a rational lower bound of $\sqrt{1 - r_2^2}$ ($b^- = 0$ if $r_2 = 1$), and define $\bar{m}(B) = 1$ if $b^- = 0$ or $r_2 d(t_2) \ge b^-$, and $\bar{m}(B) = r_2 d(t_2)/b^-$ otherwise. Then $\bar{m}(B) \in (0, 1]$ and $m \le \min(1, a_2/b) \le \bar{m}(B)$ at every point of B with $r < 1$, because $a_2 = rd(t) \le r_2 d(t_2)$ and $b \ge b^-$. A box of kind lpv carries a vertex certificate for $([t_1, t_2] \times [r_1, r_2], (1, s), [u_1, u_2], \bar{m}(B), -)$.

Lemma 4.25. *At every point of an lpv box with $r < 1$, $\mathbb{E}|L| < T$.*

Proof. By Lemma 4.17, $\mathbb{E}|L| = \mathbb{E}F_{p_2(t,r)}(M)$, and $M \in \mathcal{Z}$ since $m \le \bar{m}(B)$. Apply Lemma 4.23. □

4.7 Near $(e_1 + e_2)/\sqrt{2}$: the near-circle lemma

Lemma 4.26 (tail bound)**.** *Let $y \in \mathbb{R}$, $b \ge 0$ and let Z be a random variable with $\mathbb{E}Z = 0$ and $\mathbb{E}Z^4 < \infty$. Then*

$$\mathbb{E}|y + bZ| \le |y| + \min\Big(b\,\mathbb{E}|Z|,\ \frac{27}{128}\,\frac{b^4 \mathbb{E}Z^4}{|y|^3}\Big),$$

where for $y = 0$ the minimum is read as its first entry. The same convention is used below whenever this bound is applied at a point where $y = 0$.

Proof. The first bound is the triangle inequality. For the second ($y \ne 0$), $|y + z| - |y| - \operatorname{sgn}(y) z = 2(-\operatorname{sgn}(y) z - |y|)_+ \le 2(|z| - |y|)_+$, and $\mathbb{E}[\operatorname{sgn}(y) bZ] = 0$. For $x \ge 0$ and $\eta > 0$, $(x - \eta)_+ \le \frac{27}{256} x^4/\eta^3$: the maximum of $(x - \eta)/x^4$ over $x > \eta$ is at $x = \frac{4}{3}\eta$ and equals $\frac{27}{256}\eta^{-3}$. Hence $\mathbb{E}|y + bZ| - |y| \le 2 \cdot \frac{27}{256}\, b^4 \mathbb{E}Z^4/|y|^3$. □

Lemma 4.27 (near-circle tests)**.** *Let B be a box with $r_1 > 0$. Let y_j ($j = 1, \dots, 4$) be the atoms of $c\chi_1 + sd\chi_2$, so that the atoms of $a_1\chi_1 + sa_2\chi_2$ are ry_j. Let $\eta_j \ge 0$ be a lower bound of $|y_j|$ on B, p_j^+ an upper bound of p_j, b^+ an upper bound of $\sqrt{1 - r_1^2}$, and $E_4 = 3 + \max(0, w^+ - 4)\,\bar{m}(B)^2$. Let $T^- = T^-(u_1, u_2)$.*

(A) If all $\eta_j > 0$ and $\frac{27}{128} E_4 (b^+)^2 \frac{1 + r_2}{r_1^3} \sum_j p_j^+ \eta_j^{-3} < T^-$, then $\mathbb{E}|L| < T$ at every point of B with $r < 1$ and $q \le q_3$.

(B) Let G^+ be an upper bound of $\mathbb{E}|c\chi_1 + sd\chi_2| = \tau \sum_j |g_j|$ on B with $G^+ \le T^-$, and $e_j^+ = \min\big(b^+, \frac{27}{128}(b^+)^4 E_4/(r_1^3 \eta_j^3)\big)$ ($e_j^+ = b^+$ if $\eta_j = 0$). If $\sum_j p_j^+ e_j^+ < T^-(1 - r_2) + r_1(T^- - G^+)$, then $\mathbb{E}|L| < T$ at every point of B with $r < 1$.

Proof. At a point of B with $r < 1$, condition on (χ_1, χ_2) and apply Lemma 4.26 with $Z = M$. Here $\mathbb{E}M^4 = 3 + \kappa_4 p_4 \le E_4$ by Lemma 4.10, since $p_4 \le m^2 \le \bar{m}(B)^2$ and $\kappa_4 = w - 4 \le w^+ - 4$; also $\mathbb{E}|M| \le 1$. This gives $\mathbb{E}|L| \le rG + \sum_j p_j e_j$, where $G = \mathbb{E}|c\chi_1 + sd\chi_2|$ and $e_j = \min(b, \frac{27}{128} b^4 E_4/(r^3 |y_j|^3))$. (A) By Lemma 4.5 ($q \le q_3$), $G \le T$. Since $1 - r = b^2/(1 + r)$ and $b > 0$, $\sum_j p_j e_j \le \frac{27}{128} \frac{b^4 E_4}{r^3} \sum_j \frac{p_j}{|y_j|^3} \le b^2 \cdot \frac{27}{128} E_4 (b^+)^2 \frac{1}{r_1^3} \sum_j \frac{p_j^+}{\eta_j^3} < \frac{b^2 T^-}{1 + r_2} \le T(1 - r)$. So $\mathbb{E}|L| < rT + T(1 - r) = T$. (B) $\mathbb{E}|L| \le rG^+ + \sum_j p_j^+ e_j^+ < rG^+ + T^-(1 - r_2) + r_1(T^- - G^+) \le rG^+ + T^-(1 - r) + r(T^- - G^+) = T^- \le T$, using $r_1 \le r \le r_2$ and $T^- - G^+ \ge 0$. □

Boxes of kind ncA pass test (A) or test (B). In our range $q < q_3$, so (A) applies.

4.8 Near the extremisers: the m-split

The extremiser $(e_1+e_2+e_3)/\sqrt{3}$ is, in our coordinates, the point $a_1 = a_2 = b = 1/\sqrt{3}$ with $M = \chi_3$, so $m = 1$; at q_4 the second extremiser $(e_1 + e_2 + e_3 + e_4)/2$ is the point $a_1 = a_2 = \frac{1}{2}$, $b = \frac{1}{\sqrt{2}}$ with $M = (\chi_3 + \chi_4)/\sqrt{2}$, so $m = \frac{1}{\sqrt{2}}$. In both cases equality holds, so no certificate with a strict bound can contain these points. As in Theorem 3 we split according to $m = \max_{i\ge 3} |\beta_i|$ and the sign of a largest remaining coefficient; in addition, after removing a coefficient $+m$, we split the new remainder once more.

4.8.1 Three split coordinates

Lemma 4.28 (three-coordinate near-sphere bound)**.** *Consider a point with $r < 1$ and suppose $\beta_{i_0} = +m$ for some $i_0 \ge 3$. Put $a_3 = bm$, $b' = b\sqrt{1-m^2}$, $Y = a_1\chi_1 + sa_2\chi_2 + a_3\chi_{i_0}$ with atoms y_j and probabilities p_j $(j = 1, \dots, 8)$, $r' = \sqrt{a_1^2 + a_2^2 + a_3^2} = \sqrt{1 - b'^2}$ and $E_4' = 3 + \max(0, \kappa_4)$. Then*

$$\mathbb{E}|L| \le \mathbb{E}|Y| + \sum_j p_j \min\Big(b',\ \frac{27}{128}\frac{b'^4 E_4'}{|y_j|^3}\Big).$$

If moreover $q \in [q_U, q_L]$, all $y_j \ne 0$ and $\frac{27}{128}E_4'\, b'^2(1 + r')\sum_j p_j|y_j|^{-3} < T$, then $\mathbb{E}|L| < T$ if $b' > 0$, and if $b' = 0$ then $\mathbb{E}|L| = G_3(a_1, sa_2, a_3) \le T$.

Proof. If $m = 1$ then $b' = 0$ and $L = Y$. Otherwise $L = Y + b'M'$ with M' as in Lemma 4.17. Then M' is independent of Y, $\sum \beta_i'^2 = 1$ and $\sum \beta_i'^4 \le 1$, so $\mathbb{E}M'^4 = 3 + \kappa_4 \sum \beta_i'^4 \le E_4'$ by Lemma 4.10. Conditioning on $(\chi_1, \chi_2, \chi_{i_0})$ and applying Lemma 4.26 with $Z = M'$ (and $\mathbb{E}|M'| \le 1$) gives the first bound. By Lemma 4.6, $\mathbb{E}|Y| = G_3(a_1, sa_2, a_3) \le Tr'$. If $b' > 0$, the hypothesis and $1 - r' = b'^2/(1 + r')$ give $\sum_j p_j \frac{27}{128}\frac{b'^4 E_4'}{|y_j|^3} < T\frac{b'^2}{1+r'} = T(1 - r')$, hence $\mathbb{E}|L| < Tr' + T(1 - r') = T$. □

Piece tests (A3), (B3). Let B be a box with $b^- > 0$ and $[m_1, m_2] \subset (0, 1]$. On $B \times [m_1, m_2]$ we enclose $a_1 = rc(t)$, $a_2 = rd(t)$, $a_3 = bm \in [b^-m_1, b^+m_2]$, $b'^2 \le (b'^2)^+ := (b^+)^2(1 - m_1^2)$, and $r' \le r'^+ := \min\big(1, \sqrt{1 - (b^-)^2(1 - m_2^2)}\big)$ (recall $r'^2 = 1 - b^2(1 - m^2)$). The atoms $y_j = a_1x_{j1} + sa_2x_{j2} + a_3x_{j3}$ $(x \in \{u, -v\}^3)$ and the products $p_jy_j = \tau\sum_i(\pm a_i)\prod_{l\ne i}\Pr[x_{jl}]$ (by $qu = (1-q)v = \tau$) are enclosed in interval arithmetic. Let η_j be a lower bound of $|y_j|$, p_j^+ an upper bound of p_j, and $E_4'^+ = 3 + \max(0, w^+ - 4)$. The piece passes

- test (A3) if all $\eta_j > 0$ and $\frac{27}{128}E_4'^+(b'^2)^+(1 + r'^+)\sum_j p_j^+\eta_j^{-3} < T^-(u_1, u_2)$;
- test (B3) if $\sum_j \big(|p_jy_j|^+ + p_j^+ \min\big(b'^+, \frac{27}{128}((b'^2)^+)^2E_4'^+/\eta_j^3\big)\big) < T^-(u_1, u_2)$, where $|p_jy_j|^+$ is an upper bound of $|p_jy_j|$, b'^+ an upper bound of $\sqrt{(b'^2)^+}$, and the second entry of the minimum is omitted if $\eta_j = 0$.

By Lemma 4.28, if a piece passes (A3), then at every point of B with $q \in [q_U, q_L]$ and every remainder with $\beta_{i_0} = +m$, $m \in [m_1, m_2]$, we have $\mathbb{E}|L| < T$ if $b' > 0$, and $\mathbb{E}|L| = G_3(a_1, sa_2, bm) \le T$ if $b' = 0$. If it passes (B3), then $\mathbb{E}|L| < T$ by the first bound of Lemma 4.28 alone ($\mathbb{E}|Y| = \sum_j |p_jy_j|$).

Definition 4.29 (pieces of type TC and SG)**.** Let B be a box with $b^- > 0$, sign s, and $[m_1, m_2] \subset (0, 1]$.

- A TC piece with sign $s_3 \in \{1,-1\}$ is a rational cap $\kappa \in (0,1]$ with $\kappa \geq \min(1, m_2/\sqrt{1-m_2^2})$ (that is, $\kappa = 1$, or $m_2 < 1$ and $\kappa^2(1-m_2^2) \geq m_2^2$), and a vertex certificate for $([t_1,t_2] \times [r_1,r_2] \times [m_1,m_2], (1,s,s_3), [u_1,u_2], \kappa, -)$.
- An SG piece (for $s_3 = -1$) is a rational p^* with $2m_1^2 > 1$ and $\varphi(m_1) \leq p^* < 0$, a rational cap $\kappa \in (0,1]$ with $\kappa \geq \min(m_2, \bar{m}(B))$, and a vertex certificate for $([t_1,t_2] \times [r_1,r_2], (1,s), [u_1,u_2], \kappa, p^*)$.

Lemma 4.30. *Let B be a box with $b^- > 0$ and consider a point of B with $r < 1$ whose remainder has $m = \max_{i \geq 3} |\beta_i| \in [m_1, m_2]$ and $\beta_{i_0} = s_3 m$.*

(i) If $[m_1, m_2]$ carries a TC piece with sign s_3, then $\mathbb{E}|L| < T$.

(ii) If $s_3 = -1$ and $[m_1, m_2]$ carries an SG piece, then $\mathbb{E}|L| < T$.

Proof. (i) If $m < 1$, Lemma 4.17 gives $\mathbb{E}|L| = \mathbb{E}F_{p_3(t,r,m)}(M')$ with $\max|\beta_i'| \leq \min(1, m/\sqrt{1-m^2}) \leq \min(1, m_2/\sqrt{1-m_2^2}) \leq \kappa$, so $M' \in \mathcal{Z}$ and Lemma 4.23 applies. If $m = 1$, then $m_2 = 1$ and $\kappa = 1$, and $\mathbb{E}|L| = F_{p_3(t,r,1)}(y)$ for every y; taking $Z = \chi'$ (one bit, an element of $\mathcal{Z}$), $\mathbb{E}|L| = \mathbb{E}F_{p_3(t,r,1)}(Z) < T$ by Lemma 4.23. (ii) By Lemma 4.12 with $m_c = m_1$, $p_3 \leq \varphi(m_1) \leq p^*$. Also $m \leq m_2$ and $m \leq \bar{m}(B)$, so $m \leq \kappa$. Thus $M \in \mathcal{Z}$, and Lemmas 4.17 and 4.23 give $\mathbb{E}|L| < T$. □

4.8.2 Four split coordinates

Lemma 4.31 (four-coordinate near-sphere bound)**.** *Consider a point with $r < 1$, $\beta_{i_0} = +m$ with $m < 1$, and let M' be as in Lemma 4.17. Suppose $\beta'_{i_1} = +m'$ for some i_1, where $m' = \max|\beta_i'|$. Put $a_3 = bm$, $b' = b\sqrt{1-m^2}$, $a_4 = b'm'$, $b'' = b'\sqrt{1-m'^2}$, $Y_4 = a_1\chi_1 + sa_2\chi_2 + a_3\chi_{i_0} + a_4\chi_{i_1}$ with atoms y_j and probabilities p_j ($j = 1,\dots,16$), $r'' = \sqrt{a_1^2+a_2^2+a_3^2+a_4^2} = \sqrt{1-b''^2}$ and $E_4' = 3 + \max(0,\kappa_4)$. Then*

$$\mathbb{E}|L| \leq \mathbb{E}|Y_4| + \sum_j p_j \min\Big(b'',\ \frac{27}{128}\frac{b''^4 E_4'}{|y_j|^3}\Big).$$

If moreover $q \in [q_4, q_L]$, all $y_j \neq 0$ and $\frac{27}{128}E_4' b''^2(1+r'')\sum_j p_j|y_j|^{-3} < T$, then $\mathbb{E}|L| < T$ if $b'' > 0$, and if $b'' = 0$ then $\mathbb{E}|L| = G_4(a_1, sa_2, a_3, a_4) \leq T$.

Proof. If $m' = 1$ then $b'' = 0$ and $L = Y_4$. Otherwise $L = Y_4 + b''M''$ with $M'' = \sum_{i \neq i_0, i_1} \beta_i'' \chi_i$, $\beta_i'' = \beta_i'/\sqrt{1-m'^2}$, which is independent of Y_4 and has $\sum \beta_i''^2 = 1$, so $\mathbb{E}M''^4 \leq E_4'$ and $\mathbb{E}|M''| \leq 1$. Conditioning on the four bits of Y_4 and applying Lemma 4.26 gives the first bound. By Lemma 4.7, $\mathbb{E}|Y_4| = G_4(a_1, sa_2, a_3, a_4) \leq Tr''$. If $b'' > 0$, the hypothesis and $1 - r'' = b''^2/(1+r'')$ give $\mathbb{E}|L| < Tr'' + T(1-r'') = T$. □

Piece tests (A4), (B4). Let B be a box with $b^- > 0$, $[m_1,m_2] \subset (0,1]$ and $[n_1,n_2] \subset (0,1]$. On $B \times [m_1,m_2] \times [n_1,n_2]$ (with $m \in [m_1,m_2]$, $m < 1$, and $m' \in [n_1,n_2]$) we enclose a_1, a_2, a_3 as in (A3), $b'^2 \in [(b^-)^2(1-m_2^2), (b^+)^2(1-m_1^2)]$, b' by the square roots of these bounds, $a_4 = b'm' \in [b'^- n_1, b'^+ n_2]$, $b''^2 \leq (b''^2)^+ := (b'^2)^+(1-n_1^2)$, and $r'' \leq r''^+ := \min\big(1, \sqrt{1-(b'^2)^-(1-n_2^2)}\big)$. The 16 atoms and the products $p_j y_j$ are enclosed as in (A3). The piece passes

- test (A4) if all $\eta_j > 0$ and $\frac{27}{128}E_4'^+(b''^2)^+(1+r''^+)\sum_j p_j^+ \eta_j^{-3} < T^-(u_1,u_2)$;
- test (B4) if $\sum_j \big(|p_j y_j|^+ + p_j^+ \min\big(b''^+, \frac{27}{128}((b''^2)^+)^2 E_4'^+/\eta_j^3\big)\big) < T^-(u_1,u_2)$.

Definition 4.32 (pieces of type TCS)**.** Let B be a box with $b^- > 0$, sign s, and $[m_1, m_2] \subset (0, 1]$. A TCS piece is: a rational cap $\kappa \in (0, 1]$ with $\kappa \geq \min(1, m_2/\sqrt{1 - m_2^2})$; a rational $m_c' \in (0, 1]$ and a rational p'^* with $2m_c'^2 > 1$ and $\varphi(m_c') \leq p'^* < 0$; a vertex certificate $\mathcal{C}'$ for $(X_3, (1, s, 1), [u_1, u_2], m_c', -)$ and a vertex certificate $\mathcal{C}''$ for $(X_3, (1, s, 1), [u_1, u_2], \kappa, p'^*)$, where $X_3 = [t_1, t_2] \times [r_1, r_2] \times [m_1, m_2]$; and sub-pieces $[n_1, n_2] \subset (0, 1]$, each passing (A4) or (B4) (on $B \times [m_1, m_2] \times [n_1, n_2]$), whose union contains $[m_c', \kappa]$.

Lemma 4.33. *Let $[m_1, m_2]$ carry a TCS piece for B. At every point of B with $r < 1$ and $q \in [q_4, q_L]$ whose remainder has $\beta_{i_0} = +m$, $m = \max|\beta_i| \in [m_1, m_2]$, we have $\mathbb{E}|L| \leq T$. Equality forces $q = q_4$, $s = 1$ and $\alpha = \frac{1}{2}(e_1 + e_2 + e_{i_0} + e_{i_1})$ for some $i_1 \notin \{1, 2, i_0\}$.*

Proof. If $m = 1$: $\mathbb{E}|L| = F_{p_3(t,r,1)}(y)$ for every y; take $Z = N^{-1/2}(\chi_1' + \cdots + \chi_N')$ with $N^{-1/2} \leq m_c'$, which belongs to the class of $\mathcal{C}'$. Lemma 4.23 gives $\mathbb{E}|L| = \mathbb{E}F_{p_3(t,r,1)}(Z) < T$.

Now let $m < 1$ and $m' = \max|\beta_i'|$. By Lemma 4.17,

$$\mathbb{E}|L| = \mathbb{E}F_{p_3(t,r,m)}(M'), \qquad m' \leq \min\left(1, m/\sqrt{1 - m^2}\right) \leq \kappa.$$

- If $m' \leq m_c'$: M' is in the class of $\mathcal{C}'$, and Lemma 4.23 gives $\mathbb{E}|L| < T$.
- If $m' \geq m_c'$ and $\beta_{i_1}' = -m'$ for some i_1: by Lemma 4.12, $p_3(M') \leq \varphi(m_c') \leq p'^*$, and $m' \leq \kappa$, so M' is in the class of $\mathcal{C}''$, and $\mathbb{E}|L| < T$.
- Otherwise $\beta_{i_1}' = +m'$ for some i_1, with $m' \in [m_c', \kappa]$, so m' lies in a sub-piece $[n_1, n_2]$, and $m \in [m_1, m_2]$. If the sub-piece passes (B4), Lemma 4.31 (first bound) gives $\mathbb{E}|L| < T$. If it passes (A4), Lemma 4.31 gives $\mathbb{E}|L| < T$ when $b'' > 0$, and $\mathbb{E}|L| = G_4(c) \leq T$ with $c = (a_1, sa_2, a_3, a_4)$, $|c| = 1$, when $b'' = 0$.

In the last case with $b'' = 0$ (so $m' = 1$ and $a_4 = b' > 0$, as $m < 1$), equality means $G_4(c) = T|c|$. All entries of c are nonzero ($a_1 > 0$, $a_2 \geq |\alpha_{i_0}| = a_3 = bm > 0$, $a_4 > 0$), so by Lemma 4.7, $q = q_4$ and c is a positive multiple of $\pm(1, 1, 1, 1)$; since $a_1, a_3, a_4 > 0$, $s = 1$ and $a_1 = a_2 = a_3 = a_4 = \frac{1}{2}$. □

4.8.3 The m-split boxes

Definition 4.34 (m-split box)**.** An m-split box (kind ms5) is a box B with sign s, $r_2 < 1$ (so $b^- > 0$) and $u_1 \geq 2$, together with: a rational m_c with $0 < m_c < \min(1, \bar{m}(B))$; a vertex certificate $\mathcal{C}^{(1)}$ for $([t_1, t_2] \times [r_1, r_2], (1, s), [u_1, u_2], m_c, -)$; *plus pieces* $[m_1, m_2]$, each of type (A3), (B3), TC with $s_3 = 1$, or TCS, whose union contains $[m_c, \min(1, \bar{m}(B))]$; and *minus pieces* $[m_1, m_2]$, each of type SG or TC with $s_3 = -1$, whose union contains $[m_c, \min(1, \bar{m}(B))]$.

Lemma 4.35 (m-split lemma)**.** *Let B be an m-split box. At every point of B with $r < 1$ and $q \in [q_4, q_L]$ we have $\mathbb{E}|L| \leq T$. Equality forces $s = 1$ and either $\alpha = \frac{1}{\sqrt{3}}(e_1 + e_2 + e_{i_0})$, or $q = q_4$ and $\alpha = \frac{1}{2}(e_1 + e_2 + e_{i_0} + e_{i_1})$.*

Proof. Recall $m \leq \min(1, \bar{m}(B))$. If $m \leq m_c$, use $\mathcal{C}^{(1)}$: by Lemmas 4.17 and 4.23, $\mathbb{E}|L| < T$. Let $m \geq m_c$. If $\beta_{i_0} = +m$ for some i_0, then m lies in a plus piece. A piece (B3) or TC gives $\mathbb{E}|L| < T$ (Lemma 4.30(i) for TC). A piece (A3) gives $\mathbb{E}|L| < T$ if $b' > 0$, and $\mathbb{E}|L| = G_3(a_1, sa_2, b) \leq T$ if $b' = 0$ (i.e. $m = 1$); in the latter case equality forces, by Lemma 4.6 ($q \in [q_4, q_L] \subset [q_U, q_L]$), (a_1, sa_2, b) to be a positive multiple of $\pm(1, 1, 1)$, so $s = 1$, $a_1 = a_2 = b = \frac{1}{\sqrt{3}}$ and $\beta = e_{i_0}$. A piece TCS gives $\mathbb{E}|L| \leq T$ with equality only as in Lemma 4.33. Otherwise the maximum m is attained only by negative coefficients, $\beta_{i_0} = -m$, and m lies in a minus piece; Lemma 4.30 gives $\mathbb{E}|L| < T$. □

4.9 Computer verification

All scripts and outputs are in the repository (`scripts/`, `outputs/`). Floating point (HiGHS linear programming via scipy, numpy) is used only to *find* certificates. Every *verification* is exact or uses outward-rounded interval arithmetic.

4.9.1 Data

The list of data files is `outputs/k3b_manifest.json` ($U_- = \frac{12}{5}$, $U_+ = \frac{127123}{50000}$, $T_8 = \frac{41422}{100000}$, $A_S = \frac{7}{20}$); md5 sums are in `outputs/k3b_MD5SUMS.txt`.

- One-coordinate cells: `outputs/k3b/one_0.json`, `one_1.json`, `one_2.json` ($u \in [\frac{12}{5}, \frac{247}{100}]$, $[\frac{247}{100}, \frac{127}{50}]$, $[\frac{127}{50}, U_+]$; 98, 126 and 64 cells, all of degree 10), covering $u \in [U_-, U_+]$ and $a \in [0, \frac{7}{20}]$. Widths: $6.2 \cdot 10^{-4}$ to 0.0175 in u, 0.022 to 0.044 in a.
- Two-coordinate boxes: `outputs/k3b/b5_i_s.json` for $i = 0, \dots, 14$ and $s = \pm 1$ (u-slabs $[\frac{12}{5}, \frac{241}{100}]$, $[\frac{241}{100}, \frac{121}{50}]$, $\dots$, $[\frac{253}{100}, \frac{127}{50}]$, $[\frac{127}{50}, U_+]$), except that the slab $[\frac{253}{100}, \frac{127}{50}]$ with $s = +1$ is split into four files `outputs/k3b/sub13_a_1.json`, $\dots$, `sub13_d_1.json` of width $\frac{1}{400}$. For each sign the boxes cover $[U_-, U_+] \times [0, T_8] \times [\frac{7}{20}, 1]$. Each file records $K = 3$ and $A_S = \frac{7}{20}$. Each box record has its kind and data: lpv (n_0, the vertices and one coefficient vector per vertex), ncA, and ms5 (m_c, $\mathcal{C}^{(1)}$ and the pieces, with their vertex certificates, caps, p^* values and sub-pieces).

sign	lpv	ncA	ms5	small	total
$s = +1$	626	13	302	0	941
$s = -1$	480	0	0	0	480

Table 4.1: Two-coordinate boxes for Theorem 4. Widths range from $2.46 \cdot 10^{-3}$ to 0.01 in u, from $3.2 \cdot 10^{-3}$ to 0.104 in t and from $5.1 \cdot 10^{-3}$ to 0.081 in r. The ms5 boxes use $m_c \in \{\frac{2}{5}, \frac{9}{20}, \frac{1}{2}, \frac{3}{5}, \frac{3}{4}, \frac{4}{5}, \frac{17}{20}, \frac{9}{10}\}$ and carry 1 350 pieces: plus pieces 123 (A3), 689 TC, 210 TCS (all with $m_c' = \frac{17}{20}$, with 301 sub-pieces, all of type (A4)); minus pieces 146 SG, 182 TC. In total there are 2 845 vertex certificates (1 106 lpv, 302 $\mathcal{C}^{(1)}$, 871 TC, 146 SG, 2×210 in TCS) with 16 544 vertices; all their polynomials have degree 6.

4.9.2 Generation

`scripts/run_k3b.sh` runs the 36 jobs of `outputs/k3b/jobs.txt` (about 40 minutes with 8 parallel jobs). A two-coordinate job is `RQ_K=3 RQ_AS=7/20 python3 cover5.py u1 u2 s out.json 1 4 8 16`: it bisects $[u_1, u_2] \times [0, T_8] \times [\frac{7}{20}, 1]$ adaptively (4 initial t-intervals, 8 r-intervals, depth ≤ 16) and on each box tries, in order: small; the near-circle tests (`nearcircle.py`); a vertex certificate (`cert5.py`); from depth 2 on, the m-split (`cover5.try_ms5`, with `nsphere3.py` and `cert4.py` for the near-sphere pieces). A vertex set is built from the centre of the parameter box: n_0 is a rational approximation of the patch point at the centre with $|n_0| \ge 1$, the polytope is a box in an exactly orthogonal rational basis of $n_0^\perp$ that contains the gnomonic projection of a 7^k grid of the patch with a relative margin (4%, enlarged to 10% and 25% if the cone check fails), and its corners are the vertices. The coefficient vectors come from a discretised moment linear program (as in Theorem 3, with the objective of Definition 4.13), rounded to rationals and repaired; (W1), (W2)

and (P1)–(P4) are checked exactly before a record is accepted. One-coordinate cells come from `cover_lp10.py` (degree-ten certificates, `tenmom.py`). No box or cell failed.

4.9.3 Independent verification

`python3 verify_k3b.py` re-checks everything from the data files (93 seconds on 8 cores; output `outputs/verify_k3b_ABCDEFG.txt`, all parts pass). It shares no code with the generators (`cert2c`, `cert4`, `cert5`, `cover5`, `cover_lp10`, `tenmom`, `nsphere3`, `nearcircle`, `exactcert`, `fourbit`); it reuses only the Sturm-sequence, integer-square-root and tiling helpers of `verify_all.py` (the verifier of Theorem 1, audited in A.6). Its parts:

A. Symbolic identities (sympy). Lemma 4.9: the cumulants of χ, computed from its moments, are $d^{[j \text{ odd}]}G_j(w)$ for $j = 3, \dots, 10$. Lemma 4.10: the recursion reproduces the Gaussian moments, and also the moments of χ at $u = \frac{5}{2}$, up to order ten.

B. Coverage (exact). $\sqrt{5} < U_- \le \frac{12}{5}$; $U_+ \ge u_4$, checked as $U_+^2 > 3$ and $(U_+^2 - 3)^2 \ge 12$; and $T_8 \ge \sqrt{2} - 1$. The 288 cells tile $[U_-, U_+] \times [0, \frac{7}{20}]$. For each sign the boxes tile $[U_-, U_+] \times [0, T_8] \times [\frac{7}{20}, 1]$: they lie in the region, have pairwise disjoint interiors and total volume equal to the volume of the region (a closed subset of full measure is dense, so it is the whole region). Every file has $K = 3$ and $A_S = \frac{7}{20}$.

C. One-coordinate cells: (V1)–(V3) by Sturm sequences; $\Theta_1 > 0$; (V4) strictly (Definition 4.13 re-implemented: the polynomials μ_n from the recursion, the monomial bounds, and a Sturm count of the roots of h on $[0, \bar{m}]$ together with $h(0) > 0$).

D. Vertex certificates (all lpv records and all certificates inside ms5 records: $\mathcal{C}^{(1)}$, TC, SG, and $\mathcal{C}'$, $\mathcal{C}''$ of TCS): (P1) and (P2) exactly; (P3) by exact Gaussian elimination (rank k of each facet, normal vector, orientation by the centre); (P4) by interval bisection of the parameter box against the $2k$ facet normals, with componentwise rational enclosures of the patch (monotonicity of c, d and outward square-root bounds), failing if any sub-box has a facet value with negative upper bound or if more than 20 000 sub-boxes are needed; (W1) on every linear piece of every vertex envelope (Definition 4.20, recomputed from the atom enclosures over $[u_1, u_2]$); (W2) strictly with the target $T^-(u_1, u_2)$. The caps are taken from the structure: $\bar{m}(B)$ (recomputed exactly) for lpv, m_c for $\mathcal{C}^{(1)}$, the recorded cap $\kappa \in (0, 1]$ for TC, SG and $\mathcal{C}''$, and m_c' for $\mathcal{C}'$; the p^* values are those of the records.

E. Near-circle boxes: mpmath interval arithmetic (120 bits), tests (A)/(B) strictly, with T^- computed from an interval enclosure of $\sqrt{3}$.

F. m-split structure: $r_2 < 1$, $u_1 \ge 2$, $0 < m_c < \min(1, \bar{m}(B))$; the plus pieces and the minus pieces each cover $[m_c, \min(1, \bar{m}(B))]$; each (A3)/(B3) piece passes its test (mpmath, 120 bits, strict); TC caps satisfy $\kappa = 1$ or $\kappa^2(1 - m_2^2) \ge m_2^2$; SG: $0 < m_1 \le 1$, $2m_1^2 > 1$, $p^* < 0$, $p^* \ge \varphi(m_1)$ (checked as $p^* + m_1^3 \ge 0$ and $(p^* + m_1^3)^2 \ge (1 - m_1^2)^3$) and $\kappa \ge \min(m_2, \bar{m}(B))$; TCS: the cap condition, the same φ check for (m_c', p'^*), the sub-pieces cover $[m_c', \kappa]$, and each sub-piece passes (A4) or (B4) (mpmath, strict).

G. The claims (C1) and (C2) of Lemmas 4.6 and 4.7, for all 2^8 and all 2^{16} functions, exactly as described there, on $[q_U, q_L]$ and $[q_4, q_L]$ with $q_L = 1/(1 + U_-^2)$, including the lists of equality cases ($\pm$OR of three bits identically; $\pm$OR of four bits at q_4 only).

The generator side has its own exact check of the four-bit lemma (`scripts/fourbit.py`, same result).

Negative tests. `python3 break_tests_k3b.py` corrupts random samples of records and runs the check functions of `verify_k3b.py` on them (output `outputs/break_tests_k3b.txt`). Every corruption below is rejected in every case: on 40 lpv boxes, lowering the constant term of one vertex polynomial by $\frac{1}{20}$ (domination fails), raising it by 1 (the objective bound fails), shrinking the polytope by 10% about its centre (the cone check fails) and moving one vertex by 10^{-6} (the hyperplane/parallelepiped check fails); on 25 ms5 boxes, removing one plus piece or one minus piece, and lowering the top of the pieces by $\frac{1}{100}$ (coverage fails); replacing a TC/TCS cap by m_2 (43 cases; the cap check fails); lowering an SG value p^* by $\frac{1}{100}$ below $\varphi(m_1)$ (25 cases); widening an (A4) sub-piece from $[n_1, n_2]$ to $[n_1/2, n_2]$ (25 cases; the near-sphere test fails); lowering the constant term of a TC vertex polynomial by $\frac{1}{20}$ (20 cases); removing one box from the tiling, for each sign. A separate sanity check (not a corruption) confirms on the same 40 boxes that the recomputed cap $\bar{m}(B)$ is at least $\min(1, a_2/b)$ on the box.

4.9.4 Reproducing

```
pip install numpy scipy sympy mpmath
cd scripts
python3 verify_k3b.py          # parts A-G, about 2 minutes on 8 cores
python3 break_tests_k3b.py     # negative tests
python3 fourbit.py             # four-bit lemma (generator-side check)
bash run_k3b.sh                # regenerate all data (about 40 minutes, 8 jobs)
```

4.10 Proof of Theorem 4

(a) By Lemma 4.3 let $q \in [q_4, q_L]$, i.e. $u \in [U_-, u_4] \subseteq [U_-, U_+]$; then $q < q_3$ and $q \in [q_U, q_L]$. Reduce α as in Section 4.2.3.

(1) $a_1 = 1$: $\alpha = e_1$ and $\mathbb{E}|L| = 2\tau < T$ (Lemma 4.4(ii)).

(2) $a_1 \le \frac{7}{20}$: (u, a_1) lies in a cell, and Lemma 4.15 gives $\mathbb{E}|L| < T$.

(3) $a_1 > \frac{7}{20}$ and $r = 1$: $L = a_1\chi_1 + sa_2\chi_2$, and Lemma 4.5 ($q < q_3$) gives $\mathbb{E}|L| < T$.

(4) $a_1 > \frac{7}{20}$ and $r < 1$: (u, t, r) lies in a box of the cover for the sign s (part B), since $t \in [0, \sqrt{2} - 1] \subseteq [0, T_8]$ and $r \ge a_1 > \frac{7}{20}$. If it is lpv, Lemma 4.25 gives $\mathbb{E}|L| < T$. If it is ncA, Lemma 4.27 gives $\mathbb{E}|L| < T$ ($q < q_3$). If it is ms5, Lemma 4.35 gives $\mathbb{E}|L| \le T$. (There are no small boxes.)

So $\mathbb{E}|L| \le T$ always, and $(e_1 + e_2 + e_3)/\sqrt{3}$ attains T (Lemma 4.4, $q < \frac{1}{3}$). Hence $R(q) = T(q)$. For $q \in [1 - q_L, 1 - q_4]$ use Lemma 4.3: $R(q) = R(1 - q) = 2\sqrt{3}\, q^2\tau$.

(b) Equality can occur only in the ms5 case of (4). By Lemma 4.35, after the reduction, $\alpha = \frac{1}{\sqrt{3}}(e_1 + e_2 + e_{i_0})$, or $q = q_4$ and $\alpha = \frac{1}{2}(e_1 + e_2 + e_{i_0} + e_{i_1})$. Undoing the reduction (global sign and permutation) gives the list in (b). Conversely, each listed vector attains T at the stated q: $(e_i + e_j + e_k)/\sqrt{3}$ gives T for $q < \frac{1}{3}$, and $(e_i + e_j + e_k + e_l)/2$ gives $T_4 = T$ at q_4 (Lemma 4.4). For $q \ge \frac{1}{2}$ use Lemma 4.3.

(c) For $q < q_4 < \frac{1}{4}$, $R(q) \ge \mathbb{E}|\chi_1 + \cdots + \chi_4|/2 = T_4(q) > T(q)$ by Lemma 4.4 and (iii). □

4.11 Remarks

1. **The $k = 3$ regime is closed.** With Theorem 3, $R(q) = 2\sqrt{3}(1-q)^2\sqrt{q(1-q)}$ holds exactly on $[q_4, q_3]$, which is the largest possible interval (Corollary 4.1). Both ends are ties: at q_3 with $(e_1 + e_2)/\sqrt{2}$, at q_4 with $(e_1 + \cdots + e_4)/2$. Corollary 4.2 confirms the conjecture $R(q) = 2\tau \max_k \sqrt{k}\,\hat{q}^{\,k-1}$ (BF3, Stone; RQ-C's Conjecture S) on $[q_4, 1-q_4]$. Its next regime, $k = 4$ on $[q_5, q_4]$ with q_5 defined by $2\sqrt{5}(1-q)^4 = 4(1-q)^3$, is not treated here.

2. **Where the method is tight.** The m-split is used in 302 of the 941 boxes with $s = +1$. TCS pieces, the only place where the four-bit lemma is used, occur in 93 boxes, all with $u_1 \geq 2.48$; the slabs between 2.52 and 2.54 are the most expensive part of the cover. For $u > u_4$ the four-bit lemma fails, and test (A4) would claim too much; this is why the boxes with $u > u_4$ (up to U_+) are used only for $u \leq u_4$, and why Lemma 4.33 and Lemma 4.35 are stated for $q \geq q_4$.

3. **Ten moments.** The one-coordinate cells need degree ten: as $a_1 \to 0$ the remainder becomes Gaussian, and the six-moment Gaussian value 0.888074 (resp. eight-moment value 0.886410) exceeds $T(q_4) \approx 0.884970$, while the ten-moment value is 0.856068 (floating-point linear programs over polynomial majorants of $|y|$; numerical, used only to choose the degree). The vertex certificates of the two-coordinate route all have degree 6; the expectation bound of Definition 4.13 is used for them as well.

4. **Status.** Audited VALID by RQ-AUD (A.18, 2026-10-22 12:41 UTC), with no fix, and refereed VALID by RQ-REF1 (2026-10-22 15:38 UTC), with no fixes; after the referee's report only this item was changed. The computer steps have been run twice (generator and independent verifier), the verifier rejects corrupted data (negative tests above), and the referee re-did every computer step with its own exact programs.

Chapter 5

The $k = 4$ regime of $R(q)$: $R(q) = 4(1-q)^3\sqrt{q(1-q)}$ exactly for $1 - \frac{2}{\sqrt{5}} \le q \le 1 - \frac{\sqrt{3}}{2}$

Source: RQ-A, `MAIN_RESULT_K4.tex` (md5 `01d916597bedd8f9ee25a40a66f33768`), by "RQ-A (R(q) attack)", dated 22 October 2026. Its main result is Theorem 5 (claim MAIN-5), which keeps this name.

Refereed version: md5 `158934d2ea9f18df4f717b169dc52292`, the file in commit `6ecd564`. The source differs from it only in the status item of the closing remarks, which now records the referee's verdict.

Audit: A.25, VALID and NEW (22 October, 16:53 UTC), no fix to the mathematics. Its two text remarks r1–r2 were applied at 17:47 UTC. RQ-A's text corrections c1–c2 (20:51 UTC) were confirmed in the addendum of 21:19 UTC; A.25 stays VALID.

Referee: RQ-REF2, VALID, no fixes (report `REFEREE.md`, md5 `bd18da81...`, written at 01:05 UTC on 23 October).

Use in the Main Theorem: Step 1. Corollary 5.2 combines Theorems 1–5 into the formula on $[q_5, 1-q_5]$.

Transcription: the whole paper, with the mechanical changes of Appendix C: labels prefixed by `ch05:`, numbers n become $5.n$, the title becomes the chapter title, no table of contents, the abstract as a quoted block. No editorial footnotes.

Abstract of the source paper. For $q \in (0,1)$ let $\chi_1, \chi_2, \dots$ be i.i.d. normalised q-biased bits and let $R(q)$ be the supremum of $\mathbb{E}|\sum \alpha_i \chi_i|$ over unit vectors α. We prove that $R(q) = 4(1-q)^3\sqrt{q(1-q)}$ for every $q \in [q_5, q_4]$, where $q_5 = 1 - 2/\sqrt{5} \approx 0.105573$ and $q_4 = 1 - \sqrt{3}/2 \approx 0.133975$ (and the mirror statement on $[1-q_4, 1-q_5]$). We also determine all extremisers: $(e_i + e_j + e_k + e_l)/2$; at $q = q_4$ also $(e_i + e_j + e_k)/\sqrt{3}$; and at $q = q_5$ also $(e_{i_1} + \cdots + e_{i_5})/\sqrt{5}$. The interval $[q_5, q_4]$ is exactly the set of $q \le \frac{1}{2}$ where this formula holds. With our Theorems 1–4 we obtain $R(q) = 2\sqrt{q(1-q)}\max_{k \ge 1} \sqrt{k}\, \hat{q}^{\,k-1}$, $\hat{q} = \max(q, 1-q)$, for all $q \in [q_5, 1-q_5]$. The proof follows our Theorem 4 (`MAIN_RESULT_K3B`) with three changes: the target $4(1-q)^3\sqrt{q(1-q)}$ with $k = 4$ versions of the three- and four-bit lemmas; an exact formula for $\mathbb{E}|c \cdot \chi|$ in the region where every c_i exceeds $q\sum_j c_j$; and one more level of the m-split, which ends in a five-coordinate near-sphere bound around the third extremiser $(e_1 + \cdots + e_5)/\sqrt{5}$. The computer-assisted steps (7 261 boxes with 21 014 sets of vertex certificates, 1 268 cells, and the bit lemmas) use exact rational arithmetic and certified interval arithmetic, and an independent program repeated all of them.

5.1 Statement

Fix $q \in (0,1)$ and put

$$u = \sqrt{\tfrac{1-q}{q}}, \qquad v = \frac{1}{u}, \qquad \tau = \sqrt{q(1-q)}.$$

Let $\chi, \chi_1, \chi_2, \dots$ be i.i.d. with $\Pr[\chi = u] = q$ and $\Pr[\chi = -v] = 1-q$, so that $\mathbb{E}\chi = 0$, $\mathbb{E}\chi^2 = 1$ and $\mathbb{E}|\chi| = 2\tau$. Let

$$R(q) = \sup_{n \ge 1} \sup_{\alpha \in \mathbb{R}^n \setminus \{0\}} \frac{\mathbb{E}|\sum_{i=1}^n \alpha_i \chi_i|}{|\alpha|_2}.$$

Put

$$q_4 = 1 - \tfrac{\sqrt{3}}{2} \approx 0.133975, \qquad q_5 = 1 - \tfrac{2}{\sqrt{5}} \approx 0.105573,$$

$$T_2 = 2\sqrt{2}\,(1-q)\,\tau, \quad T_3 = 2\sqrt{3}\,(1-q)^2\,\tau, \quad T_4 = 4(1-q)^3\,\tau, \quad T_5 = 2\sqrt{5}\,(1-q)^4\,\tau.$$

Theorem 5. *(a) For every $q \in [q_5, q_4]$, every $n \ge 1$ and every $\alpha \in \mathbb{R}^n$ with $|\alpha|_2 = 1$,*

$$\mathbb{E}\Big|\sum_{i=1}^n \alpha_i \chi_i\Big| \le 4(1-q)^3\sqrt{q(1-q)}.$$

For $q \in [1-q_4, 1-q_5]$ the same holds with $1-q$ replaced by q. Consequently $R(q) = 4\max(q, 1-q)^3\sqrt{q(1-q)}$ for $q \in [q_5, q_4] \cup [1-q_4, 1-q_5]$.

(b) (Extremisers.) Let $q \in [q_5, q_4] \cup [1-q_4, 1-q_5]$. Equality in (a) holds if and only if $\alpha = \pm\frac{1}{2}(e_i + e_j + e_k + e_l)$ with i,j,k,l distinct, or $q \in \{q_4, 1-q_4\}$ and $\alpha = \pm\frac{1}{\sqrt{3}}(e_i + e_j + e_k)$ with i,j,k distinct, or $q \in \{q_5, 1-q_5\}$ and $\alpha = \pm\frac{1}{\sqrt{5}}(e_{i_1} + \cdots + e_{i_5})$ with $i_1, \dots, i_5$ distinct.

(c) (Sharpness.) $R(q) > T_4(q)$ for $q \in (0, q_5) \cup (q_4, \frac{1}{2}]$. More precisely, $R(q) \ge T_5(q) > T_4(q)$ for $q < q_5$, $R(q) \ge T_3(q) > T_4(q)$ for $q_4 < q < \frac{1}{3}$, and $R(q) \ge 2\tau > T_4(q)$ for $\frac{1}{3} \le q \le \frac{1}{2}$.

Corollary 5.1 (the whole $k = 4$ regime)**.** $\{q \in (0, \frac{1}{2}] : \ R(q) = T_4(q)\} = [q_5, q_4]$, *and* $\{q \in [\frac{1}{2}, 1) : R(q) = 4q^3\tau\} = [1-q_4, 1-q_5]$.

Proof. Theorem 5(a) and (c), and Lemma 5.3 for the mirror statement. □

Corollary 5.2. *With Theorem 4 of `MAIN_RESULT_K3B` ($R = T_3$ on $[q_4, \frac{25}{169}]$; MAIN-4, audited VALID as A.18), Theorem 1 of `MAIN_RESULT` ($R(q) = 2\tau$ on $[1-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}]$, audited VALID as A.6), Theorem 2 of `MAIN_RESULT_K2` ($R = T_2$ on $[1-\sqrt{2/3}, 1-\frac{1}{\sqrt{2}}]$, A.11, VALID) and Theorem 3 of `MAIN_RESULT_K3` ($R = T_3$ on $[\frac{25}{169}, 1-\sqrt{2/3}]$, A.14, VALID),*

$$R(q) = 2\sqrt{q(1-q)}\,\max\{1,\ \sqrt{2}\,\hat{q},\ \sqrt{3}\,\hat{q}^2,\ 2\hat{q}^3\} = 2\sqrt{q(1-q)}\,\max_{k \ge 1}\sqrt{k}\,\hat{q}^{k-1}, \qquad \hat{q} = \max(q, 1-q),$$

for all $q \in [q_5, 1-q_5] = [1-\frac{2}{\sqrt{5}}, \frac{2}{\sqrt{5}}]$.

Proof. By Lemma 5.3 let $q \le \frac{1}{2}$, so $\hat{q} = 1-q$. On $[q_4, \frac{1}{2}]$, Corollary 2 of `MAIN_RESULT_K3B` (which combines Theorems 1–4) gives $R(q) = 2\tau\max\{1, \sqrt{2}(1-q), \sqrt{3}(1-q)^2\}$; there $2(1-q)^3 \le \sqrt{3}(1-q)^2$ because $1-q \le \frac{\sqrt{3}}{2}$, so adding the entry $2\hat{q}^3$ does not change the maximum. On $[q_5, q_4]$, Theorem 5 gives $R(q) = 2\tau\cdot 2(1-q)^3$, and $2(1-q)^3$ is the largest of the four entries there: $2(1-q)^3 \ge \sqrt{3}(1-q)^2$ iff $1-q \ge \frac{\sqrt{3}}{2}$; $(1-q)^2 \ge \frac{3}{4} > \frac{1}{\sqrt{2}}$ gives $2(1-q)^3 > \sqrt{2}(1-q)$; and $2(1-q)^3 \ge 2(\frac{3}{4})^{3/2} > 1$.

This proves the first formula. For the second, let $k \geq 5$ and $1-q \leq \frac{2}{\sqrt{5}}$ (i.e. $q \geq q_5$). Then $\sqrt{k}(1-q)^{k-1} \leq 2(1-q)^3$ iff $\frac{\sqrt{k}}{2}(1-q)^{k-4} \leq 1$, and $\frac{\sqrt{k}}{2}(1-q)^{k-4} \leq (\frac{k}{4}(\frac{4}{5})^{k-4})^{1/2}$. The sequence $\frac{k}{4}(\frac{4}{5})^{k-4}$ equals 1 at $k=5$ and decreases for $k \geq 5$, since $\frac{k+1}{k} \cdot \frac{4}{5} \leq \frac{6}{5} \cdot \frac{4}{5} < 1$. So on $[q_5, \frac{1}{2}]$ the terms with $k \geq 5$ never exceed the term with $k=4$. □

Part (c) and the lower bound $R \geq T_4$ in (a) are elementary (Lemma 5.4). The content is the upper bound in (a), and (b).

Relation to Theorem 4. The proof follows `MAIN_RESULT_K3B` (Theorem 4) step by step. The changes are:

(i) the target T_4, the range $u \in [u_4, u_5]$ (Section 5.2) and the threshold $A_S = \frac{33}{100}$ of the one-coordinate route;

(ii) $k=4$ versions of the three- and four-bit lemmas ($\sum_i \Delta_i(f)^2 \leq 16(1-q)^6$ on $[q_5, q_4]$; Lemmas 5.7 and 5.8);

(iii) the *OR-region identity* (Lemma 5.6): if every c_i exceeds $q\sum_j c_j$, then $\mathbb{E}|c \cdot \chi| = 2\tau(1-q)^{n-1}\sum_i c_i$. It gives the five-coordinate near-sphere bound (Lemma 5.35) near the third extremiser $(e_1+\cdots+e_5)/\sqrt{5}$, which ties with $(e_1+\cdots+e_4)/2$ at q_5;

(iv) one more level of the m-split (Section 5.8.3): pieces of type TCN, with vertex certificates for patches with four split coordinates and an inner m-split of the second remainder;

(v) an exact check of the cone condition (P4) of the vertex sets by a chain of one-variable minima (Lemma 5.21), instead of the interval bisection used for Theorem 4.

The lemmas that are unchanged from Theorem 4 are proved again here, so that the document can be read on its own.

Conventions. $x_+ = \max(x, 0)$. All polynomials in the computer-assisted parts have rational coefficients. "Verified" means verified in exact rational arithmetic or in outward-rounded interval arithmetic, as specified in Section 5.9. For a rational $x \geq 0$ and an integer $N \geq 1$, *rational lower and upper bounds of* $\sqrt{x}$ are $\lfloor N\sqrt{x} \rfloor / N$ and $(\lfloor N\sqrt{x} \rfloor + 1)/N$ computed with integer square roots (the verifier uses $N = 10^{15}$).

5.2 Reductions

5.2.1 Symmetry and parametrisation

Lemma 5.3. *The law of $-\chi^{(q)}$ is the law of $\chi^{(1-q)}$. Hence $\mathbb{E}|\sum \alpha_i \chi_i^{(q)}| = \mathbb{E}|\sum \alpha_i \chi_i^{(1-q)}|$, $R(q) = R(1-q)$, and the extremisers for q and $1-q$ coincide.*

Proof. $-\chi^{(q)}$ takes the value $-u_q$ with probability q and v_q with probability $1-q$; since $u_{1-q} = v_q$ and $v_{1-q} = u_q$, this is the law of $\chi^{(1-q)}$. Finally $|\sum \alpha_i(-\chi_i)| = |\sum \alpha_i \chi_i|$. □

From now on $q \leq \frac{1}{2}$, i.e. $u \geq 1$, and

$$q = \frac{1}{1+u^2}, \quad 1-q = \frac{u^2}{1+u^2}, \quad v = \frac{1}{u}, \quad \tau = \frac{u}{1+u^2}, \quad qu = (1-q)v = \tau. \tag{5.1}$$

On $u \geq 1$, τ and q are decreasing and $1-q$ is increasing in u. The target is

$$T_4 = 4(1-q)^3\tau = \frac{4u^7}{(1+u^2)^4}, \qquad \frac{d}{du}\frac{u^7}{(1+u^2)^4} = \frac{u^6(7-u^2)}{(1+u^2)^5},$$

so T_4 is increasing on $[1,\sqrt{7}]$ and decreasing on $[\sqrt{7},\infty)$. Hence, for $1 \leq u_1 < u_2$ and $u \in [u_1,u_2]$,

$$T_4(u) \;\geq\; T^-(u_1,u_2) := \min\{T_4(u_1), T_4(u_2)\} : \tag{5.2}$$

if $u \leq \sqrt{7}$ then T_4 is increasing on $[u_1,u]$, and if $u \geq \sqrt{7}$ it is decreasing on $[u,u_2]$. For rational u_1,u_2 the number $T^-(u_1,u_2)$ is rational. The range $q \in [q_5,q_4]$ corresponds to $u \in [u_4,u_5]$ with

$$u_4 = \sqrt{3+2\sqrt{3}} \approx 2.5424598, \qquad u_5 = \sqrt{4+2\sqrt{5}} \approx 2.9106935,$$

because $(1-q_4)/q_4 = \frac{\sqrt{3}}{2-\sqrt{3}} = \sqrt{3}(2+\sqrt{3}) = 3+2\sqrt{3}$ and $(1-q_5)/q_5 = \frac{2}{\sqrt{5}-2} = 2(\sqrt{5}+2) = 4+2\sqrt{5}$. We fix the rationals

$$U_- = \frac{1589}{625} = 2.5424 \;\leq u_4, \qquad U_+ = \frac{29107}{10000} = 2.9107 \;\geq u_5.$$

Indeed $U_-^2 > 3$ and $(U_-^2-3)^2 \leq 12$, so $U_-^2 \leq 3+2\sqrt{3}$; and $U_+^2 > 4$ and $(U_+^2-4)^2 \geq 20$, so $U_+^2 \geq 4+2\sqrt{5}$. The computations cover $u \in [U_-,U_+]$; the theorem uses only $u \in [u_4,u_5]$. We also record that $U_- \geq 2$ and that $w_- = U_-^2/(1+U_-^2)$ (the value of $1-q$ at $u=U_-$) satisfies

$$w_-^4 \geq \tfrac{1}{2}, \qquad 2w_-^3 \geq 1 \tag{5.3}$$

(exact check; $w_- \approx 0.866025$). Since w_- is rational and $2^{1/4}, 2^{1/3}$ are irrational, both inequalities are strict, and since $1-q$ increases with u, $(1-q)^4 > \frac{1}{2}$ and $2(1-q)^3 > 1$ for all $u \geq U_-$.

5.2.2 Values of a few vectors

Lemma 5.4. *Let $k \geq 1$ and $q < 1/k$. Then $\mathbb{E}|\chi_1+\cdots+\chi_k|/\sqrt{k} = 2\sqrt{k}\,(1-q)^{k-1}\tau$. In particular $\mathbb{E}|\chi_1| = 2\tau$, and $\mathbb{E}|\chi_1+\cdots+\chi_k|/\sqrt{k} = T_k$ for $k = 2,3,4,5$ and $q < 1/k$. Moreover, for all $q \in (0,1)$:*

(i) $T_3 \leq T_4$ iff $q \leq q_4$, with equality iff $q = q_4$;

(ii) $T_5 \leq T_4$ iff $q \geq q_5$, with equality iff $q = q_5$;

(iii) for $u \geq U_-$ (in particular for $q \in [q_5,q_4]$): $2\tau < T_4$ and $T_2 < T_4$.

Proof. Let $S = \chi_1+\cdots+\chi_k$ and let $x_i = \mathbf{1}\{\chi_i = u\}$. If some $x_i = 1$ then $S \geq u-(k-1)v > 0$, because $u^2 > k-1$ is equivalent to $q < 1/k$. If all $x_i = 0$ then $S = -kv < 0$. So $|S| = fS$ with $f = 1-2\cdot\mathbf{1}\{\text{all } x_i = 0\}$. Since $\mathbb{E}\chi_i = 0$, $\mathbb{E}[f\chi_i] = -2\mathbb{E}[\chi_i\mathbf{1}\{\text{all } x = 0\}] = -2(1-q)^k(-v) = 2(1-q)^{k-1}(1-q)v = 2(1-q)^{k-1}\tau$. Summing over i gives $\mathbb{E}|S| = 2k(1-q)^{k-1}\tau$. The comparisons: (i) $2\sqrt{3}(1-q)^2 \leq 4(1-q)^3$ iff $1-q \geq \frac{\sqrt{3}}{2}$; (ii) $2\sqrt{5}(1-q)^4 \leq 4(1-q)^3$ iff $1-q \leq \frac{2}{\sqrt{5}}$; (iii) $2\tau < 4(1-q)^3\tau$ iff $2(1-q)^3 > 1$, and $2\sqrt{2}(1-q) < 4(1-q)^3$ iff $(1-q)^4 > \frac{1}{2}$; both hold for $u \geq U_-$ by (5.3). □

5.2.3 Splitting off the two largest coefficients

Let $|\alpha|_2 = 1$ and $L = \sum \alpha_i \chi_i$. Changing the sign of α and permuting coordinates does not change $\mathbb{E}|L|$. So we may assume

$$a_1 := \alpha_1 = \max_i |\alpha_i| > 0, \qquad a_2 := |\alpha_2| = \max_{i \geq 2} |\alpha_i|, \qquad |\alpha_3| \geq |\alpha_4| \geq \cdots,$$

and we put $s = \operatorname{sgn} \alpha_2 \in \{1, -1\}$ ($s = 1$ if $\alpha_2 = 0$),

$$r = \sqrt{a_1^2 + a_2^2} \in (0, 1], \qquad b = \sqrt{1 - r^2}.$$

If $r < 1$, let $\beta_i = \alpha_i / b$ for $i \geq 3$ and $M = \sum_{i \geq 3} \beta_i \chi_i$. Then

$$L = a_1 \chi_1 + s\, a_2 \chi_2 + b M, \qquad \sum_{i \geq 3} \beta_i^2 = 1, \qquad m := \max_{i \geq 3} |\beta_i| = \frac{|\alpha_3|}{b} \leq \min\Big(1, \frac{a_2}{b}\Big),$$

and M is independent of (χ_1, χ_2). We use half-angle coordinates for (a_1, a_2):

$$a_1 = r\, c(t), \quad a_2 = r\, d(t), \qquad c(t) = \frac{1 - t^2}{1 + t^2}, \quad d(t) = \frac{2t}{1 + t^2}, \qquad t = \frac{a_2}{r + a_1}.$$

Since $0 \leq a_2 \leq a_1$, the angle θ with $\tan\theta = a_2/a_1$ is in $[0, \pi/4]$ and $t = \tan(\theta/2) \in [0, \sqrt{2} - 1]$. We fix $T_8 = \frac{20711}{50000} = 0.41422 \geq \sqrt{2} - 1$ (indeed $(T_8 + 1)^2 \geq 2$). On $[0, 1]$, c is decreasing and d is increasing in t, both are ≥ 0, and $c^2 + d^2 = 1$. Thus every unit α gives a point

$$(u, t, r, s) \in [U_-, U_+] \times [0, T_8] \times (0, 1] \times \{1, -1\} \qquad (u \in [u_4, u_5]).$$

We put $A_S = \frac{33}{100}$. If $a_1 \leq A_S$ we use the one-coordinate route of Section 5.5; otherwise $r \geq a_1 > A_S$ and we use the two-coordinate route of Sections 5.6–5.8.

5.3 Exact evaluations

5.3.1 Two coordinates

Lemma 5.5 (two-coordinate value)**.** *Let $q \leq \frac{1}{2}$, $c, d \geq 0$, $s \in \{1, -1\}$, and $X = c\chi_1 + s\, d\chi_2$. List the atoms of X as $(\chi_1, \chi_2) = (u, u), (u, -v), (-v, u), (-v, -v)$, with probabilities $p = (q^2,\ q(1-q),\ q(1-q),\ (1-q)^2)$ and values x_j. Then $p_j x_j = \tau g_j$ with*

$$g = \big(q(c + sd),\ (1 - q)c - s\, q\, d,\ -q\, c + s(1 - q)d,\ -(1 - q)(c + sd)\big), \tag{5.4}$$

and

$$\mathbb{E}|X| = 2\tau \max\{c,\ d,\ [s = 1]\,(1 - q)(c + d)\}$$

(the last entry is present only for $s = 1$). Consequently $\mathbb{E}|X| \leq \max(2\tau, T_2)\sqrt{c^2 + d^2}$, and if $u \geq U_-$ and $(c, d) \neq 0$, then $\mathbb{E}|X| < T_4\sqrt{c^2 + d^2}$.

Proof. The identities $p_j x_j = \tau g_j$ follow from (5.1); for example $q(1-q)(cu - sdv) = (1-q)\tau c - q\tau sd$. Since $\mathbb{E}X = 0$, $\mathbb{E}|X| = 2\mathbb{E}X_+ = 2\tau \sum_j (g_j)_+$. For $s = 1$: $g_1 \geq 0 \geq g_4$, so $\mathbb{E}X_+/\tau = q(c + d) + ((1 - q)c - qd)_+ + ((1 - q)d - qc)_+$. If both middle terms are nonnegative this equals $(1 - q)(c + d)$, and then $(1 - q)(c + d) - c = (1 - q)d - qc \geq 0$ and similarly $\geq d$. If only the first is nonnegative it equals $q(c + d) + (1 - q)c - qd = c$, and $(1 - q)(c + d) - c = (1 - q)d - qc < 0$, while $c \geq d$

(otherwise $(1-q)d - qc \geq (1-2q)c \geq 0$). The case where only the second is nonnegative is symmetric. Both negative would give $(1-q)(c+d) < q(c+d)$, impossible for $q \leq \frac{1}{2}$ unless $c = d = 0$. In all cases $\mathbb{E}X_+/\tau = \max\{c, d, (1-q)(c+d)\}$. For $s = -1$: $g_2 \geq 0 \geq g_3$. If $c \geq d$ then $g_1 \geq 0 \geq g_4$ and $\mathbb{E}X_+/\tau = q(c-d) + (1-q)c + qd = c$. If $c < d$ then $g_1 < 0 < g_4$ and $\mathbb{E}X_+/\tau = (1-q)c + qd + (1-q)(d-c) = d$. So $\mathbb{E}X_+/\tau = \max(c, d)$.

For the bound let $\rho = \sqrt{c^2 + d^2}$. Then $\max(c, d) \leq \rho$ and $(1-q)(c+d) \leq \sqrt{2}(1-q)\rho$, so $\mathbb{E}|X| \leq \max(2\tau\rho, 2\sqrt{2}(1-q)\tau\rho) = \max(2\tau, T_2)\rho$. For $u \geq U_-$ and $\rho > 0$ this is $< T_4\rho$ by Lemma 5.4(iii). □

5.3.2 Bits, OR functions and the OR region

For $n \geq 1$, $f : \{0,1\}^n \to [-1,1]$ and $x_i = \mathbf{1}\{\chi_i = u\}$ put $\Delta_i(f) = \mathbb{E}[f \mid x_i = 1] - \mathbb{E}[f \mid x_i = 0]$, a polynomial in q. Then, by (5.1),

$$\mathbb{E}[f\chi_i] = qu\,\mathbb{E}[f \mid x_i = 1] - (1-q)v\,\mathbb{E}[f \mid x_i = 0] = \tau\,\Delta_i(f). \tag{5.5}$$

For $c \in \mathbb{R}^n$ write $G_n(c) = \mathbb{E}|c_1\chi_1 + \cdots + c_n\chi_n|$. For a set $S \subseteq \{1, \ldots, n\}$ let $\mathrm{OR}_S = 2 \cdot \mathbf{1}\{\exists i \in S : x_i = 1\} - 1$. By the computation in the proof of Lemma 5.4,

$$\Delta_i(\mathrm{OR}_S) = 2(1-q)^{|S|-1} \ (i \in S), \qquad \Delta_i(\mathrm{OR}_S) = 0 \ (i \notin S). \tag{5.6}$$

(For $i \in S$: $\mathbb{E}[\mathrm{OR}_S \mid x_i = 1] = 1$ and $\mathbb{E}[\mathrm{OR}_S \mid x_i = 0] = 1 - 2(1-q)^{|S|-1}$; for $i \notin S$, OR_S does not depend on x_i.)

Lemma 5.6 (OR-region identity)**.** *Let $n \geq 1$, $q \in (0,1)$ and $c \in \mathbb{R}^n$ with $c_i > 0$ and $c_i > q\sum_{l=1}^n c_l$ for every i. Then*

$$G_n(c) = 2\tau(1-q)^{n-1}\sum_{i=1}^n c_i \ \leq \ 2\sqrt{n}\,(1-q)^{n-1}\tau\,|c|.$$

In particular, for $n = 5$ and $q \geq q_5$: $G_5(c) \leq T_5|c| \leq T_4|c|$, and $G_5(c) = T_4|c|$ holds if and only if $q = q_5$ and $c_1 = \cdots = c_5$.

Proof. Let $S = \sum_l c_l\chi_l$. If all $x_l = 0$ then $S = -v\sum_l c_l < 0$. Otherwise pick i with $x_i = 1$. Every l with $x_l = 1$ contributes $c_l u$ instead of $-c_l v$, a gain of $c_l(u+v) > 0$, so $S \geq c_i u - v\sum_{l \neq i} c_l = c_i(u+v) - v\sum_l c_l$. By (5.1), $u + v = (1+u^2)/u = v/q$, so $S \geq \frac{v}{q}\big(c_i - q\sum_l c_l\big) > 0$. Hence $|S| = \mathrm{OR}_{\{1,\ldots,n\}} \cdot S$, and by (5.5) and (5.6), $G_n(c) = \sum_i c_i\mathbb{E}[\mathrm{OR}\,\chi_i] = \tau\sum_i c_i \cdot 2(1-q)^{n-1}$. The inequality is Cauchy–Schwarz, $\sum_i c_i \leq \sqrt{n}|c|$, with equality iff all c_i are equal. For $n = 5$ the bound is $T_5|c|$, and $T_5 \leq T_4$ for $q \geq q_5$ with equality iff $q = q_5$ (Lemma 5.4(ii)). So $G_5(c) = T_4|c|$ forces equality in both steps, i.e. $c_1 = \cdots = c_5$ and $q = q_5$; conversely these give equality. □

5.3.3 Three and four bits for $k = 4$

Lemma 5.7 (three-bit lemma for $k = 4$)**.** *Let $q \in [q_5, q_4]$ and $c \in \mathbb{R}^3$. Then $G_3(c) \leq T_4\,|c|$. For $c \neq 0$ equality holds if and only if $q = q_4$ and c is a positive multiple of $\pm(e_1 + e_2 + e_3)$.*

Lemma 5.8 (four-bit lemma for $k = 4$)**.** *Let $q \in [q_5, q_4]$ and $c \in \mathbb{R}^4$. Then $G_4(c) \leq T_4\,|c|$. For $c \neq 0$ equality holds if and only if c is a positive multiple of $\pm(e_1 + e_2 + e_3 + e_4)$, or $q = q_4$ and c is a positive multiple of $\pm(e_i + e_j + e_k)$ for distinct i, j, k.*

Proof of Lemmas 5.7 and 5.8. Let $n \in \{3,4\}$, $X = c\cdot\chi$ and $f^* = \operatorname{sgn} X$ (with $\operatorname{sgn} 0 = 1$), a function of $(x_1,\dots,x_n)$ with values ± 1. By (5.5) and Cauchy–Schwarz,

$$G_n(c) = \mathbb{E}[f^* X] = \tau \sum_i c_i \Delta_i(f^*) \le \tau|c|\,|\Delta(f^*)|.$$

For $f : \{0,1\}^n \to \{-1,1\}$ put $H_f(q) = 16(1-q)^6 - \sum_{i=1}^n \Delta_i(f)^2$, a polynomial with integer coefficients. *Claims* (finite exact computations, Section 5.9, part G):

(C1) ($n=3$, all 2^8 functions) $H_f \ge 0$ on $[q_5, q_4]$; no H_f vanishes identically; $H_f(q_4) = 0$ exactly for $f = \pm\mathrm{OR}_{\{1,2,3\}}$, and these two H_f are > 0 on $[q_5, q_4)$; every other H_f is > 0 on $[q_5, q_4]$.

(C2) ($n=4$, all 2^{16} functions) $H_f \ge 0$ on $[q_5, q_4]$; $H_f \equiv 0$ exactly for $f = \pm\mathrm{OR}_{\{1,2,3,4\}}$; $H_f(q_4) = 0 \not\equiv H_f$ exactly for the eight functions $f = \pm\mathrm{OR}_S$ with $|S| = 3$, and these eight H_f are > 0 on $[q_5, q_4)$; every other H_f is > 0 on $[q_5, q_4]$.

Given the claims, $G_n(c) \le \tau|c| \cdot 4(1-q)^3 = T_4|c|$ on $[q_5, q_4]$. If equality holds with $c \ne 0$, then $\Delta(f^*) \ne 0$, c is a positive multiple of $\Delta(f^*)$, and $H_{f^*}(q) = 0$. By the claims and (5.6): for $n=3$, $q = q_4$, $f^* = \pm\mathrm{OR}_{\{1,2,3\}}$ and $\Delta(f^*) = \pm 2(1-q)^2(1,1,1)$; for $n=4$, either $f^* = \pm\mathrm{OR}_{\{1,2,3,4\}}$ and $\Delta(f^*) = \pm 2(1-q)^3(1,1,1,1)$, or $q = q_4$, $f^* = \pm\mathrm{OR}_S$ with $|S| = 3$ and $\Delta(f^*) = \pm 2(1-q)^2 \sum_{i\in S} e_i$. Conversely these vectors attain $T_4|c|$ by Lemma 5.4: $(1,1,1,1)$ gives T_4 for $q < \frac14$, and at q_4, $e_i + e_j + e_k$ gives $T_3 = T_4$ (the fourth coordinate does not contribute).

How the claims are checked. For each f, $\Delta_i(f) = \sum_{x:x_i=1} (f(x) - f(x-e_i)) \prod_{l\ne i} q^{x_l}(1-q)^{1-x_l}$ is computed as an integer polynomial, and the distinct polynomials H_f are tested (39 for $n=3$, 1 630 for $n=4$). Let $g_4(q) = 4q^2 - 8q + 1$ and $g_5(q) = 5q^2 - 10q + 1$, with roots q_4 and q_5 in $(0,1)$ ($4(1-q)^2 = 3$, resp. $5(1-q)^2 = 4$); both are decreasing on $[0,1]$, and g_4 is irreducible over $\mathbb{Q}$ (its discriminant 48 is not a square). Take rationals $q_5^- < q_5$ and $q_4^+ > q_4$ from rational bounds of $\sqrt{4/5}$ and $\sqrt{3/4}$, with $g_5(q_5^-) > 0$ and $g_4(q_4^+) < 0$ (and $q_5^+ < q_4^-$ for the companion bounds). For $H_f \not\equiv 0$: either $g_4 \mid H_f$, $H_f = g_4 Q$, where Q has no root in $[q_5^-, q_4^+]$ (Sturm) and $Q(q_5^-) > 0$; then $Q > 0$ on $[q_5, q_4]$, and $H_f = g_4 Q \ge 0$ there with equality only at q_4, since $g_4 > 0$ on $[0, q_4)$. Or $g_4 \nmid H_f$, and H_f has no root in $[q_5^-, q_4^+]$ and $H_f(q_5^-) > 0$, so $H_f > 0$ on $[q_5, q_4]$. Since g_4 is irreducible, $H_f(q_4) = 0$ iff $g_4 \mid H_f$. The lists of functions with $H_f \equiv 0$ and with $g_4 \mid H_f$ are compared with the truth tables of the OR functions. As a check of (5.6): for $n=3$, $H_{\mathrm{OR}_{\{1,2,3\}}} = 16(1-q)^6 - 12(1-q)^4 = 4(1-q)^4 g_4(q)$, and for $n=4$, $H_{\mathrm{OR}_{\{1,2,3,4\}}} = 16(1-q)^6 - 4\cdot 4(1-q)^6 = 0$. □

Remark 5.9. Lemmas 5.7 and 5.8 are the cases $n = 3, 4$ of RQ-C's result C6 ($R_n(q) = 2\tau\sqrt{\max_{k\le n} k(1-q)^{2k-2}}$ for $q \le \frac12$ and $n \le 7$, audited VALID as A.5, A.5b). Our check is independent of it. Both lemmas are false for $q > q_4$, where $(e_1+e_2+e_3)/\sqrt{3}$ gives $T_3 > T_4$, and the bound $G_5 \le T_4|c|$ of Lemma 5.6 is false for $q < q_5$, where $(e_1 + \cdots + e_5)/\sqrt{5}$ gives $T_5 > T_4$. These are the only places where the ends q_4 and q_5 of Theorem 5 enter the proof.

5.4 Moments of the remainder

Lemma 5.10 (cumulants)**.** *Let $w = u^2 + v^2$ and $d = u - v$. The cumulants of χ are $\kappa_1 = 0$, $\kappa_2 = 1$ and $\kappa_j = d^{[j \text{ odd}]} G_j(w)$ for $3 \le j \le 10$, where*

$$G_3 = 1, \qquad G_4 = w - 4,$$
$$G_5 = w - 10, \qquad G_6 = w^2 - 26w + 64,$$
$$G_7 = w^2 - 56w + 244, \qquad G_8 = w^3 - 120w^2 + 1188w - 2176,$$
$$G_9 = w^3 - 246w^2 + 4044w - 11080, \qquad G_{10} = w^4 - 502w^3 + 14604w^2 - 86728w + 126976.$$

Proof. By (5.1), $m_k = \mathbb{E}\chi^k = qu^k + (1-q)(-v)^k = (u^k + (-1)^k u^{2-k})/(1+u^2)$. The cumulants are determined by the recursion $\kappa_n = m_n - \sum_{k=1}^{n-1} \binom{n-1}{k-1} \kappa_k m_{n-k}$. For example $m_3 = u - v$, $m_4 = w - 1$, so $\kappa_3 = d$ and $\kappa_4 = m_4 - 3 = w - 4$. The identities for $j \le 10$ are verified symbolically (sympy, part A1 of the verifier: the difference of the two sides simplifies to 0 as a rational function of u). □

Lemma 5.11 (moments from cumulants)**.** *Let $M = \sum \beta_i \chi_i$ (finite sum) with $\sum \beta_i^2 = 1$ and power sums $p_j = \sum_i \beta_i^j$. Then M has cumulants $K_1 = 0$, $K_2 = 1$, $K_j = \kappa_j p_j$, and $\mathbb{E}M^n = \mu_n(K_3, \dots, K_n)$ for $n \le 10$, where $\mu_0 = 1$ and*

$$\mu_n = \sum_{k=2}^{n} \binom{n-1}{k-1} K_k \, \mu_{n-k} \qquad (K_2 = 1).$$

Each μ_n is a polynomial in $K_3, \dots, K_{10}$ with nonnegative integer coefficients; we write $\mu_n = \sum_e N_n(e) \prod_{j=3}^{10} K_j^{e_j}$ over exponent vectors $e = (e_3, \dots, e_{10})$. The term with $e = 0$ is the Gaussian moment: $N_n(0) = (n-1)!!$ for even n and 0 for odd n.

Proof. Cumulants of independent sums add and $K_j(\beta\chi) = \beta^j \kappa_j$, so $K_j(M) = \kappa_j p_j$, with $K_1 = 0$ and $K_2 = \sum \beta_i^2 = 1$. The recursion is the moment–cumulant relation $m_n = \sum_{k=1}^{n} \binom{n-1}{k-1} K_k m_{n-k}$ with $K_1 = 0$. The value at $K_3 = \cdots = K_{10} = 0$ is the n-th moment of a standard Gaussian. (Part A2 of the verifier checks the recursion against the Gaussian moments and against $\mathbb{E}\chi^n$ at $u = \frac{5}{2}$ for $n \le 10$.) □

Lemma 5.12 (power sums)**.** *Let $\sum \beta_i^2 = 1$, $\max |\beta_i| \le m \le 1$ and $\rho = \sqrt{p_4}$. Then $0 \le \rho \le m$, $|p_3| \le \rho$, $|p_j| \le m^{j-4}\rho^2$ for $5 \le j \le 10$, and $p_j \ge \rho^{j-2}$ for even $j \ge 4$.*

Proof. $p_4 \le m^2 \sum \beta_i^2 = m^2$. Cauchy–Schwarz gives $p_3^2 = (\sum \beta_i \beta_i^2)^2 \le p_2 p_4 = p_4$. For $j \ge 5$, $|p_j| \le \sum |\beta_i|^{j-4} \beta_i^4 \le m^{j-4} p_4$. For even $j \ge 4$, Jensen's inequality for the probability weights β_i^2 and the convex function $x \mapsto x^{(j-2)/2}$ gives $p_j = \sum \beta_i^2 (\beta_i^2)^{(j-2)/2} \ge (\sum \beta_i^2 \beta_i^2)^{(j-2)/2} = \rho^{j-2}$. □

Lemma 5.13 (sign information)**.** *Let $\sum \beta_i^2 = 1$, $m = \max |\beta_i|$, and suppose $\beta_{i_0} = -m$ for some i_0. If $m \ge m_c \in (0, 1]$, then $p_3 \le \varphi(m_c) := -m_c^3 + (1 - m_c^2)^{3/2}$. Moreover $\varphi(m) < 0$ iff $2m^2 > 1$.*

Proof. For $i \ne i_0$, $|\beta_i| \le (\sum_{i \ne i_0} \beta_i^2)^{1/2} = \sqrt{1 - m^2}$. Hence $p_3 = -m^3 + \sum_{i \ne i_0} \beta_i^3 \le -m^3 + \sqrt{1-m^2} \sum_{i \ne i_0} \beta_i^2 = \varphi(m)$, and $\varphi'(m) = -3m^2 - 3m\sqrt{1-m^2} \le 0$, so $\varphi(m) \le \varphi(m_c)$. Finally $\varphi(m) < 0$ iff $(1-m^2)^{3/2} < m^3$ iff $1 - m^2 < m^2$. □

Cumulant enclosures. For $1 \le u_1 \le u \le u_2$: $d = u - 1/u$ and $w = u^2 + u^{-2}$ are increasing and $d \ge 0$, so $d \in [d^-, d^+] = [u_1 - \frac{1}{u_1}, u_2 - \frac{1}{u_2}]$ and $w \in [w^-, w^+] = [u_1^2 + u_1^{-2}, u_2^2 + u_2^{-2}]$. Let $[G_j^-, G_j^+]$ be the exact range of the polynomial G_j on $[w^-, w^+]$ (computed by isolating the real roots of G_j' by Sturm sequences and bisection). Then $\kappa_j \in [\kappa_j^-, \kappa_j^+]$, where this is $[G_j^-, G_j^+]$ for even j and the interval product $[d^-, d^+] \cdot [G_j^-, G_j^+]$ for odd j.

Definition 5.14 (objective bound)**.** Let $D \le 10$, $c = (c_0, \dots, c_D) \in \mathbb{Q}^{D+1}$, $1 < u_1 < u_2$ rationals, $m^* \in (0, 1]$, $p^* < 0$ optional, and Θ a target. Put $L_e = \sum_n c_n N_n(e)$ and $A = L_0 = \sum_{n \text{ even}} c_n (n-1)!!$. For every $e \ne 0$ with $L_e \ne 0$ let $[C_e^-, C_e^+]$ be the interval product $L_e \prod_j [\kappa_j^-, \kappa_j^+]^{e_j}$, and put

$$u_e = e_3 + 2 \sum_{j \ge 4} e_j, \qquad U_e = \prod_{j \ge 5} (m^*)^{(j-4)e_j}.$$

Call e *even* if e_j is even for every odd j. For even e let $(\ell_e, l_e) = (0, 0)$ if $e_j > 0$ for some odd j, and $(\ell_e, l_e) = (1, \sum_{j \text{ even}} (j-2)e_j)$ otherwise. Define the term bounds

(T0) if p^* is given, $e=(1,0,\dots,0)$ (i.e. the monomial p_3) and $C_e^- \ge 0$: replace A by $A + C_e^- p^*$, and $b_e = 0$;

(T1) otherwise, if e is not even: $b_e(\rho) = \max(|C_e^-|, |C_e^+|)\, U_e\, \rho^{u_e}$;

(T2) if e is even and $C_e^+ \le 0$: $b_e(\rho) = C_e^+\, \ell_e\, \rho^{l_e}$;

(T3) if e is even and $C_e^+ > 0$: $b_e(\rho) = C_e^+\, U_e\, \rho^{u_e}$.

We say that c *satisfies the objective bound for* $(u_1, u_2, m^*, p^*, \Theta)$ if $h(\rho) = \Theta - A - \sum_e b_e(\rho) > 0$ for all $\rho \in [0, m^*]$.

Lemma 5.15 (expectation bound)**.** *Suppose c satisfies the objective bound for $(u_1, u_2, m^*, p^*, \Theta)$ and let $P(y) = \sum_n c_n y^n$. Then $\mathbb{E}P(M) < \Theta$ for every $u \in [u_1, u_2]$ and every $M = \sum \beta_i \chi_i$ with $\sum \beta_i^2 = 1$, $\max|\beta_i| \le m^*$ and, if p^* is given, $p_3 \le p^*$.*

Proof. By Lemma 5.11, $\mathbb{E}P(M) = \sum_n c_n \mu_n = L_0 + \sum_{e \ne 0} C_e p^e$ with $C_e = L_e \prod_j \kappa_j^{e_j} \in [C_e^-, C_e^+]$ and $p^e = \prod_j p_j^{e_j}$. Let $\rho = \sqrt{p_4} \in [0, m^*]$. By Lemma 5.12, $|p^e| \le \rho^{e_3} (\rho^2)^{e_4} \prod_{j \ge 5} (m^{*\,j-4} \rho^2)^{e_j} = U_e \rho^{u_e}$; if e is even then $p^e \ge 0$ (odd power sums appear to even powers, and $p_j \ge 0$ for even j); and if moreover $e_j = 0$ for all odd j, then $p^e \ge \prod_{j \text{ even}} \rho^{(j-2)e_j} = \rho^{l_e}$. Hence: in case (T0), $p_3 \le p^* < 0$ and $C_e \ge C_e^- \ge 0$ give $C_e p_3 \le C_e p^* \le C_e^- p^*$; in case (T1), $C_e p^e \le |C_e||p^e| \le b_e(\rho)$; in case (T2), $C_e \le C_e^+ \le 0$ and $p^e \ge \ell_e \rho^{l_e} \ge 0$ give $C_e p^e \le C_e^+ p^e \le C_e^+ \ell_e \rho^{l_e}$; in case (T3), $p^e \ge 0$ gives $C_e p^e \le C_e^+ p^e \le C_e^+ U_e \rho^{u_e}$. Summing, $\mathbb{E}P(M) \le \Theta - h(\rho) < \Theta$. □

5.5 The one-coordinate route ($a_1 \le \frac{33}{100}$)

Here we split off only $a = a_1$: $L = a\chi_1 + b_1 M_1$ with $b_1 = \sqrt{1-a^2}$ and $M_1 = \sum_{i \ge 2} (\alpha_i / b_1) \chi_i$, whose coefficients are at most $\min(1, a/b_1)$ in absolute value. For $y \in \mathbb{R}$,

$$\mathbb{E}|a\chi + y| = 2\tau a + 2R_a(y) - (1-2q)y, \qquad R_a(y) = \max\{0,\ (1-q)(y - av),\ q(-y - au)\}$$

(BF3, Lemma 9.4; Lemma 3 of `MAIN_RESULT`, audited VALID). Indeed $\mathbb{E}|a\chi + y| = q|au + y| + (1-q)|y - av|$ equals $2\tau a - (1-2q)y$ for $-au \le y \le av$ (using $qau = (1-q)av = \tau a$), y for $y > av$, and $-y$ for $y < -au$, and so does the right-hand side. Conditioning on M_1 and using $\mathbb{E}M_1 = 0$,

$$\mathbb{E}|L| = 2\tau a + 2\mathbb{E}R_a(b_1 M_1), \qquad \text{so} \qquad \mathbb{E}|L| < T_4 \iff \mathbb{E}R_a(b_1 M_1) < \tau\big(2(1-q)^3 - a\big).$$

A *cell* is $[u_1, u_2] \times [\underline{a}, \overline{a}]$ with rationals $1 < u_1 < u_2$ and $0 \le \underline{a} < \overline{a} \le A_S$. Let $\bar{b}$ be a rational upper bound of $\sqrt{1-\underline{a}^2}$, $\bar{m} = \min\{1, \overline{a}/\beta\}$ with β a rational lower bound of $\sqrt{1-\overline{a}^2}$, and

$$\bar{\ell}_1(y) = \frac{u_2^2}{1+u_2^2}\Big(\bar{b}y - \frac{\underline{a}}{u_2}\Big), \quad \bar{\ell}_2(y) = \frac{1}{1+u_1^2}\big(-\bar{b}y - \underline{a}u_1\big), \quad \Theta_1 = \tau(u_2)\Big(2\Big(\frac{u_1^2}{1+u_1^2}\Big)^3 - \overline{a}\Big).$$

A *cell certificate* is $c \in \mathbb{Q}^{D+1}$, $D \le 10$, with $P(y) = \sum c_n y^n$ such that (V1) $P > 0$, (V2) $P > \bar{\ell}_1$, (V3) $P > \bar{\ell}_2$ on $\mathbb{R}$, and (V4) c satisfies the objective bound for $(u_1, u_2, \bar{m}, -, \Theta_1)$.

Lemma 5.16. *If a cell with $u_1 \ge U_-$ has a certificate, then $\mathbb{E}|L| < T_4$ for every $u \in [u_1, u_2]$ and every unit α with $\underline{a} \le \max_i |\alpha_i| \le \overline{a}$.*

Proof. For $u \in [u_1,u_2]$, $a \in [\underline{a},\overline{a}]$ and $b_1=\sqrt{1-a^2}$ we have $R_a(b_1y)=\max\{0,\ell_1,\ell_2\}$ with $\ell_1=\frac{u^2}{1+u^2}(b_1y-\frac{a}{u})$ and $\ell_2=\frac{1}{1+u^2}(-b_1y-au)$. If $\ell_1(y)>0$ then $y>0$ and $0<b_1y-\frac{a}{u}\le \bar b y-\frac{\underline a}{u_2}$, and $\frac{u^2}{1+u^2}\le\frac{u_2^2}{1+u_2^2}$, so $\ell_1(y)\le\bar\ell_1(y)$. If $\ell_2(y)>0$ then $y<0$ and $0<-b_1y-au\le-\bar b y-\underline a u_1$, and $\frac{1}{1+u^2}\le\frac{1}{1+u_1^2}$, so $\ell_2(y)\le\bar\ell_2(y)$. So by (V1)–(V3), $R_a(b_1y)<P(y)$ for all y, and $\mathbb{E}R_a(b_1M_1)\le\mathbb{E}P(M_1)$. Since $a/\sqrt{1-a^2}$ is increasing, the coefficients of M_1 are at most $\bar m$ in absolute value. By Lemma 5.15, $\mathbb{E}P(M_1)<\Theta_1$. Finally $\Theta_1\le\tau(u)(2(1-q)^3-a)$, because $\tau(u)\ge\tau(u_2)$, $(1-q)^3\ge(\frac{u_1^2}{1+u_1^2})^3$, $a\le\overline a$, and the bracket is positive: $2(\frac{u_1^2}{1+u_1^2})^3\ge 2w_-^3\ge 1>\frac{33}{100}\ge\overline a$ by (5.3) (the verifier also asserts $\Theta_1>0$ for every cell). □

5.6 The two-coordinate route: vertex certificates

5.6.1 The functions F_x, nested patches and peeling

Let $k\in\{2,3,4\}$ and a sign vector $\sigma\in\{1,-1\}^k$ with $\sigma_1=1$. For $x\in\mathbb{R}^{k+1}$ and $y\in\mathbb{R}$ put

$$F_x(y)=\mathbb{E}\Big|\sum_{i=1}^{k}\sigma_i x_i\chi_i+x_{k+1}\,y\Big|,$$

where $\chi_1,\dots,\chi_k$ are i.i.d. normalised q-biased bits. We use $\sigma=(1,s)$ for $k=2$, $\sigma=(1,s,s_3)$ for $k=3$ and $\sigma=(1,s,s_3,s_4)$ for $k=4$.

Lemma 5.17. *For fixed q and y, the map $x\mapsto F_x(y)$ is convex and positively homogeneous of degree one. Consequently, if $x=\sum_l\nu_l V_l$ with $\nu_l\ge0$, then $F_x(y)\le\sum_l\nu_l F_{V_l}(y)$.*

Proof. $F_x(y)$ is the expectation of the absolute value of a linear function of x, i.e. a seminorm of x. A seminorm N satisfies $N(\sum\nu_lV_l)\le\sum\nu_lN(V_l)$ for $\nu_l\ge0$. □

The *patches* are the maps, for $j\in\{0,1,2\}$ and $k=2+j$,

$$p_k(t,r,\mu_1,\dots,\mu_j)=\big(rc(t),\,rd(t),\,b_0\mu_1,\,\dots,\,b_{j-1}\mu_j,\,b_j\big),\qquad b_0=\sqrt{1-r^2},\quad b_i=b_{i-1}\sqrt{1-\mu_i^2},$$

for $t\in[0,1]$ and $r,\mu_1,\dots,\mu_j\in[0,1]$. Thus $p_2(t,r)=(rc,rd,b_0)$, $p_3(t,r,m)=(rc,rd,b_0m,b_0\sqrt{1-m^2})$ and $p_4(t,r,m,m')=(rc,rd,b_0m,b_1m',b_1\sqrt{1-m'^2})$. Their values are unit vectors with nonnegative entries: $b_{i-1}^2\mu_i^2+b_i^2=b_{i-1}^2$, so $|p_k|^2=r^2c^2+r^2d^2+b_0^2=1$.

Peeling. Let $N=\sum_{i\in I}\gamma_i\chi_i$ be a finite sum with $\sum\gamma_i^2=1$, and $\mu(N)=\max_i|\gamma_i|$. If $\mu=\mu(N)<1$ and $\gamma_{i^*}=\varsigma\mu$ with $\varsigma\in\{1,-1\}$, the *peeled remainder* is $N^\flat=\sum_{i\in I\setminus\{i^*\}}(\gamma_i/\sqrt{1-\mu^2})\chi_i$. Then

$$N=\varsigma\mu\chi_{i^*}+\sqrt{1-\mu^2}\,N^\flat,\qquad \sum_{i\ne i^*}\frac{\gamma_i^2}{1-\mu^2}=1,\qquad \mu(N^\flat)\le\min\Big(1,\frac{\mu}{\sqrt{1-\mu^2}}\Big),\tag{5.7}$$

and $N^\flat$ is independent of χ_{i^*}: indeed $\sum_{i\ne i^*}\gamma_i^2=1-\mu^2$, and each $|\gamma_i|$ is at most μ and at most $\sqrt{1-\mu^2}$. If $\mu(N)=1$, then $N=\varsigma\chi_{i^*}$ (all other coefficients vanish).

Lemma 5.18 (conditional expectation)**.** *Consider a point with $r<1$ and remainder M, and let $j\in\{0,1,2\}$. Put $M^{(0)}=M$ and, for $i=1,\dots,j$, let $\mu_i=\mu(M^{(i-1)})$, attained by the coefficient $\varsigma_i\mu_i$ of χ_{l_i}, and $M^{(i)}=(M^{(i-1)})^\flat$ if $\mu_i<1$.*

(i) If $\mu_1,\dots,\mu_j<1$, then $\mathbb{E}|L|=\mathbb{E}F_{p_{2+j}(t,r,\mu_1,\dots,\mu_j)}(M^{(j)})$ with $\sigma=(1,s,\varsigma_1,\dots,\varsigma_j)$, the bits being $\chi_1,\chi_2,\chi_{l_1},\dots,\chi_{l_j}$; here $M^{(j)}$ is independent of these bits, $\sum$(coefficients of $M^{(j)})^2=1$, and $\mu(M^{(j)})\le\min(1,\mu_j/\sqrt{1-\mu_j^2})$ if $j\ge1$.

(ii) If $j\ge1$, $\mu_1,\dots,\mu_{j-1}<1$ and $\mu_j=1$, then $L=a_1\chi_1+sa_2\chi_2+\sum_{i<j}\varsigma_i b_{i-1}\mu_i\chi_{l_i}+\varsigma_j b_{j-1}\chi_{l_j}$, and $F_{p_{2+j}(t,r,\mu_1,\dots,\mu_j)}(y)=\mathbb{E}|L|$ for every $y\in\mathbb{R}$ (with the same σ).

Proof. $L=a_1\chi_1+sa_2\chi_2+b_0M^{(0)}$ with $(a_1,a_2)=(rc(t),rd(t))$, and by (5.7), if $\mu_i<1$, $b_{i-1}M^{(i-1)}=\varsigma_i b_{i-1}\mu_i\chi_{l_i}+b_iM^{(i)}$. By induction $L=a_1\chi_1+sa_2\chi_2+\sum_{i\le j}\varsigma_i b_{i-1}\mu_i\chi_{l_i}+b_jM^{(j)}$, where the bits are distinct and independent of $M^{(j)}$; conditioning on $M^{(j)}$ gives (i), and the bound on $\mu(M^{(j)})$ is (5.7). In (ii), $M^{(j-1)}=\varsigma_j\chi_{l_j}$, which gives the formula for L; the last entry of p_{2+j} is $b_j=b_{j-1}\sqrt{1-1}=0$, so $F_{p_{2+j}}(y)$ does not depend on y and equals $\mathbb{E}|L|$. □

5.6.2 Vertex sets and the cone lemma

Definition 5.19 (vertex set)**.** Let $X=\prod_{i=1}^k[\xi_i^-,\xi_i^+]$ be a box of patch parameters ((t,r) for $k=2$, (t,r,m) for $k=3$, (t,r,m,m') for $k=4$) and $p=p_k$. A *vertex set for X* is a vector $n_0\in\mathbb{Q}^{k+1}$ and 2^k vectors $V_\epsilon\in\mathbb{Q}^{k+1}$, indexed by $\epsilon\in\{0,1\}^k$, such that:

(P1) $|n_0|^2\ge1$ and $V_\epsilon\cdot n_0=|n_0|^2$ for all ϵ;

(P2) (parallelepiped) $V_\epsilon=V_0+\sum_i\epsilon_iE_i$ with $E_i=V_{e_i}-V_0$;

(P3) (facets) for each i and $\delta\in\{0,1\}$ the 2^{k-1} vertices with $\epsilon_i=\delta$ span a linear subspace of dimension k; let $h_{i,\delta}$ be a normal vector of it, oriented so that $h_{i,\delta}\cdot\bar c>0$ for the centre $\bar c=V_0+\frac12\sum_iE_i$ (and $h_{i,\delta}\cdot\bar c\ne0$ is required);

(P4) (enclosure) $h_{i,\delta}\cdot p(\xi)\ge0$ for all i,δ and all $\xi\in X$.

Lemma 5.20 (cone lemma)**.** *Let $(n_0,(V_\epsilon))$ be a vertex set for X. Then for every $\xi\in X$ there are $\nu_\epsilon\ge0$ with $p(\xi)=\sum_\epsilon\nu_\epsilon V_\epsilon$ and $\sum_\epsilon\nu_\epsilon\le1/|n_0|\le1$.*

Proof. First, $V_0,E_1,\dots,E_k$ is a basis of $\mathbb{R}^{k+1}$. Indeed $E_i\cdot n_0=0$ by (P1) and $V_0\cdot n_0=|n_0|^2\ne0$, so $V_0\notin\operatorname{span}\{E_i\}$. By (P2) the face $\{\epsilon_i=0\}$ spans $S_i=\operatorname{span}(V_0,\{E_j\}_{j\ne i})$, which has dimension k by (P3); hence the k vectors $V_0,\{E_j\}_{j\ne i}$ are linearly independent. Moreover $\bar c-V_0-\frac12\sum_{j\ne i}E_j=\frac12E_i$ and $h_{i,0}\cdot\bar c\ne0$ with $h_{i,0}\perp S_i$, so $E_i\notin S_i$. Thus the $k+1$ vectors are independent.

Let $z\in\mathbb{R}^{k+1}$ with $h_{i,\delta}\cdot z\ge0$ for all i,δ, and write $z=\lambda V_0+\sum_i\mu_iE_i$. Since $h_{i,0}\perp S_i$, $h_{i,0}\cdot z=\mu_i\,h_{i,0}\cdot E_i$, and $h_{i,0}\cdot\bar c=\frac12h_{i,0}\cdot E_i>0$; so $\mu_i\ge0$. The face $\{\epsilon_i=1\}$ spans $\operatorname{span}(V_0+E_i,\{E_j\}_{j\ne i})$, so $h_{i,1}\cdot E_j=0$ ($j\ne i$) and $h_{i,1}\cdot V_0=-h_{i,1}\cdot E_i$; then $h_{i,1}\cdot\bar c=-\frac12h_{i,1}\cdot E_i>0$, so $h_{i,1}\cdot V_0>0$, and $h_{i,1}\cdot z=(\lambda-\mu_i)\,h_{i,1}\cdot V_0$; so $\mu_i\le\lambda$. If $\lambda=0$ then $z=0$. Otherwise $z/\lambda=V_0+\sum_i\theta_iE_i$ with $\theta_i=\mu_i/\lambda\in[0,1]$, which is a point of the parallelepiped $\operatorname{conv}\{V_\epsilon\}$, i.e. a convex combination $\sum\omega_\epsilon V_\epsilon$ (take $\omega_\epsilon=\prod_i\theta_i^{\epsilon_i}(1-\theta_i)^{1-\epsilon_i}$). So $z=\sum\nu_\epsilon V_\epsilon$ with $\nu=\lambda\omega\ge0$ and $\sum\nu_\epsilon=\lambda$. Finally $z\cdot n_0=\lambda|n_0|^2$, so $\lambda=z\cdot n_0/|n_0|^2\le|z|/|n_0|$.

By (P4), $z=p(\xi)$ satisfies the hypothesis, and $|p(\xi)|=1$. □

Condition (P4) is checked without subdivision: the minimum of a linear functional over a parameter box of a patch is the end of a short chain of one-variable minimisations.

Lemma 5.21 (facet minima)**.** *For $\alpha,\beta\in\mathbb{R}$ and $-1\le x^-<x^+\le1$ let $g(x)=\alpha x+\beta\sqrt{1-x^2}$ and $\mathfrak{m}(\alpha,\beta;x^-,x^+)=\min_{x\in[x^-,x^+]}g(x)$.*

(i) If $\beta \geq 0$, then $\mathfrak{m}(\alpha, \beta; x^-, x^+) = \min(g(x^-), g(x^+))$.

(ii) If $\beta < 0$, put $R = \sqrt{\alpha^2 + \beta^2}$ and $x^* = -\alpha/R$. Then $\mathfrak{m}(\alpha, \beta; x^-, x^+) = -R$ if $x^- \leq x^* \leq x^+$, and $\mathfrak{m}(\alpha, \beta; x^-, x^+) = \min(g(x^-), g(x^+))$ otherwise.

(iii) $\mathfrak{m}(\alpha, \beta; x^-, x^+)$ is nondecreasing in β, and also in α if $x^- \geq 0$.

Let $k = 2+j$ with $j \in \{0, 1, 2\}$, let $X = [t^-, t^+] \times [r^-, r^+] \times \prod_{i=1}^{j} [\mu_i^-, \mu_i^+]$ with $0 \leq t^- < t^+ \leq 1$, $0 \leq r^- < r^+ \leq 1$ and $0 \leq \mu_i^- < \mu_i^+ \leq 1$, and let $h \in \mathbb{R}^{k+1}$. Put $W_j = h_{k+1}$, $W_{i-1} = \mathfrak{m}(h_{i+2}, W_i; \mu_i^-, \mu_i^+)$ for $i = j, j-1, \ldots, 1$, $A = \mathfrak{m}(h_1, h_2; c(t^+), c(t^-))$ and $G = \mathfrak{m}(A, W_0; r^-, r^+)$. Then

$$\min_{\xi \in X} h \cdot p_k(\xi) = G.$$

If in this recursion each value of $\mathfrak{m}$ is replaced by a lower bound of it (and the later steps are applied to these lower bounds), the result is a lower bound of G.

Proof. (i) The function $x \mapsto \sqrt{1-x^2}$ is concave on $[-1, 1]$, so for $\beta \geq 0$ the function g is concave, and the minimum of a concave function over an interval is attained at an endpoint.

(ii) For $\beta < 0$ the function g is convex. By the Cauchy–Schwarz inequality, $g(x) \geq -R\,|(x, \sqrt{1-x^2})| = -R$ for all $x \in [-1, 1]$. Moreover $R > 0$, $|x^*| \leq 1$ and $\sqrt{1-x^{*2}} = |\beta|/R = -\beta/R$, so $g(x^*) = -\alpha^2/R - \beta^2/R = -R$. Thus x^* is a minimum point of g on $[-1, 1]$. If $x^* \in [x^-, x^+]$, the minimum over $[x^-, x^+]$ is $-R$. Otherwise $[x^-, x^+]$ lies in $[-1, x^*]$ or in $[x^*, 1]$, where the convex function g is nonincreasing, respectively nondecreasing, so the minimum is attained at an endpoint.

(iii) For every $x \in [-1, 1]$, $g(x)$ is nondecreasing in β because $\sqrt{1-x^2} \geq 0$, and nondecreasing in α if $x \geq 0$. Minima over x of pointwise nondecreasing families are nondecreasing.

Now the patch. Put $w_j = h_{k+1}$ and $w_{i-1}(\mu_i, \ldots, \mu_j) = h_{i+2}\mu_i + \sqrt{1-\mu_i^2}\; w_i(\mu_{i+1}, \ldots, \mu_j)$ for $i = j, \ldots, 1$. Since $b_i = b_{i-1}\sqrt{1-\mu_i^2}$, we have $b_{i-1}w_{i-1} = h_{i+2}\, b_{i-1}\mu_i + b_i w_i$, and therefore

$$h \cdot p_k(t, r, \mu_1, \ldots, \mu_j) = r\,\big(h_1 c(t) + h_2 d(t)\big) + b_0\, w_0(\mu_1, \ldots, \mu_j), \qquad b_0 = \sqrt{1-r^2}.$$

First, $\min w_{i-1} = W_{i-1}$, the minimum being over $\mu_l \in [\mu_l^-, \mu_l^+]$ for $l \geq i$. This holds for $i - 1 = j$, since $w_j = h_{k+1} = W_j$. If it holds for i, then for fixed μ_i the minimum of w_{i-1} over $\mu_{i+1}, \ldots, \mu_j$ is $h_{i+2}\mu_i + \sqrt{1-\mu_i^2}\, W_i$, because the weight $\sqrt{1-\mu_i^2}$ is nonnegative and w_i does not depend on μ_i. Minimising over $\mu_i \in [\mu_i^-, \mu_i^+]$ gives $\mathfrak{m}(h_{i+2}, W_i; \mu_i^-, \mu_i^+) = W_{i-1}$.

Second, c is a decreasing bijection of $[t^-, t^+]$ onto $[c(t^+), c(t^-)]$, and $d(t) = \sqrt{1-c(t)^2}$ for $t \in [0, 1]$ (because $c^2 + d^2 = 1$ and $d \geq 0$). Hence $\min_{t \in [t^-, t^+]}(h_1 c(t) + h_2 d(t)) = \mathfrak{m}(h_1, h_2; c(t^+), c(t^-)) = A$.

Third, for fixed r the two brackets depend on disjoint sets of parameters and have the nonnegative weights r and b_0, so the minimum over t and μ is $rA + \sqrt{1-r^2}\, W_0$. Minimising over $r \in [r^-, r^+]$ gives G.

The last statement follows from (iii) by induction along the recursion: in the steps for W_{i-1} the replaced value enters as β, and in the step for G the values A and W_0 enter as α and β, with $x = r \geq r^- \geq 0$. □

Checking (P4). (P4) holds if and only if $G(h_{i,\delta}) \geq 0$ for all $2k$ facet normals. A rational lower bound of G is computed by the recursion of Lemma 5.21 in exact rational arithmetic: an endpoint value $g(x^\pm)$ is bounded below using a rational lower bound of $\sqrt{1-(x^\pm)^2}$ if $\beta \geq 0$ and a rational

upper bound if $\beta < 0$; the value $-R$ is bounded below by $-R^+$ with $R^+ \geq R$ rational; and the condition $x^- \leq x^* \leq x^+$ is decided exactly. For rationals p, q the sign of $p - qR$ is: ≥ 0 if $p \geq 0 \geq q$; < 0 if $p \leq 0 \leq q$ and $(p,q) \neq (0,0)$; the sign of $p^2 - q^2R^2$ if $p, q > 0$; and the sign of $q^2R^2 - p^2$ if $p, q < 0$. Then $x^- \leq x^*$ if and only if $p - qR \geq 0$ for $(p,q) = (-\alpha, x^-)$, and $x^* \leq x^+$ if and only if $p - qR \leq 0$ for $(p,q) = (-\alpha, x^+)$. (P4) is accepted if the lower bound is ≥ 0 for every facet normal.

5.6.3 Vertex envelopes and vertex certificates

Fix a u-interval $[u_1, u_2]$ with $u_1 > 1$. For a vertex $V \in \mathbb{Q}^{k+1}$ let $\gamma = (\sigma_1 V_1, \ldots, \sigma_k V_k)$ and $b_V = V_{k+1}$. The atoms of $\sum_i \gamma_i \chi_i$ are indexed by $\omega \in \{u, -v\}^k$, with probability $\pi_\omega = \prod_i q^{[\omega_i = u]}(1-q)^{[\omega_i = -v]}$ and value $y_\omega = \sum_i \gamma_i \omega_i$, and by (5.1)

$$\pi_\omega y_\omega = \tau \sum_i \gamma_i \, (\pm 1)_i \prod_{l \neq i} q^{[\omega_l = u]}(1-q)^{[\omega_l = -v]}, \qquad (\pm 1)_i = +1 \text{ if } \omega_i = u, \ -1 \text{ otherwise.}$$

Using $q \in [\frac{1}{1+u_2^2}, \frac{1}{1+u_1^2}]$, $1 - q \in [\frac{u_1^2}{1+u_1^2}, \frac{u_2^2}{1+u_2^2}]$ and $\tau \in [\tau(u_2), \tau(u_1)]$, interval arithmetic gives rational enclosures $\pi_\omega y_\omega \in [\eta_\omega^-, \eta_\omega^+]$ and $\pi_\omega \in [\pi_\omega^-, \pi_\omega^+]$, valid for all $u \in [u_1, u_2]$. Put $[\beta_\omega^-, \beta_\omega^+] = [\min(\pi_\omega^- b_V, \pi_\omega^+ b_V), \max(\pi_\omega^- b_V, \pi_\omega^+ b_V)]$.

Definition 5.22 (vertex envelope)**.** $\Phi_V(y) = \sum_\omega \max(\eta_\omega^+ + \beta_\omega^+ y, \ -\eta_\omega^- - \beta_\omega^- y)$ for $y \geq 0$, and $\Phi_V(y) = \sum_\omega \max(\eta_\omega^+ + \beta_\omega^- y, \ -\eta_\omega^- - \beta_\omega^+ y)$ for $y < 0$.

Lemma 5.23 (envelope)**.** *$F_V(y) \leq \Phi_V(y)$ for all $y \in \mathbb{R}$ and all $u \in [u_1, u_2]$. On each closed half-line, Φ_V is continuous and piecewise linear, with breakpoints among the points where the two lines of one summand cross.*

Proof. $F_V(y) = \sum_\omega \pi_\omega |y_\omega + b_V y| = \sum_\omega |\pi_\omega y_\omega + \pi_\omega b_V \, y|$ and $|z| = \max(z, -z)$. For $y \geq 0$: $\pi_\omega y_\omega + \pi_\omega b_V y \leq \eta_\omega^+ + \beta_\omega^+ y$ and $-\pi_\omega y_\omega - \pi_\omega b_V y \leq -\eta_\omega^- - \beta_\omega^- y$, since $\pi_\omega b_V \in [\beta_\omega^-, \beta_\omega^+]$ (whatever the sign of b_V). For $y < 0$ the roles of $\beta^\pm$ are exchanged. □

Definition 5.24 (vertex certificate)**.** Let X be a parameter box, σ a sign vector, $[u_1, u_2]$ a u-interval, $m^* \in (0, 1]$ a cap, and $p^* < 0$ optional. A *vertex certificate for* $(X, \sigma, [u_1, u_2], m^*, p^*)$ is a vertex set $(n_0, (V_\epsilon))$ for X and coefficient vectors $c^{(\epsilon)} \in \mathbb{Q}^{D+1}$, $D \leq 10$, with $P_\epsilon(y) = \sum_n c_n^{(\epsilon)} y^n$, such that for every ϵ: (W1) $P_\epsilon(y) > \Phi_{V_\epsilon}(y)$ for all $y \in \mathbb{R}$; and (W2) $c^{(\epsilon)}$ satisfies the objective bound for $(u_1, u_2, m^*, p^*, T^-(u_1, u_2))$.

(W1) is checked as follows: on each half-line, Φ_V coincides on each interval between consecutive breakpoints with one line $\lambda_0 + \lambda_1 y$ (one choice of line per summand); for every such line, $P_\epsilon - \lambda_0 - \lambda_1 y$ is shown to be positive on all of $\mathbb{R}$ by Sturm sequences.

Lemma 5.25 (vertex certificate lemma)**.** *Let a vertex certificate for $(X, \sigma, [u_1, u_2], m^*, p^*)$ be given. Let $\mathcal{Z}$ be the class of random variables $Z = \sum \beta_i \chi_i'$ (finite sums of i.i.d. copies of χ, independent of $\chi_1, \ldots, \chi_k$) with $\sum \beta_i^2 = 1$, $\max |\beta_i| \leq m^*$ and, if p^* is given, $p_3 \leq p^*$. Then for every $u \in [u_1, u_2]$, every $\xi \in X$ and every $Z \in \mathcal{Z}$,*

$$\mathbb{E} F_{p(\xi)}(Z) < T^-(u_1, u_2) \leq T_4(u).$$

Proof. By Lemma 5.20, $p(\xi) = \sum \nu_\epsilon V_\epsilon$ with $\nu \geq 0$ and $\sum \nu_\epsilon \leq 1$. By Lemmas 5.17 and 5.23 and (W1), for every y, $F_{p(\xi)}(y) \leq \sum_\epsilon \nu_\epsilon F_{V_\epsilon}(y) \leq \sum_\epsilon \nu_\epsilon P_\epsilon(y)$. Taking expectations over Z, $\mathbb{E} F_{p(\xi)}(Z) \leq \sum_\epsilon \nu_\epsilon \mathbb{E} P_\epsilon(Z)$. By (W1) and Lemma 5.23, $\mathbb{E} P_\epsilon(Z) > \mathbb{E} F_{V_\epsilon}(Z) \geq 0$, and by (W2) and Lemma 5.15, $\mathbb{E} P_\epsilon(Z) < T^-$. Since $\sum \nu_\epsilon \leq 1$ and $\max_\epsilon \mathbb{E} P_\epsilon(Z) \geq 0$, $\sum_\epsilon \nu_\epsilon \mathbb{E} P_\epsilon(Z) \leq \max_\epsilon \mathbb{E} P_\epsilon(Z) < T^-$. Finally $T^- \leq T_4(u)$ by (5.2). □

Two members of $\mathcal{Z}$ are used repeatedly: $Z = N^{-1/2}(\chi'_1 + \cdots + \chi'_N)$ with $N^{-1/2} \le m^*$ (no p^*), and, if $m^* = 1$, $Z = \chi'_1$ (no p^*).

5.6.4 Boxes

A *box* is $B = [u_1, u_2] \times [t_1, t_2] \times [r_1, r_2]$ with rationals $1 < u_1 < u_2$, $0 \le t_1 < t_2 \le 1$, $0 \le r_1 < r_2 \le 1$, together with a sign s. Let b^- be a rational lower bound of $\sqrt{1 - r_2^2}$ ($b^- = 0$ if $r_2 = 1$), and define $\bar{m}(B) = 1$ if $b^- = 0$ or $r_2 d(t_2) \ge b^-$, and $\bar{m}(B) = r_2 d(t_2)/b^-$ otherwise. Then $\bar{m}(B) \in (0, 1]$ and $m \le \min(1, a_2/b) \le \bar{m}(B)$ at every point of B with $r < 1$, because $a_2 = rd(t) \le r_2 d(t_2)$ and $b \ge b^-$. A box of kind lpv carries a vertex certificate for $([t_1, t_2] \times [r_1, r_2], (1, s), [u_1, u_2], \bar{m}(B), -)$. A box of kind small satisfies $r_2 c(t_1) \le A_S$, so $a_1 = rc(t) \le A_S$ on it.

Lemma 5.26. *At every point of an lpv box with $r < 1$, $\mathbb{E}|L| < T_4$.*

Proof. By Lemma 5.18 ($j = 0$), $\mathbb{E}|L| = \mathbb{E}F_{p_2(t,r)}(M)$, and $M \in \mathcal{Z}$ since $m \le \bar{m}(B)$. Apply Lemma 5.25. □

5.7 Near $(e_1 + e_2)/\sqrt{2}$: the near-circle lemma

Lemma 5.27 (tail bound)**.** *Let $y \in \mathbb{R}$, $b \ge 0$ and let Z be a random variable with $\mathbb{E}Z = 0$ and $\mathbb{E}Z^4 < \infty$. Then*

$$\mathbb{E}|y + bZ| \le |y| + \min\Big(b\,\mathbb{E}|Z|,\ \frac{27}{128}\,\frac{b^4 \mathbb{E}Z^4}{|y|^3}\Big),$$

where for $y = 0$ the minimum is read as its first entry. The same convention is used below whenever this bound is applied at a point where $y = 0$.

Proof. The first bound is the triangle inequality. For the second ($y \ne 0$), $|y + z| - |y| - \operatorname{sgn}(y) z = 2(-\operatorname{sgn}(y) z - |y|)_+ \le 2(|z| - |y|)_+$, and $\mathbb{E}[\operatorname{sgn}(y) bZ] = 0$. For $x \ge 0$ and $\eta > 0$, $(x - \eta)_+ \le \frac{27}{256} x^4/\eta^3$: the maximum of $(x - \eta)/x^4$ over $x > \eta$ is at $x = \frac{4}{3}\eta$ and equals $\frac{27}{256}\eta^{-3}$. Hence $\mathbb{E}|y + bZ| - |y| \le 2 \cdot \frac{27}{256}\, b^4 \mathbb{E}Z^4/|y|^3$. □

Lemma 5.28 (near-circle tests)**.** *Let B be a box with $r_1 > 0$ and $u_1 \ge U_-$. Let y_j ($j = 1, \dots, 4$) be the atoms of $c\chi_1 + sd\chi_2$, so that the atoms of $a_1\chi_1 + sa_2\chi_2$ are ry_j. Let $\eta_j \ge 0$ be a lower bound of $|y_j|$ on B, p_j^+ an upper bound of p_j, b^+ an upper bound of $\sqrt{1 - r_1^2}$, and $E_4 = 3 + \max(0, w^+ - 4)\,\bar{m}(B)^2$. Let $T^- = T^-(u_1, u_2)$.*

(A) If all $\eta_j > 0$ and $\frac{27}{128} E_4 (b^+)^2 \frac{1 + r_2}{r_1^3} \sum_j p_j^+ \eta_j^{-3} < T^-$, then $\mathbb{E}|L| < T_4$ at every point of B with $r < 1$.

(B) Let G^+ be an upper bound of $\mathbb{E}|c\chi_1 + sd\chi_2| = \tau \sum_j |g_j|$ on B with $G^+ \le T^-$, and $e_j^+ = \min\big(b^+, \frac{27}{128}(b^+)^4 E_4/(r_1^3 \eta_j^3)\big)$ ($e_j^+ = b^+$ if $\eta_j = 0$). If $\sum_j p_j^+ e_j^+ < T^-(1 - r_2) + r_1(T^- - G^+)$, then $\mathbb{E}|L| < T_4$ at every point of B with $r < 1$.

Proof. At a point of B with $r < 1$, condition on (χ_1, χ_2) and apply Lemma 5.27 with $Z = M$. Here $\mathbb{E}M^4 = 3 + \kappa_4 p_4 \le E_4$ by Lemma 5.11, since $p_4 \le m^2 \le \bar{m}(B)^2$ and $\kappa_4 = w - 4 \le w^+ - 4$; also $\mathbb{E}|M| \le 1$. This gives $\mathbb{E}|L| \le rG + \sum_j p_j e_j$, where $G = \mathbb{E}|c\chi_1 + sd\chi_2|$ and $e_j = \min(b, \frac{27}{128} b^4 E_4/(r^3 |y_j|^3))$. (A) By Lemma 5.5 ($u \ge U_-$, $c^2 + d^2 = 1$), $G < T_4$. Since $1 - r = b^2/(1 + r)$ and $b > 0$, $\sum_j p_j e_j \le \frac{27}{128} \frac{b^4 E_4}{r^3} \sum_j \frac{p_j}{|y_j|^3} \le b^2 \cdot \frac{27}{128} E_4 (b^+)^2 \frac{1}{r_1^3} \sum_j \frac{p_j^+}{\eta_j^3} < \frac{b^2 T^-}{1 + r_2} \le T_4(1 - r)$. So $\mathbb{E}|L| < rT_4 + T_4(1 - r) = T_4$. (B) $\mathbb{E}|L| \le rG^+ + \sum_j p_j^+ e_j^+ < rG^+ + T^-(1 - r_2) + r_1(T^- - G^+) \le rG^+ + T^-(1 - r) + r(T^- - G^+) = T^- \le T_4$, using $r_1 \le r \le r_2$ and $T^- - G^+ \ge 0$. □

Boxes of kind ncA pass test (A) or test (B).

5.8 Near the extremisers: the m-split

In our coordinates the extremisers are the following points (all with $s = 1$ and $t = \sqrt{2} - 1$, since $a_1 = a_2$):

- $(e_1 + e_2 + e_3 + e_4)/2$, for every $q \in [q_5, q_4]$: $a_1 = a_2 = \frac{1}{2}$, $b = \frac{1}{\sqrt{2}}$, $M = (\chi_3 + \chi_4)/\sqrt{2}$, so $m = \frac{1}{\sqrt{2}}$, and after peeling χ_3, $M' = \chi_4$, $m' = 1$;
- $(e_1 + e_2 + e_3)/\sqrt{3}$, at q_4: $a_1 = a_2 = b = \frac{1}{\sqrt{3}}$, $M = \chi_3$, $m = 1$;
- $(e_1 + \cdots + e_5)/\sqrt{5}$, at q_5: $a_1 = a_2 = \frac{1}{\sqrt{5}}$, $b = \sqrt{3/5}$, $M = (\chi_3 + \chi_4 + \chi_5)/\sqrt{3}$, $m = \frac{1}{\sqrt{3}}$; after peeling, $M' = (\chi_4 + \chi_5)/\sqrt{2}$, $m' = \frac{1}{\sqrt{2}}$, and $M'' = \chi_5$, $m'' = 1$.

Equality holds at these points, so no certificate with a strict bound can contain them. We split according to $m = \max_{i \geq 3} |\beta_i|$ and the sign of a largest remaining coefficient, and inside some pieces we peel off the largest coefficient and split the new remainder again, up to five split coordinates in total. We write $M' = M^{(1)}$, $m' = \mu(M')$, $M'' = M^{(2)}$, $m'' = \mu(M'')$ (Lemma 5.18), and

$$a_3 = bm, \quad b' = b\sqrt{1 - m^2}, \quad a_4 = b'm', \quad b'' = b'\sqrt{1 - m'^2}, \quad a_5 = b''m'', \quad b''' = b''\sqrt{1 - m''^2},$$

so that $L = a_1\chi_1 + sa_2\chi_2 + bM$, $bM = \pm a_3\chi_{i_0} + b'M'$, $b'M' = \pm a_4\chi_{i_1} + b''M''$ and $b''M'' = \pm a_5\chi_{i_2} + b'''M'''$, with the signs of the peeled coefficients. Throughout, $E_4' = 3 + \max(0, \kappa_4)$; for any remainder $N = \sum \gamma_i\chi_i$ with $\sum \gamma_i^2 = 1$, $\mathbb{E}N^4 = 3 + \kappa_4 \sum \gamma_i^4 \leq E_4'$ by Lemma 5.11 (as $0 \leq \sum \gamma_i^4 \leq 1$), and $\mathbb{E}|N| \leq 1$.

5.8.1 Three split coordinates

Lemma 5.29 (three-coordinate near-sphere bound)**.** *Consider a point with $r < 1$ and suppose $\beta_{i_0} = +m$ for some $i_0 \geq 3$. Let $Y = a_1\chi_1 + sa_2\chi_2 + a_3\chi_{i_0}$ with atoms y_j and probabilities p_j ($j = 1, \ldots, 8$), and $r' = \sqrt{a_1^2 + a_2^2 + a_3^2} = \sqrt{1 - b'^2}$. Then*

$$\mathbb{E}|L| \leq \mathbb{E}|Y| + \sum_j p_j \min\Big(b',\ \frac{27}{128}\frac{b'^4 E_4'}{|y_j|^3}\Big).$$

If moreover $q \in [q_5, q_4]$, all $y_j \neq 0$ and $\frac{27}{128}E_4'\, b'^2(1 + r') \sum_j p_j |y_j|^{-3} < T_4$, then $\mathbb{E}|L| < T_4$ if $b' > 0$, and if $b' = 0$ then $\mathbb{E}|L| = G_3(a_1, sa_2, a_3) \leq T_4$.

Proof. If $m = 1$ then $b' = 0$ and $L = Y$. Otherwise $L = Y + b'M'$ with M' independent of Y (Lemma 5.18), and conditioning on $(\chi_1, \chi_2, \chi_{i_0})$ and applying Lemma 5.27 with $Z = M'$ gives the first bound. By Lemma 5.7, $\mathbb{E}|Y| = G_3(a_1, sa_2, a_3) \leq T_4 r'$. If $b' > 0$, the hypothesis and $1 - r' = b'^2/(1 + r')$ give $\sum_j p_j \frac{27}{128}\frac{b'^4 E_4'}{|y_j|^3} < T_4 \frac{b'^2}{1 + r'} = T_4(1 - r')$, hence $\mathbb{E}|L| < T_4 r' + T_4(1 - r') = T_4$. □

Piece tests (A3), (B3). Let B be a box with $b^- > 0$ and $[m_1, m_2] \subset (0, 1]$. On $B \times [m_1, m_2]$ we enclose $a_1 = rc(t)$, $a_2 = rd(t)$, $a_3 = bm \in [b^- m_1, b^+ m_2]$, $b'^2 \leq (b'^2)^+ := (b^+)^2(1 - m_1^2)$, and $r' \leq r'^+ := \min\big(1, \sqrt{1 - (b^-)^2(1 - m_2^2)}\big)$ (recall $r'^2 = 1 - b^2(1 - m^2)$). The atoms $y_j = a_1 x_{j1} + sa_2 x_{j2} + a_3 x_{j3}$ ($x \in \{u, -v\}^3$) and the products $p_j y_j = \tau \sum_i (\pm a_i) \prod_{l \neq i} \Pr[x_{jl}]$ (by $qu = (1 - q)v = \tau$) are enclosed in interval arithmetic. Let η_j be a lower bound of $|y_j|$, p_j^+ an upper bound of p_j, and $E_4'^+ = 3 + \max(0, w^+ - 4)$. The piece passes

- test (A3) if all $\eta_j > 0$ and $\frac{27}{128}E_4'^{+}(b'^2)^{+}(1+r'^{+})\sum_j p_j^{+}\eta_j^{-3} < T^{-}(u_1,u_2)$;
- test (B3) if $\sum_j \big(|p_jy_j|^{+} + p_j^{+}\min\big(b'^{+}, \frac{27}{128}((b'^2)^{+})^2E_4'^{+}/\eta_j^3\big)\big) < T^{-}(u_1,u_2)$, where $|p_jy_j|^{+}$ is an upper bound of $|p_jy_j|$, b'^{+} an upper bound of $\sqrt{(b'^2)^{+}}$, and the second entry of the minimum is omitted if $\eta_j = 0$.

By Lemma 5.29, if a piece passes (A3), then at every point of B with $q \in [q_5, q_4]$ and every remainder with $\beta_{i_0} = +m$, $m \in [m_1, m_2]$, we have $\mathbb{E}|L| < T_4$ if $b' > 0$, and $\mathbb{E}|L| = G_3(a_1, sa_2, bm) \le T_4$ if $b' = 0$. If it passes (B3), then $\mathbb{E}|L| < T_4$ at every $u \in [u_1, u_2]$ by the first bound of Lemma 5.29 alone ($\mathbb{E}|Y| = \sum_j |p_jy_j|$).

Definition 5.30 (pieces of type TC and SG)**.** Let B be a box with $b^{-} > 0$, sign s, and $[m_1, m_2] \subset (0, 1]$.

- A TC piece with sign $s_3 \in \{1, -1\}$ is a rational cap $\kappa \in (0, 1]$ with $\kappa \ge \min(1, m_2/\sqrt{1-m_2^2})$ (that is, $\kappa = 1$, or $m_2 < 1$ and $\kappa^2(1-m_2^2) \ge m_2^2$), and a vertex certificate for $([t_1, t_2] \times [r_1, r_2] \times [m_1, m_2], (1, s, s_3), [u_1, u_2], \kappa, -)$.
- An SG piece (for $s_3 = -1$) is a rational p^* with $2m_1^2 > 1$ and $\varphi(m_1) \le p^* < 0$, a rational cap $\kappa \in (0, 1]$ with $\kappa \ge \min(m_2, \bar{m}(B))$, and a vertex certificate for $([t_1, t_2] \times [r_1, r_2], (1, s), [u_1, u_2], \kappa, p^*)$.

Lemma 5.31. *Let B be a box with $b^{-} > 0$ and consider a point of B with $r < 1$ whose remainder has $m = \max_{i \ge 3}|\beta_i| \in [m_1, m_2]$ and $\beta_{i_0} = s_3 m$.*

(i) If $[m_1, m_2]$ carries a TC piece with sign s_3, then $\mathbb{E}|L| < T_4$.

(ii) If $s_3 = -1$ and $[m_1, m_2]$ carries an SG piece, then $\mathbb{E}|L| < T_4$.

Proof. (i) If $m < 1$, Lemma 5.18 ($j = 1$) gives $\mathbb{E}|L| = \mathbb{E}F_{p_3(t,r,m)}(M')$ with $\mu(M') \le \min(1, m/\sqrt{1-m^2}) \le \min(1, m_2/\sqrt{1-m_2^2}) \le \kappa$, so $M' \in \mathcal{Z}$ and Lemma 5.25 applies. If $m = 1$, then $m_2 = 1$ and $\kappa = 1$, and $\mathbb{E}|L| = F_{p_3(t,r,1)}(y)$ for every y (Lemma 5.18(ii)); taking $Z = \chi' \in \mathcal{Z}$, $\mathbb{E}|L| = \mathbb{E}F_{p_3(t,r,1)}(Z) < T_4$ by Lemma 5.25. (ii) By Lemma 5.13 with $m_c = m_1$, $p_3(M) \le \varphi(m_1) \le p^*$. Also $m \le m_2$ and $m \le \bar{m}(B)$, so $m \le \kappa$. Thus $M \in \mathcal{Z}$, and Lemmas 5.18 ($j = 0$) and 5.25 give $\mathbb{E}|L| < T_4$. □

5.8.2 Four split coordinates

Lemma 5.32 (four-coordinate near-sphere bound)**.** *Consider a point with $r < 1$, $\beta_{i_0} = +m$ with $m < 1$, and suppose that M' has the coefficient $+m'$ at χ_{i_1}, where $m' = \mu(M')$. Let $Y_4 = a_1\chi_1 + sa_2\chi_2 + a_3\chi_{i_0} + a_4\chi_{i_1}$ with atoms y_j and probabilities p_j ($j = 1, \dots, 16$), and $r'' = \sqrt{a_1^2+a_2^2+a_3^2+a_4^2} = \sqrt{1-b'^2}$. Then*

$$\mathbb{E}|L| \le \mathbb{E}|Y_4| + \sum_j p_j \min\Big(b'', \ \frac{27}{128}\frac{b''^4E_4'}{|y_j|^3}\Big).$$

If moreover $q \in [q_5, q_4]$, all $y_j \ne 0$ and $\frac{27}{128}E_4'\,b''^2(1+r'')\sum_j p_j|y_j|^{-3} < T_4$, then $\mathbb{E}|L| < T_4$ if $b'' > 0$, and if $b'' = 0$ then $\mathbb{E}|L| = G_4(a_1, sa_2, a_3, a_4) \le T_4$.

Proof. If $m' = 1$ then $b'' = 0$ and $L = Y_4$ (Lemma 5.18(ii) with $j = 2$). Otherwise $L = Y_4 + b''M''$ with M'' independent of Y_4; conditioning on the four bits of Y_4 and applying Lemma 5.27 with $Z = M''$ gives the first bound. By Lemma 5.8, $\mathbb{E}|Y_4| = G_4(a_1, sa_2, a_3, a_4) \le T_4r''$. If $b'' > 0$, the hypothesis and $1 - r'' = b''^2/(1+r'')$ give $\mathbb{E}|L| < T_4r'' + T_4(1-r'') = T_4$. □

Piece tests (A4), (B4). Let B be a box with $b^- > 0$, $[m_1, m_2] \subset (0,1]$ and $[n_1, n_2] \subset (0,1]$. On $B \times [m_1, m_2] \times [n_1, n_2]$ (with $m \in [m_1, m_2]$, $m < 1$, and $m' \in [n_1, n_2]$) we enclose a_1, a_2, a_3 as in (A3), $b'^2 \in [(b'^2)^-, (b'^2)^+] = [(b^-)^2(1-m_2^2), (b^+)^2(1-m_1^2)]$, b' by the square roots of these bounds, $a_4 = b'm' \in [b'^- n_1, b'^+ n_2]$, $b''^2 \le (b''^2)^+ := (b'^2)^+(1-n_1^2)$, and $r'' \le r''^+ := \min\left(1, \sqrt{1-(b'^2)^-(1-n_2^2)}\right)$. The 16 atoms and the products $p_j y_j$ are enclosed as in (A3). The piece passes

- test (A4) if all $\eta_j > 0$ and $\frac{27}{128} E_4'^+ (b''^2)^+ (1 + r''^+) \sum_j p_j^+ \eta_j^{-3} < T^-(u_1, u_2)$;
- test (B4) if $\sum_j \left(|p_j y_j|^+ + p_j^+ \min\left(b''^+, \frac{27}{128}((b''^2)^+)^2 E_4'^+ / \eta_j^3\right)\right) < T^-(u_1, u_2)$.

Definition 5.33 (pieces of type TCS)**.** Let B be a box with $b^- > 0$, sign s, and $[m_1, m_2] \subset (0,1]$. A TCS piece is: a rational cap $\kappa \in (0,1]$ with $\kappa \ge \min(1, m_2/\sqrt{1-m_2^2})$; a rational $m_c' \in (0,1]$ and a rational p'^* with $2m_c'^2 > 1$ and $\varphi(m_c') \le p'^* < 0$; a vertex certificate $\mathcal{C}'$ for $(X_3, (1,s,1), [u_1, u_2], m_c', -)$ and a vertex certificate $\mathcal{C}''$ for $(X_3, (1,s,1), [u_1, u_2], \kappa, p'^*)$, where $X_3 = [t_1, t_2] \times [r_1, r_2] \times [m_1, m_2]$; and sub-pieces $[n_1, n_2] \subset (0,1]$, each passing (A4) or (B4) (on $B \times [m_1, m_2] \times [n_1, n_2]$), whose union contains $[m_c', \kappa]$.

Lemma 5.34. *Let $[m_1, m_2]$ carry a TCS piece for B. At every point of B with $r < 1$ and $q \in [q_5, q_4]$ whose remainder has $\beta_{i_0} = +m$, $m = \max|\beta_i| \in [m_1, m_2]$, we have $\mathbb{E}|L| \le T_4$. Equality forces $s = 1$ and $\alpha = \frac{1}{2}(e_1 + e_2 + e_{i_0} + e_{i_1})$ for some $i_1 \notin \{1, 2, i_0\}$.*

Proof. If $m = 1$: $\mathbb{E}|L| = F_{p_3(t,r,1)}(y)$ for every y (Lemma 5.18(ii)); take $Z = N^{-1/2}(\chi_1' + \cdots + \chi_N')$ with $N^{-1/2} \le m_c'$, which belongs to the class of $\mathcal{C}'$. Lemma 5.25 gives $\mathbb{E}|L| = \mathbb{E}F_{p_3(t,r,1)}(Z) < T_4$.

Now let $m < 1$. By Lemma 5.18,

$$\mathbb{E}|L| = \mathbb{E}F_{p_3(t,r,m)}(M'), \qquad m' = \mu(M') \le \min\left(1, m/\sqrt{1-m^2}\right) \le \kappa.$$

- If $m' \le m_c'$: M' is in the class of $\mathcal{C}'$, and Lemma 5.25 gives $\mathbb{E}|L| < T_4$.
- If $m' \ge m_c'$ and M' has the coefficient $-m'$ at some χ_{i_1}: by Lemma 5.13, $p_3(M') \le \varphi(m_c') \le p'^*$, and $m' \le \kappa$, so M' is in the class of $\mathcal{C}''$, and $\mathbb{E}|L| < T_4$.
- Otherwise M' has the coefficient $+m'$ at some χ_{i_1}, with $m' \in [m_c', \kappa]$, so m' lies in a sub-piece $[n_1, n_2]$, and $m \in [m_1, m_2]$. If the sub-piece passes (B4), Lemma 5.32 (first bound) gives $\mathbb{E}|L| < T_4$. If it passes (A4), Lemma 5.32 gives $\mathbb{E}|L| < T_4$ when $b'' > 0$, and $\mathbb{E}|L| = G_4(c) \le T_4$ with $c = (a_1, sa_2, a_3, a_4)$, $|c| = 1$, when $b'' = 0$.

In the last case with $b'' = 0$ (so $m' = 1$ and $a_4 = b' > 0$, as $m < 1$), equality means $G_4(c) = T_4|c|$. All entries of c are nonzero ($a_1 > 0$, $a_2 \ge |\alpha_{i_0}| = a_3 = bm > 0$, $a_4 > 0$), so by Lemma 5.8 (the alternative $c \parallel e_i + e_j + e_k$ has a zero entry), c is a positive multiple of $\pm(1,1,1,1)$; since $a_1, a_3, a_4 > 0$, $s = 1$ and $a_1 = a_2 = a_3 = a_4 = \frac{1}{2}$, i.e. $\alpha = \frac{1}{2}(e_1 + e_2 + e_{i_0} + e_{i_1})$. □

5.8.3 Five split coordinates

Lemma 5.35 (five-coordinate near-sphere bound)**.** *Consider a point with $r < 1$, $\beta_{i_0} = +m$ with $m < 1$, M' with the coefficient $+m'$ at χ_{i_1} ($m' = \mu(M') < 1$), and M'' with the coefficient $+m''$ at χ_{i_2} ($m'' = \mu(M'')$). Let $Y_5 = a_1\chi_1 + sa_2\chi_2 + a_3\chi_{i_0} + a_4\chi_{i_1} + a_5\chi_{i_2}$ with atoms y_j and probabilities p_j ($j = 1, \ldots, 32$), and $r''' = |(a_1, \ldots, a_5)| = \sqrt{1 - b'''^2}$. Then*

$$\mathbb{E}|L| \le \mathbb{E}|Y_5| + \sum_j p_j \min\left(b''', \ \frac{27}{128}\frac{b'''^4 E_4'}{|y_j|^3}\right).$$

If moreover $s = 1$, $q \in [q_5, q_4]$, $a_i > 0$ *and* $a_i > q\sum_{l=1}^5 a_l$ *for* $i = 1, \dots, 5$, *all* $y_j \neq 0$, *and* $\frac{27}{128} E_4' b'''^2 (1 + r''') \sum_j p_j |y_j|^{-3} < T_4$, *then* $\mathbb{E}|L| < T_4$ *if* $b''' > 0$, *and if* $b''' = 0$ *then* $\mathbb{E}|L| = 2\tau(1-q)^4 \sum_i a_i \leq T_4$, *with equality if and only if* $q = q_5$ *and* $a_1 = \cdots = a_5 = \frac{1}{\sqrt{5}}$.

Proof. If $m'' = 1$ then $b''' = 0$ and $L = Y_5$ (as in Lemma 5.18(ii), one level deeper: $M'' = \chi_{i_2}$). Otherwise peel M'' once more: $b''M'' = a_5\chi_{i_2} + b'''M'''$ with $M''' = (M'')^\flat$ independent of the five bits of Y_5 (5.7), so $L = Y_5 + b'''M'''$; conditioning on the five bits and applying Lemma 5.27 with $Z = M'''$ gives the first bound. Under the extra hypotheses, Lemma 5.6 (applied to $(a_1, \dots, a_5)$, as $s = 1$) gives $\mathbb{E}|Y_5| = G_5(a) = 2\tau(1-q)^4 \sum_i a_i \leq T_4 r'''$, with equality iff $q = q_5$ and $a_1 = \cdots = a_5$. If $b''' > 0$, the hypothesis and $1 - r''' = b'''^2/(1 + r''')$ give $\mathbb{E}|L| < T_4 r''' + T_4(1 - r''') = T_4$. If $b''' = 0$, then $r''' = 1$, $\mathbb{E}|L| = \mathbb{E}|Y_5| \leq T_4$, and equality holds iff $q = q_5$ and $a_i = \frac{1}{\sqrt{5}}$ for all i. □

Piece tests (A5), (B5). Let B be a box with $b^- > 0$ and $[m_1, m_2], [n_1, n_2], [o_1, o_2] \subset (0, 1]$. On $B \times [m_1, m_2] \times [n_1, n_2] \times [o_1, o_2]$ (with $m \in [m_1, m_2]$, $m' \in [n_1, n_2]$, $m'' \in [o_1, o_2]$, $m, m' < 1$) we enclose $a_1, \dots, a_4$ and b''^2 as in (A4) (with $(b''^2)^- = (b'^2)^-(1 - n_2^2)$), b'' by the square roots of the bounds of b''^2, $a_5 = b''m'' \in [b''^- o_1, b''^+ o_2]$, $b'''^2 \leq (b'''^2)^+ := (b''^2)^+(1 - o_1^2)$, and $r''' \leq r'''^+ := \min\left(1, \sqrt{1 - (b''^2)^-(1 - o_2^2)}\right)$. The 32 atoms and the products $p_j y_j$ are enclosed as before. Let a_i^- and a_i^+ be the lower and upper bounds of a_i and $q^+ = \frac{1}{1+u_1^2}$. The piece passes

- test (A5) if $s = 1$, $a_i^- > q^+ \sum_{l=1}^5 a_l^+$ for $i = 1, \dots, 5$, all $\eta_j > 0$, and $\frac{27}{128} E_4'^+ (b'''^2)^+ (1 + r'''^+) \sum_j p_j^+ \eta_j^{-3} < T^-(u_1, u_2)$;
- test (B5) if $\sum_j \left(|p_j y_j|^+ + p_j^+ \min\left(b'''^+, \frac{27}{128}((b'''^2)^+)^2 E_4'^+ / \eta_j^3\right)\right) < T^-(u_1, u_2)$.

In (A5), $\sum_l a_l^+ > 0$ (as $a_1^+ > 0$), so the first condition also gives $a_i > 0$, and it implies $a_i > q\sum_l a_l$ at every point. Thus, by Lemma 5.35: if a piece passes (A5), then at every point with $q \in [q_5, q_4]$ in its range, $\mathbb{E}|L| < T_4$ if $b''' > 0$ and $\mathbb{E}|L| \leq T_4$ if $b''' = 0$, with equality only as in Lemma 5.35; if it passes (B5), then $\mathbb{E}|L| < T_4$ at every $u \in [u_1, u_2]$ by the first bound alone ($\mathbb{E}|Y_5| = \sum_j |p_j y_j|$), for either sign s.

Definition 5.36 (inner pieces)**.** Let B be a box with $b^- > 0$ and sign s, $[m_1, m_2] \subset (0, 1]$, $X_3 = [t_1, t_2] \times [r_1, r_2] \times [m_1, m_2]$, $[n_1, n_2] \subset (0, 1]$ and $X_4 = X_3 \times [n_1, n_2]$.

- A TC4 piece with sign $s_4 \in \{1, -1\}$ is a rational cap $\kappa_4 \in (0, 1]$ with $\kappa_4 \geq \min(1, n_2/\sqrt{1 - n_2^2})$ and a vertex certificate for $(X_4, (1, s, 1, s_4), [u_1, u_2], \kappa_4, -)$.
- A TC4S piece is: a rational cap $\kappa_4 \in (0, 1]$ with $\kappa_4 \geq \min(1, n_2/\sqrt{1 - n_2^2})$; a rational m_c'' and a rational p''^* with $2m_c''^2 > 1$, $\varphi(m_c'') \leq p''^* < 0$ and $m_c'' < \kappa_4$; a vertex certificate $\mathcal{D}'$ for $(X_4, (1, s, 1, 1), [u_1, u_2], m_c'', -)$ and a vertex certificate $\mathcal{D}''$ for $(X_4, (1, s, 1, 1), [u_1, u_2], \kappa_4, p''^*)$; and sub-pieces $[o_1, o_2] \subset (0, 1]$, each passing (A5) or (B5) on $B \times [m_1, m_2] \times [n_1, n_2] \times [o_1, o_2]$, whose union contains $[m_c'', \kappa_4]$.
- An SG3 piece is a rational p'^* with $2n_1^2 > 1$ and $\varphi(n_1) \leq p'^* < 0$, a rational cap $\kappa_3 \in (0, 1]$ with $\kappa_3 \geq n_2$ or $\kappa_3 \geq \min(1, m_2/\sqrt{1 - m_2^2})$, and a vertex certificate for $(X_3, (1, s, 1), [u_1, u_2], \kappa_3, p'^*)$.

Definition 5.37 (pieces of type TCN)**.** Let B be a box with $b^- > 0$, sign s, and $[m_1, m_2] \subset (0, 1]$. A TCN piece is: a rational cap $\kappa \in (0, 1]$ with $\kappa \geq \min(1, m_2/\sqrt{1 - m_2^2})$; a rational m_c' with $0 < m_c' < \kappa$; a vertex certificate $\mathcal{C}'$ for $(X_3, (1, s, 1), [u_1, u_2], m_c', -)$; *inner plus pieces* $[n_1, n_2] \subset (0, 1]$, each passing (A4) or (B4) on $B \times [m_1, m_2] \times [n_1, n_2]$ or carrying a TC4 piece with $s_4 = 1$ or a TC4S piece, whose union contains $[m_c', \kappa]$; and *inner minus pieces* $[n_1, n_2] \subset (0, 1]$, each carrying an SG3 piece or a TC4 piece with $s_4 = -1$, whose union contains $[m_c', \kappa]$.

Lemma 5.38. *Let $[m_1, m_2]$ carry a TCN piece for B. At every point of B with $r < 1$ and $q \in [q_5, q_4]$ whose remainder has $\beta_{i_0} = +m$, $m = \max|\beta_i| \in [m_1, m_2]$, we have $\mathbb{E}|L| \le T_4$. Equality forces $s = 1$ and either $\alpha = \frac{1}{2}(e_1 + e_2 + e_{i_0} + e_{i_1})$, or $q = q_5$ and $\alpha = \frac{1}{\sqrt{5}}(e_1 + e_2 + e_{i_0} + e_{i_1} + e_{i_2})$, for some distinct $i_1, i_2 \notin \{1, 2, i_0\}$.*

Proof. If $m = 1$: as in Lemma 5.34, $\mathbb{E}|L| = F_{p_3(t,r,1)}(y)$ for every y, and $Z = N^{-1/2}(\chi'_1 + \cdots + \chi'_N)$ with $N^{-1/2} \le m'_c$ is in the class of $\mathcal{C}'$; so $\mathbb{E}|L| < T_4$.

Let $m < 1$. By Lemma 5.18 ($j = 1$), $\mathbb{E}|L| = \mathbb{E}F_{p_3(t,r,m)}(M')$ and $m' = \mu(M') \le \min(1, m/\sqrt{1-m^2}) \le \kappa$.

(1) $m' \le m'_c$: M' is in the class of $\mathcal{C}'$, and $\mathbb{E}|L| < T_4$ (Lemma 5.25).

(2) $m' \ge m'_c$, and M' has no coefficient $+m'$, so it has the coefficient $-m'$ at some χ_{i_1}. Then $m' \in [m'_c, \kappa]$ lies in an inner minus piece $[n_1, n_2]$.

- SG3: by Lemma 5.13 (with $m_c = n_1 \le m'$), $p_3(M') \le \varphi(n_1) \le p'^*$; and $m' \le \kappa_3$, since $m' \le n_2$ and $m' \le \min(1, m_2/\sqrt{1-m_2^2})$. So M' is in the class of the SG3 certificate (patch p_3, $\sigma = (1, s, 1)$), and $\mathbb{E}|L| < T_4$.
- TC4 with $s_4 = -1$: if $m' < 1$, Lemma 5.18 ($j = 2$, $\varsigma_2 = -1$) gives $\mathbb{E}|L| = \mathbb{E}F_{p_4(t,r,m,m')}(M'')$ with $\mu(M'') \le \min(1, n_2/\sqrt{1-n_2^2}) \le \kappa_4$, so $\mathbb{E}|L| < T_4$ by Lemma 5.25. If $m' = 1$, then $n_2 = 1$, $\kappa_4 = 1$, $\mathbb{E}|L| = F_{p_4(t,r,m,1)}(y)$ for every y (Lemma 5.18(ii)), and $Z = \chi'$ gives $\mathbb{E}|L| < T_4$.

(3) $m' \ge m'_c$ and M' has the coefficient $+m'$ at some χ_{i_1}. Then $m' \in [m'_c, \kappa]$ lies in an inner plus piece $[n_1, n_2]$, and $m \in [m_1, m_2]$.

- (A4) or (B4): Lemma 5.32 gives $\mathbb{E}|L| < T_4$, except in case (A4) with $b'' = 0$, where $\mathbb{E}|L| = G_4(a_1, sa_2, a_3, a_4) \le T_4$, with equality only for $s = 1$ and $\alpha = \frac{1}{2}(e_1 + e_2 + e_{i_0} + e_{i_1})$ (exactly as in the proof of Lemma 5.34).
- TC4 with $s_4 = 1$: as for $s_4 = -1$ above (now $\varsigma_2 = +1$), $\mathbb{E}|L| < T_4$.
- TC4S: if $m' = 1$, then $\mathbb{E}|L| = F_{p_4(t,r,m,1)}(y)$ for every y, and $Z = N^{-1/2}(\chi'_1 + \cdots + \chi'_N)$ with $N^{-1/2} \le m''_c$ is in the class of $\mathcal{D}'$; so $\mathbb{E}|L| < T_4$. If $m' < 1$, then $\mathbb{E}|L| = \mathbb{E}F_{p_4(t,r,m,m')}(M'')$ with $m'' = \mu(M'') \le \min(1, n_2/\sqrt{1-n_2^2}) \le \kappa_4$, and: if $m'' \le m''_c$, M'' is in the class of $\mathcal{D}'$; if $m'' \ge m''_c$ and M'' has no coefficient $+m''$, it has the coefficient $-m''$, so $p_3(M'') \le \varphi(m''_c) \le p''^*$ (Lemma 5.13) and M'' is in the class of $\mathcal{D}''$; in both cases $\mathbb{E}|L| < T_4$. Otherwise M'' has the coefficient $+m''$ at some χ_{i_2} with $m'' \in [m''_c, \kappa_4]$, so m'' lies in a sub-piece $[o_1, o_2]$, and Lemma 5.35 (via (A5) or (B5)) gives $\mathbb{E}|L| < T_4$, except in case (A5) with $b''' = 0$, where $\mathbb{E}|L| \le T_4$ with equality only if $q = q_5$ and $a_1 = \cdots = a_5 = \frac{1}{\sqrt{5}}$ (and $s = 1$, which (A5) requires). In that case $m'' = 1$, $M'' = \chi_{i_2}$, and $\alpha = \frac{1}{\sqrt{5}}(e_1 + e_2 + e_{i_0} + e_{i_1} + e_{i_2})$.

The indices i_0, i_1, i_2 are distinct and different from $1, 2$, because each peeling removes the peeled coordinate from the remainder. □

5.8.4 The m-split boxes

Definition 5.39 (m-split box)**.** An m-split box (kind ms5) is a box B with sign s, $r_2 < 1$ (so $b^- > 0$) and $u_1 \ge 2$, together with: a rational m_c with $0 < m_c < \min(1, \bar{m}(B))$; a vertex certificate $\mathcal{C}^{(1)}$ for $([t_1, t_2] \times [r_1, r_2], (1, s), [u_1, u_2], m_c, -)$; *plus pieces* $[m_1, m_2]$, each of type (A3), (B3), TC

with $s_3 = 1$, TCS or TCN, whose union contains $[m_c, \min(1, \bar{m}(B))]$; and *minus pieces* $[m_1, m_2]$, each of type SG or TC with $s_3 = -1$, whose union contains $[m_c, \min(1, \bar{m}(B))]$.

Lemma 5.40 (m-split lemma)**.** *Let B be an m-split box. At every point of B with $r < 1$ and $q \in [q_5, q_4]$ we have $\mathbb{E}|L| \le T_4$. Equality forces $s = 1$ and one of: $\alpha = \frac{1}{2}(e_1 + e_2 + e_{i_0} + e_{i_1})$; or $q = q_4$ and $\alpha = \frac{1}{\sqrt{3}}(e_1 + e_2 + e_{i_0})$; or $q = q_5$ and $\alpha = \frac{1}{\sqrt{5}}(e_1 + e_2 + e_{i_0} + e_{i_1} + e_{i_2})$ (with distinct indices outside $\{1, 2\}$).*

Proof. Recall $m \le \min(1, \bar{m}(B))$. If $m \le m_c$, use $\mathcal{C}^{(1)}$: by Lemmas 5.18 ($j = 0$) and 5.25, $\mathbb{E}|L| < T_4$. Let $m \ge m_c$. If $\beta_{i_0} = +m$ for some i_0, then m lies in a plus piece. A piece (B3) or TC gives $\mathbb{E}|L| < T_4$ (Lemma 5.31(i) for TC). A piece (A3) gives $\mathbb{E}|L| < T_4$ if $b' > 0$, and $\mathbb{E}|L| = G_3(a_1, sa_2, b) \le T_4$ if $b' = 0$ (i.e. $m = 1$); in the latter case equality forces, by Lemma 5.7, $q = q_4$ and (a_1, sa_2, b) to be a positive multiple of $\pm(1, 1, 1)$, so $s = 1$, $a_1 = a_2 = b = \frac{1}{\sqrt{3}}$ and $\beta = e_{i_0}$. A piece TCS gives $\mathbb{E}|L| \le T_4$ with equality only as in Lemma 5.34, and a piece TCN gives $\mathbb{E}|L| \le T_4$ with equality only as in Lemma 5.38. Otherwise the maximum m is attained only by negative coefficients, $\beta_{i_0} = -m$, and m lies in a minus piece; Lemma 5.31 gives $\mathbb{E}|L| < T_4$. □

5.9 Computer verification

All scripts and outputs are in the repository (`scripts/`, `outputs/`). Floating point (HiGHS linear programming via scipy, numpy) is used only to *find* certificates. Every *verification* is exact or uses outward-rounded interval arithmetic.

5.9.1 Data

The list of data files is `outputs/k4_manifest.json` ($U_- = \frac{1589}{625}$, $U_+ = \frac{29107}{10000}$, $T_8 = \frac{20711}{50000}$, $A_S = \frac{33}{100}$); md5 sums are in `outputs/k4_MD5SUMS.txt`.

- One-coordinate cells: `outputs/k4/one_0.json`, …, `one_3.json` ($u \in [U_-, \frac{66}{25}]$, $[\frac{66}{25}, \frac{273}{100}]$, $[\frac{273}{100}, \frac{141}{50}]$, $[\frac{141}{50}, U_+]$; 256, 257, 300 and 455 cells, all with degree-ten certificates), covering $u \in [U_-, U_+]$ and $a \in [0, \frac{33}{100}]$.
- Two-coordinate boxes: `outputs/k4/p_i.json` ($s = +1$) and `outputs/k4/m_i.json` ($s = -1$) for $i = 0, \ldots, 37$, on the u-slabs $[U_-, \frac{255}{100}]$, $[\frac{255}{100}, \frac{256}{100}]$, …, $[\frac{290}{100}, \frac{291}{100}]$, $[\frac{291}{100}, U_+]$. For each sign the boxes cover $[U_-, U_+] \times [0, T_8] \times [\frac{33}{100}, 1]$. Each file records $K = 4$ and $A_S = \frac{33}{100}$. Each box record has its kind and data: small, lpv (n_0, the vertices and one coefficient vector per vertex), ncA, and ms5 (m_c, $\mathcal{C}^{(1)}$ and the pieces, with their vertex certificates, caps, p^* values, sub-pieces and, for TCN, the inner pieces).

5.9.2 Generation

`scripts/run_k4.sh` writes the 80 jobs to `outputs/k4/jobs_all.txt` and runs them (7 parallel jobs by default). A two-coordinate job is `RQ_K=4 RQ_AS=33/100 RQ_MSD=5 RQ_TCN=`θ `python3 cover5.py u1 u2 s out.json` ν `4 8 16`, with $\theta = 1$ for the slabs with $u_1 \ge \frac{275}{100}$ and $\theta = 0$ otherwise, and $\nu = 1$ except for the plus slabs in $[\frac{286}{100}, \frac{289}{100}]$ ($\nu = 4$) and $[\frac{289}{100}, \frac{291}{100}]$ ($\nu = 8$), just below u_5: it bisects $[u_1, u_2] \times [0, T_8] \times [\frac{33}{100}, 1]$ adaptively (ν initial u-intervals, 4 initial t-intervals, 8 r-intervals, depth ≤ 16) and on each box tries, in order: small; the near-circle tests (`nearcircle.py`); a vertex certificate (`cert5.py`); from depth 5 on, the m-split (`cover5.try_ms5`, with $m_c \in \{\frac{9}{10}, \frac{17}{20}, \frac{4}{5}, \frac{3}{4}, \frac{1}{2}, \frac{9}{20}, \frac{2}{5}, \frac{3}{5}\}$; plus pieces in the order (A3)/(B3), TC, TCS with $m_c' \in$

sign	lpv	ncA	ms5	small	total
$s=+1$	3 327	0	2 718	0	6 045
$s=-1$	1 216	0	0	0	1 216

Table 5.1: Two-coordinate boxes for Theorem 5. Widths range from $7\cdot10^{-4}$ to 0.01 in u, from $3.2\cdot10^{-3}$ to 0.104 in t and from $5.2\cdot10^{-3}$ to 0.084 in r. The ms5 boxes use $m_c=\frac{1}{2}$ (2 194 boxes), $\frac{9}{20}$ (240), $\frac{3}{4}$ (104), $\frac{4}{5}$ (64), $\frac{3}{5}$ (62), $\frac{17}{20}$ (25), $\frac{9}{10}$ (18) and $\frac{2}{5}$ (11). Each has exactly one minus piece (211 SG, 2 507 TC) and between one and eight plus pieces (5 467 in total: 101 (A3), 2 681 TC, 1 438 TCS and 1 247 TCN). The TCS pieces have $m_c'=\frac{17}{20}$ (1 223) or $\frac{4}{5}$ (215) and 1 999 sub-pieces, all of type (A4). The TCN pieces have $m_c'=\frac{13}{20}$ (1 193), $\frac{3}{5}$ (38) or $\frac{11}{20}$ (16), and cap $\kappa=1$ (364) or $\kappa\in[0.681,0.999]$ (883); their inner plus pieces are 534 (A4), 2 479 TC4 and 216 TC4S (all with $m_c''=\frac{17}{20}$; 383 sub-pieces, all of type (A5)), and their inner minus pieces are 1 247 TC4 and 73 SG3. In total there are 21 014 vertex certificates (4 543 lpv, 2 718 $\mathcal{C}^{(1)}$, 5 188 TC, 211 SG, $2\times1\,438$ in TCS, 1 247 $\mathcal{C}'$ of TCN, 3 726 TC4, 2×216 in TC4S, 73 SG3) with 171 488 vertices; 7 472 of them have two patch parameters, 9 384 three and 4 158 four. The polynomials of 1 894 vertices have degree 10, all others degree 6.

$\{\frac{17}{20},\frac{4}{5},\frac{3}{4}\}$, and, if $\theta=1$, TCN with $m_c'\in\{\frac{13}{20},\frac{3}{5},\frac{11}{20}\}$, whose inner plus pieces are tried as (A4)/(B4), TC4 and TC4S with $m_c''\in\{\frac{17}{20},\frac{4}{5},\frac{3}{4}\}$, and whose inner minus pieces are tried as SG3 and TC4). Vertex sets with two or three patch parameters come from `cert5.py` (as for Theorem 4) and those with four parameters from `cert6.py`: n_0 is a rational approximation of the patch point at the centre with $|n_0|\geq1$, the polytope is a box in an exactly orthogonal rational basis of $n_0^{\perp}$ that contains the gnomonic projection of a 7^k (cert5) or 5^k (cert6) grid of the patch with a relative margin (none, enlarged to 1%, 4%, 10% and 25% if the cone check fails), and its corners are the vertices. The cone check is the exact test of Lemma 5.21 (`sphmin.py`; for $K=4$ `cert5.py` uses it as well). The coefficient vectors come from a discretised moment linear program (degree 6, or 10 if degree 6 fails), rounded to rationals and repaired; (W1), (W2) and (P1)–(P4) are checked exactly before a record is accepted. One-coordinate cells come from `cover_lp10.py` (degree-ten certificates). No box or cell failed.

The data were produced on 22 October 2026 between 13:12 and 15:33 UTC on one machine with 8 cores (at most 8 jobs at a time). The two-coordinate jobs took 8.5 hours in total (at most 75 minutes each); the five plus slabs in $[\frac{286}{100},\frac{291}{100}]$ took 40% of this time and produced 2 766 of the 7 261 boxes. These five slabs were first started with $\nu=1$, progressed too slowly and were restarted with the values of ν above; the jobs unfinished at that moment were restarted with unchanged commands (`outputs/k4/jobs_only*.txt`, `outputs/k4/logs/`).

5.9.3 Independent verification

`python3 verify_k4.py` re-checks everything from the data files, and all parts pass (output `outputs/verify_k4_ABCDEFG.txt`; 367 seconds on 8 cores, 46 minutes of CPU time). It shares no code with the generators (`cert2c`, `cert4`, `cert5`, `cert6`, `sphmin`, `cover5`, `cover_lp10`, `tenmom`, `nsphere3`, `nearcircle`, `exactcert`, `fourbit`, `bitlemma_k4`). It reuses the generic exact helpers of `verify_k3b.py` (the verifier of Theorem 4: moment polynomials, objective bound, facet normals, atom enclosures, envelopes, cap and φ checks, interval coverage) and the Sturm-sequence, integer-square-root and tiling helpers of `verify_all.py` (the verifier of Theorem 1, audited in A.6). Its parts:

A. Symbolic identities (sympy). Lemma 5.10: the cumulants of χ, computed from its moments,

are $d^{[j \text{ odd}]}G_j(w)$ for $j = 3, \ldots, 10$. Lemma 5.11: the recursion reproduces the Gaussian moments, and also the moments of χ at $u = \frac{5}{2}$, up to order ten.

B. Coverage (exact). $2 \le U_- \le u_4$ (checked as $U_-^2 \le 3$ or $(U_-^2 - 3)^2 \le 12$); $U_+ \ge u_5$ (checked as $U_+^2 \ge 4$ and $(U_+^2 - 4)^2 \ge 20$); (5.3); and $T_8 \ge \sqrt{2} - 1$. The cells tile $[U_-, U_+] \times [0, \frac{33}{100}]$. For each sign the boxes tile $[U_-, U_+] \times [0, T_8] \times [\frac{33}{100}, 1]$: they lie in the region, have pairwise disjoint interiors and total volume equal to the volume of the region (a closed subset of full measure is dense, so it is the whole region). Every small box satisfies $r_2 c(t_1) \le A_S$. Every file has $K = 4$ and $A_S = \frac{33}{100}$, and no file lists a failed box. Part B does not check the kinds; `scripts/k4_kinds_check.py` (output `outputs/k4_kinds_check.txt`) checks that every box has the sign of its file and one of the kinds small, lpv, ncA, ncB, ms5, so that one of the parts B, D, E, F checks it (data md5 sums as in `outputs/k4_MD5SUMS.txt`).

C. One-coordinate cells: (V1)–(V3) by Sturm sequences; $\Theta_1 > 0$; (V4) strictly (Definition 5.14 re-implemented: the polynomials μ_n from the recursion, the monomial bounds, and a Sturm count of the roots of h on $[0, \bar{m}]$ together with $h(0) > 0$).

D. Vertex certificates of every level: all lpv records, and inside ms5 records $\mathcal{C}^{(1)}$, TC, SG, $\mathcal{C}'$ and $\mathcal{C}''$ of TCS, and inside TCN pieces $\mathcal{C}'$, TC4 (both signs), $\mathcal{D}'$ and $\mathcal{D}''$ of TC4S, and SG3. (P1) and (P2) exactly; (P3) by exact Gaussian elimination (rank k of each facet, normal vector, orientation by the centre); (P4) by the recursion of Lemma 5.21 as described after it, in an implementation of its own (exact sign decisions, integer square-root bounds, no rounding of intermediate values); (W1) on every linear piece of every vertex envelope (Definition 5.22, recomputed from the atom enclosures over $[u_1, u_2]$); (W2) strictly with the target $T^-(u_1, u_2)$. The sign vector, caps and p^* values are taken from the structure: $\bar{m}(B)$ (recomputed exactly) for lpv, m_c for $\mathcal{C}^{(1)}$, m_c' for $\mathcal{C}'$, m_c'' for $\mathcal{D}'$, and the recorded cap $\kappa \in (0, 1]$ and the recorded $p^* < 0$ for the others.

E. Near-circle boxes: mpmath interval arithmetic (120 bits), tests (A)/(B) strictly, with $T^- = \min(T_4(u_1), T_4(u_2))$ enclosed in interval arithmetic.

F. m-split structure: $r_2 < 1$, $u_1 \ge 2$, $0 < m_c < \min(1, \bar{m}(B))$; the plus pieces and the minus pieces each cover $[m_c, \min(1, \bar{m}(B))]$; each (A3)/(B3) piece passes its test (mpmath, 120 bits, strict); the cap conditions $\kappa = 1$ or $\kappa^2(1 - m_2^2) \ge m_2^2$ of TC, TCS and TCN, and the analogous conditions with n_2 for TC4 and TC4S; the φ conditions ($0 < m \le 1$, $2m^2 > 1$, $p^* < 0$, and $p^* \ge \varphi(m)$, checked as $p^* + m^3 \ge 0$ and $(p^* + m^3)^2 \ge (1 - m^2)^3$) of SG, TCS, SG3 and TC4S; the cap conditions of SG ($\kappa \ge \min(m_2, \bar{m}(B))$) and SG3 ($\kappa_3 \ge n_2$ or the cap condition with m_2); $0 < m_c' < \kappa \le 1$ for TCN and $m_c'' < \kappa_4$ for TC4S; all nested covers (sub-pieces of TCS and TC4S, inner plus and minus pieces of TCN); and each (A4)/(B4) and (A5)/(B5) piece passes its test (mpmath, strict; (A5) includes $s = 1$ and the OR-region condition).

G. The claims (C1) and (C2) of Lemmas 5.7 and 5.8, for all 2^8 and all 2^{16} functions, exactly as described there, including the lists of equality cases (±OR of three bits at q_4 only; ±OR of four bits identically; ±OR of three of the four bits at q_4 only).

The generator side has its own exact check of the bit lemmas (`scripts/bitlemma_k4.py`, output `outputs/bitlemma_k4.txt`, same result).

Negative tests. `python3 break_tests_k4.py` corrupts random samples of records (seed 11) and runs the check functions of `verify_k4.py` on them (9 seconds; output `outputs/break_tests_k4.`

txt). Every corruption below is rejected in every case. On 40 lpv boxes: lowering the constant term of one vertex polynomial by $\frac{1}{20}$ (domination fails), raising it by 1 (the objective bound fails), shrinking the polytope by 10% about its centre (the cone check fails) and moving one vertex by 10^{-6} (the hyperplane/parallelepiped check fails). On 25 ms5 boxes: removing one plus piece or one minus piece, and lowering the top of the pieces by $\frac{1}{100}$ (coverage fails); replacing a TC/TCS/TCN cap by m_2 (97 cases; the cap check fails); lowering an SG value p^* to $\varphi(m_1) - \frac{1}{100}$ (25 cases); widening an (A4)/(B4) sub-piece from $[n_1, n_2]$ to $[\frac{n_1}{2}, n_2]$ (25 cases; the near-sphere test fails); lowering the constant term of a TC vertex polynomial by $\frac{1}{20}$ (20 cases). On 25 TCN pieces: removing one inner plus or minus piece, or lowering the inner cut m_c' by $\frac{1}{50}$ without adding pieces (coverage fails); replacing a TC4/TC4S cap by n_2 (the cap check fails); lowering the constant term of one nested vertex polynomial ($\mathcal{C}'$, TC4 or TC4S) by $\frac{1}{20}$. On 25 pieces each: lowering an SG3 value to $\varphi(n_1) - \frac{1}{100}$; widening an (A5)/(B5) sub-piece from $[o_1, o_2]$ to $[\frac{o_1}{4}, o_2]$ (the near-sphere test fails); re-checking an (A5) sub-piece with $s = -1$ (test (A5) must not pass, since the OR-region identity needs $s = 1$). On 40 nested polytopes with three or four patch parameters: shrinking by $\frac{1}{2}$ about the centre (the cone check fails). Finally, removing one box from the tiling, for each sign. Two sanity checks (not corruptions) hold: on the same 40 lpv boxes the recomputed cap $\bar{m}(B)$ is at least $\min(1, a_2/b)$ on the box, and for 20 nested vertex sets the exact facet minima of the cone check are at most the minima of $h \cdot p$ over a 7^k sample of the patch and within $10^{-3}|h|_\infty$ of them.

5.9.4 Reproducing

```
pip install numpy scipy sympy mpmath
cd scripts
python3 verify_k4.py          # parts A-G, about 6 minutes on 8 cores
python3 break_tests_k4.py     # negative tests, about 10 seconds
python3 bitlemma_k4.py        # bit lemmas (generator-side check)
bash run_k4.sh                # regenerate all data (8.5 job-hours)
```

5.10 Proof of Theorem 5

(a) By Lemma 5.3 let $q \in [q_5, q_4]$, i.e. $u \in [u_4, u_5] \subseteq [U_-, U_+]$. Reduce α as in Section 5.2.3.

(1) $a_1 = 1$: $\alpha = e_1$ and $\mathbb{E}|L| = 2\tau < T_4$ (Lemma 5.4(iii)).

(2) $a_1 \le \frac{33}{100}$: (u, a_1) lies in a cell, and Lemma 5.16 gives $\mathbb{E}|L| < T_4$.

(3) $a_1 > \frac{33}{100}$ and $r = 1$: $L = a_1\chi_1 + s a_2 \chi_2$, and Lemma 5.5 gives $\mathbb{E}|L| < T_4$.

(4) $a_1 > \frac{33}{100}$ and $r < 1$: (u, t, r) lies in a box of the cover for the sign s (part B), since $t \in [0, \sqrt{2} - 1] \subseteq [0, T_8]$ and $r \ge a_1 > \frac{33}{100}$. It is not a small box, since $a_1 > A_S$. If it is lpv, Lemma 5.26 gives $\mathbb{E}|L| < T_4$. If it is ncA, Lemma 5.28 gives $\mathbb{E}|L| < T_4$. If it is ms5, Lemma 5.40 gives $\mathbb{E}|L| \le T_4$.

So $\mathbb{E}|L| \le T_4$ always, and $(e_1 + e_2 + e_3 + e_4)/2$ attains T_4 (Lemma 5.4, $q < \frac{1}{4}$). Hence $R(q) = T_4(q)$. For $q \in [1 - q_4, 1 - q_5]$ use Lemma 5.3: $R(q) = R(1 - q) = 4q^3\tau$.

(b) Equality can occur only in the ms5 case of (4). By Lemma 5.40, after the reduction, $\alpha = \frac{1}{2}(e_1 + e_2 + e_{i_0} + e_{i_1})$, or $q = q_4$ and $\alpha = \frac{1}{\sqrt{3}}(e_1 + e_2 + e_{i_0})$, or $q = q_5$ and $\alpha = \frac{1}{\sqrt{5}}(e_1 + e_2 + e_{i_0} + e_{i_1} + e_{i_2})$. Undoing the reduction (global sign and permutation) gives the list in (b). Conversely, each listed vector attains T_4 at the stated q (Lemma 5.4): $(e_i + e_j + e_k + e_l)/2$ gives T_4 for $q < \frac{1}{4}$; $(e_i + e_j + e_k)/\sqrt{3}$ gives $T_3 = T_4$ at q_4; and $(e_{i_1} + \cdots + e_{i_5})/\sqrt{5}$ gives $T_5 = T_4$ at q_5. For $q \ge \frac{1}{2}$ use Lemma 5.3.

(c) For $q < q_5 < \frac{1}{5}$, $R(q) \geq \mathbb{E}|\chi_1 + \cdots + \chi_5|/\sqrt{5} = T_5(q) > T_4(q)$ by Lemma 5.4 and (ii). For $q_4 < q < \frac{1}{3}$, $R(q) \geq T_3(q) > T_4(q)$ by Lemma 5.4 and (i). For $\frac{1}{3} \leq q \leq \frac{1}{2}$, $R(q) \geq \mathbb{E}|\chi_1| = 2\tau$, and $2\tau > 4(1-q)^3\tau$ because $(1-q)^3 \leq (\frac{2}{3})^3 < \frac{1}{2}$. □

5.11 Remarks

1. **The $k = 4$ regime is closed.** $R(q) = 4(1-q)^3\sqrt{q(1-q)}$ holds exactly on $[q_5, q_4]$, which is the largest possible interval (Corollary 5.1). Both ends are ties: at q_4 with $(e_1+e_2+e_3)/\sqrt{3}$, at q_5 with $(e_1 + \cdots + e_5)/\sqrt{5}$. Given Theorem 4, Corollary 5.2 confirms the conjecture $R(q) = 2\tau \max_k \sqrt{k}\,\hat{q}^{\,k-1}$ (BF3, Stone; RQ-C's Conjecture S) on $[q_5, 1-q_5]$. The next regime, $k = 5$ on $[q_6, q_5]$ with $q_6 = 1 - \sqrt{5/6}$, is not treated here.

2. **Range of the computations.** The boxes and cells cover $u \in [U_-, U_+]$, slightly more than $[u_4, u_5]$. Outside $[u_4, u_5]$ the bit lemmas or the bound $T_5 \leq T_4$ fail, and tests (A3), (A4), (A5) would claim too much there; this is why the near-sphere lemmas, Lemmas 5.34, 5.38 and 5.40, and the proof of Theorem 5 use the data only for $q \in [q_5, q_4]$.

3. **Where the method is tight.** The m-split is used in 2 718 of the 6 045 boxes with $s = +1$ and in none with $s = -1$. TCS pieces occur in 684 boxes, all with $u \leq 2.76$; TCN pieces occur in 1 124 boxes, all with $u \geq 2.75$ (they are enabled only there), and TC4S pieces, the only place where test (A5) is used, in 96 boxes, all with $u \geq 2.83$. The five plus slabs in $[2.86, 2.91]$, next to u_5, are the most expensive part of the cover (2 766 boxes and 40% of the generation time; see the statistics after Table 5.1 and `outputs/k4_stats.txt`, written by `scripts/cover_stats5.py`).

4. **Status.** Audited VALID by RQ-AUD (A.25, 2026-10-22 16:53 UTC), with no fix to the mathematics; A.25 asked for two status updates (this item, and the parenthesis on Theorem 4 in Corollary 5.2, which A.18 and the referee RQ-REF1 have since rated VALID), and nothing else was changed. Refereed VALID by RQ-REF2 (2026-10-23 01:05 UTC), with no fixes; after that report only this item was changed. The computer steps have been run twice (generator and independent verifier), the verifier rejects corrupted data (negative tests above), and the referee re-did every computer step with its own exact programs.

Chapter 6

The $k = 5$ regime of $R(q)$: $R(q) = 2\sqrt{5}\,(1-q)^4\sqrt{q(1-q)}$ exactly for $1 - \sqrt{5/6} \le q \le 1 - \frac{2}{\sqrt{5}}$

Source: RQ-A, `MAIN_RESULT_K5.tex` (md5 `bc42dd0f7e4382da9668403529a0b747`), by "RQ-A (R(q) attack)", dated 22 October 2026. Its main result is Theorem 6 (claim MAIN-6), which keeps this name.

Refereed version: md5 `5b13f960a228c5903de80534ce7ba7b1`, the file in commit `6ecd564`. The source differs from it only in the status item of the closing remarks, which now records the referee's verdict.

Audit: A.37, VALID and NEW, no fix (22 October, 22:58 UTC). Its cosmetic remark r1 (the height counts in Table 6.1 and in item 4 of the closing remarks) was applied at 23:04–23:06 UTC.

Referee: RQ-REF2, VALID, no fixes (report `REFEREE.md`, md5 `bd18da81...`, written at 01:05 UTC on 23 October).

Use in the Main Theorem: none for the value of R, since the small-q chain covers $(0, q_5]$. Theorem 6 gives the extremisers on $[q_6, q_5]$, and Corollary 6.2 the formula on $[q_6, 1-q_6]$.

Transcription: the whole paper, with the mechanical changes of Appendix C: labels prefixed by `ch06:`, numbers n become $6.n$, the title becomes the chapter title, no table of contents, the abstract as a quoted block. No editorial footnotes.

Abstract of the source paper. For $q \in (0,1)$ let $\chi_1, \chi_2, \dots$ be i.i.d. normalised q-biased bits and let $R(q)$ be the supremum of $\mathbb{E}|\sum \alpha_i \chi_i|$ over unit vectors α. We prove that $R(q) = 2\sqrt{5}\,(1-q)^4\sqrt{q(1-q)}$ for every $q \in [q_6, q_5]$, where $q_6 = 1 - \sqrt{5/6} \approx 0.087129$ and $q_5 = 1 - 2/\sqrt{5} \approx 0.105573$ (and the mirror statement on $[1-q_5, 1-q_6]$). We also determine all extremisers: $(e_{i_1} + \cdots + e_{i_5})/\sqrt{5}$; at $q = q_5$ also $(e_i + e_j + e_k + e_l)/2$; and at $q = q_6$ also $(e_{i_1} + \cdots + e_{i_6})/\sqrt{6}$. The interval $[q_6, q_5]$ is exactly the set of $q \le \frac{1}{2}$ where this formula holds. With our Theorems 1–5 we obtain $R(q) = 2\sqrt{q(1-q)}\,\max_{k \ge 1} \sqrt{k}\,\hat{q}^{\,k-1}$, $\hat{q} = \max(q, 1-q)$, for all $q \in [q_6, 1-q_6]$. The proof follows our Theorem 5 (`MAIN_RESULT_K4`) with three changes: the target $2\sqrt{5}(1-q)^4\sqrt{q(1-q)}$ with $k = 5$ versions of the three- and four-bit lemmas; the m-split is organised as a tree of recursive *split nodes* (of level at most three), which peel up to four coordinates and end in near-sphere bounds with up to six coordinates; and the main extremiser $(e_1 + \cdots + e_5)/\sqrt{5}$, which is extremal for every q in the regime, and the tie $(e_1 + \cdots + e_6)/\sqrt{6}$ at q_6 are handled exactly by the OR-region identity. The computer-assisted steps (9166 boxes with 52 292 sets of vertex certificates, 861 cells, and the bit lemmas) use exact rational arithmetic and certified interval arithmetic, and an independent program repeated all of them.

6.1 Statement

Fix $q \in (0,1)$ and put

$$u = \sqrt{\tfrac{1-q}{q}}, \qquad v = \frac{1}{u}, \qquad \tau = \sqrt{q(1-q)}.$$

Let $\chi, \chi_1, \chi_2, \dots$ be i.i.d. with $\Pr[\chi = u] = q$ and $\Pr[\chi = -v] = 1-q$, so that $\mathbb{E}\chi = 0$, $\mathbb{E}\chi^2 = 1$ and $\mathbb{E}|\chi| = 2\tau$. Let

$$R(q) = \sup_{n \ge 1} \sup_{\alpha \in \mathbb{R}^n \setminus \{0\}} \frac{\mathbb{E}|\sum_{i=1}^n \alpha_i \chi_i|}{|\alpha|_2}.$$

Put

$$q_5 = 1 - \tfrac{2}{\sqrt{5}} \approx 0.105573, \qquad q_6 = 1 - \sqrt{\tfrac{5}{6}} \approx 0.087129,$$

and, for $k \ge 1$, $T_k = 2\sqrt{k}\,(1-q)^{k-1}\tau$; thus

$$T_2 = 2\sqrt{2}\,(1-q)\,\tau, \quad T_4 = 4(1-q)^3\,\tau, \quad T_5 = 2\sqrt{5}\,(1-q)^4\,\tau, \quad T_6 = 2\sqrt{6}\,(1-q)^5\,\tau.$$

Theorem 6. *(a) For every $q \in [q_6, q_5]$, every $n \ge 1$ and every $\alpha \in \mathbb{R}^n$ with $|\alpha|_2 = 1$,*

$$\mathbb{E}\Big|\sum_{i=1}^n \alpha_i \chi_i\Big| \le 2\sqrt{5}\,(1-q)^4 \sqrt{q(1-q)}.$$

For $q \in [1-q_5, 1-q_6]$ the same holds with $1-q$ replaced by q. Consequently $R(q) = 2\sqrt{5}\max(q,1-q)^4\sqrt{q(1-q)}$ for $q \in [q_6,q_5] \cup [1-q_5, 1-q_6]$.

(b) (Extremisers.) Let $q \in [q_6,q_5] \cup [1-q_5,1-q_6]$. Equality in (a) holds if and only if $\alpha = \pm\frac{1}{\sqrt{5}}(e_{i_1} + \cdots + e_{i_5})$ with $i_1, \dots, i_5$ distinct, or $q \in \{q_5, 1-q_5\}$ and $\alpha = \pm\frac{1}{2}(e_i + e_j + e_k + e_l)$ with i,j,k,l distinct, or $q \in \{q_6, 1-q_6\}$ and $\alpha = \pm\frac{1}{\sqrt{6}}(e_{i_1} + \cdots + e_{i_6})$ with $i_1, \dots, i_6$ distinct.

(c) (Sharpness.) $R(q) > T_5(q)$ for $q \in (0,q_6) \cup (q_5, \frac{1}{2}]$. More precisely, $R(q) \ge T_6(q) > T_5(q)$ for $q < q_6$, $R(q) \ge T_4(q) > T_5(q)$ for $q_5 < q < \frac{1}{4}$, and $R(q) \ge 2\tau > T_5(q)$ for $\frac{1}{4} \le q \le \frac{1}{2}$.

Corollary 6.1 (the whole $k=5$ regime)**.** $\{q \in (0, \frac{1}{2}] : \ R(q) = T_5(q)\} = [q_6, q_5]$, *and* $\{q \in [\frac{1}{2}, 1) : R(q) = 2\sqrt{5}\,q^4\tau\} = [1-q_5, 1-q_6]$.

Proof. Theorem 6(a) and (c), and Lemma 6.3 for the mirror statement. □

Corollary 6.2. *With Theorem 5 of `MAIN_RESULT_K4` ($R = T_4$ on $[q_5, q_4]$, $q_4 = 1 - \frac{\sqrt{3}}{2}$; MAIN-5, audited VALID as A.25) and Theorems 1–4 (`MAIN_RESULT`, `MAIN_RESULT_K2`, `MAIN_RESULT_K3`, `MAIN_RESULT_K3B`; audited VALID as A.6, A.11, A.14, A.18 and refereed VALID),*

$$R(q) = 2\sqrt{q(1-q)} \max_{k \ge 1} \sqrt{k}\,\hat{q}^{\,k-1}, \qquad \hat{q} = \max(q, 1-q),$$

for all $q \in [q_6, 1-q_6] = [1 - \sqrt{5/6}, \sqrt{5/6}]$.

Proof. By Lemma 6.3 let $q \le \frac{1}{2}$, so $\hat{q} = 1-q$. On $[q_5, \frac{1}{2}]$ this is Corollary 2 of `MAIN_RESULT_K4` (which combines Theorems 1–5). On $[q_6, q_5]$, Theorem 6 gives $R(q) = 2\tau\sqrt{5}(1-q)^4$, and $\sqrt{5}(1-q)^4 = \max_k \sqrt{k}(1-q)^{k-1}$ there. Indeed, for $k \le 4$, $\sqrt{k}(1-q)^{k-1} \le \sqrt{5}(1-q)^4$ iff $(1-q)^{2(5-k)} \ge \frac{k}{5}$, and $(1-q)^2 \ge \frac{4}{5}$ (as $q \le q_5$) gives $(1-q)^{2(5-k)} \ge (\frac{4}{5})^{5-k} \ge \frac{k}{5}$, since $5(\frac{4}{5})^{5-k}$ equals 2.048, 2.56, 3.2, 4 for $k = 1,2,3,4$. For $k \ge 6$, $\sqrt{k}(1-q)^{k-1} \le \sqrt{5}(1-q)^4$ iff $(1-q)^{2(k-5)} \le \frac{5}{k}$, and $(1-q)^2 \le \frac{5}{6}$ (as $q \ge q_6$) gives $(1-q)^{2(k-5)} \le (\frac{5}{6})^{k-5} \le \frac{5}{k}$, because the sequence $\frac{k}{5}(\frac{5}{6})^{k-5}$ equals 1 at $k=6$ and decreases for $k \ge 6$ ($\frac{k+1}{k} \cdot \frac{5}{6} \le \frac{7}{6} \cdot \frac{5}{6} < 1$). □

Part (c) and the lower bound $R \ge T_5$ in (a) are elementary (Lemma 6.4). The content is the upper bound in (a), and (b).

Relation to Theorem 5. The proof follows `MAIN_RESULT_K4` (Theorem 5) step by step. The changes are:

(i) the target T_5, the range $u \in [u_5, u_6]$ (Section 6.2) and the threshold $A_S = \frac{1}{4}$ of the one-coordinate route;

(ii) $k = 5$ versions of the three- and four-bit lemmas ($\sum_i \Delta_i(f)^2 \le 20(1-q)^8$ on $[q_6, q_5]$; Lemmas 6.7 and 6.8);

(iii) the OR-region identity (Lemma 6.6) now carries the main extremiser $(e_1+\cdots+e_5)/\sqrt{5}$, which is extremal on the whole regime, and with six coordinates the tie $(e_1+\cdots+e_6)/\sqrt{6}$ at q_6;

(iv) the m-split is a tree of recursive *split nodes* (Section 6.8, Definition 6.30 and Lemma 6.31): children of TCN pieces have level at most two, and the child of a TCS piece in a node of level two has level three (it has only near-sphere and SG pieces); the proof allows near-sphere bounds with three to six coordinates, and the data use four, five and six (Table 6.1); the pieces TC4, TC4S and SG3 of Theorem 5 are the plus and minus pieces of a split node of level one; vertex certificates are used for patches with up to five parameters.

The lemmas that are unchanged from Theorem 5 are proved again here, so that the document can be read on its own.

Conventions. $x_+ = \max(x, 0)$. All polynomials in the computer-assisted parts have rational coefficients. "Verified" means verified in exact rational arithmetic or in outward-rounded interval arithmetic, as specified in Section 6.9. For a rational $x \ge 0$ and an integer $N \ge 1$, *rational lower and upper bounds of* $\sqrt{x}$ are $\lfloor N\sqrt{x} \rfloor / N$ and $(\lfloor N\sqrt{x} \rfloor + 1)/N$ computed with integer square roots (the verifier uses $N = 10^{15}$).

6.2 Reductions

6.2.1 Symmetry and parametrisation

Lemma 6.3. *The law of $-\chi^{(q)}$ is the law of $\chi^{(1-q)}$. Hence $\mathbb{E}|\sum \alpha_i \chi_i^{(q)}| = \mathbb{E}|\sum \alpha_i \chi_i^{(1-q)}|$, $R(q) = R(1-q)$, and the extremisers for q and $1-q$ coincide.*

Proof. $-\chi^{(q)}$ takes the value $-u_q$ with probability q and v_q with probability $1-q$; since $u_{1-q} = v_q$ and $v_{1-q} = u_q$, this is the law of $\chi^{(1-q)}$. Finally $|\sum \alpha_i(-\chi_i)| = |\sum \alpha_i \chi_i|$. □

From now on $q \le \frac{1}{2}$, i.e. $u \ge 1$, and

$$q = \frac{1}{1+u^2}, \quad 1-q = \frac{u^2}{1+u^2}, \quad v = \frac{1}{u}, \quad \tau = \frac{u}{1+u^2}, \quad qu = (1-q)v = \tau. \tag{6.1}$$

On $u \ge 1$, τ and q are decreasing and $1-q$ is increasing in u. The target is

$$T_5 = 2\sqrt{5}\,(1-q)^4\tau = \frac{2\sqrt{5}\,u^9}{(1+u^2)^5}, \qquad \frac{d}{du}\frac{u^9}{(1+u^2)^5} = \frac{u^8(9-u^2)}{(1+u^2)^6},$$

so T_5 is increasing on $[1,3]$ and decreasing on $[3,\infty)$. Hence, for $1 \le u_1 < u_2$ and $u \in [u_1, u_2]$,

$$T_5(u) \;\ge\; \min\{T_5(u_1), T_5(u_2)\} \;\ge\; T^-(u_1,u_2) := \sqrt{5}^{\,-} \min\left\{\frac{2u_1^9}{(1+u_1^2)^5}, \frac{2u_2^9}{(1+u_2^2)^5}\right\}: \tag{6.2}$$

if $u \le 3$ then T_5 is increasing on $[u_1, u]$, and if $u \ge 3$ it is decreasing on $[u, u_2]$; here $\sqrt{5}^-$ is a fixed rational lower bound of $\sqrt{5}$ (the verifier uses $N = 10^{15}$). For rational u_1, u_2 the number $T^-(u_1, u_2)$ is rational. The range $q \in [q_6, q_5]$ corresponds to $u \in [u_5, u_6]$ with

$$u_5 = \sqrt{4 + 2\sqrt{5}} \approx 2.9106934, \qquad u_6 = \sqrt{5 + \sqrt{30}} \approx 3.2368543,$$

because $(1 - q_5)/q_5 = \frac{2}{\sqrt{5}-2} = 2(\sqrt{5} + 2) = 4 + 2\sqrt{5}$ and $(1 - q_6)/q_6 = \frac{\sqrt{5}}{\sqrt{6}-\sqrt{5}} = \sqrt{5}(\sqrt{6} + \sqrt{5}) = 5 + \sqrt{30}$. We fix the rationals

$$U_- = \frac{29106}{10000} = 2.9106 \ \le u_5, \qquad U_+ = \frac{3236855}{1000000} = 3.236855 \ \ge u_6.$$

Indeed $U_-^2 > 4$ and $(U_-^2 - 4)^2 \le 20$, so $U_-^2 \le 4 + 2\sqrt{5}$; and $U_+^2 > 5$ and $(U_+^2 - 5)^2 \ge 30$, so $U_+^2 \ge 5 + \sqrt{30}$. The computations cover $u \in [U_-, U_+]$; the theorem uses only $u \in [u_5, u_6]$. We also record that $w_- = U_-^2/(1 + U_-^2)$ (the value of $1 - q$ at $u = U_-$) satisfies

$$5w_-^8 > 1, \qquad 5w_-^6 > 2 \tag{6.3}$$

(exact check; $w_- \approx 0.894421$, $5w_-^8 \approx 2.05$, $5w_-^6 \approx 2.56$). Since $1 - q$ increases with u, $5(1 - q)^8 > 1$ and $5(1 - q)^6 > 2$ for all $u \ge U_-$.

6.2.2 Values of a few vectors

Lemma 6.4. *Let $k \ge 1$ and $q < 1/k$. Then $\mathbb{E}|\chi_1 + \cdots + \chi_k|/\sqrt{k} = 2\sqrt{k}\,(1 - q)^{k-1}\tau = T_k$. In particular $\mathbb{E}|\chi_1| = 2\tau$. Moreover, for all $q \in (0, 1)$:*

(i) $T_4 \le T_5$ iff $q \le q_5$, with equality iff $q = q_5$;

(ii) $T_6 \le T_5$ iff $q \ge q_6$, with equality iff $q = q_6$; and $T_{k+1} \le T_k$ for every $k \ge 6$ and $q \ge q_6$;

(iii) for $u \ge U_-$ (in particular for $q \in [q_6, q_5]$): $2\tau < T_5$ and $T_2 < T_5$.

Proof. Let $S = \chi_1 + \cdots + \chi_k$ and let $x_i = \mathbf{1}\{\chi_i = u\}$. If some $x_i = 1$ then $S \ge u - (k - 1)v > 0$, because $u^2 > k - 1$ is equivalent to $q < 1/k$. If all $x_i = 0$ then $S = -kv < 0$. So $|S| = fS$ with $f = 1 - 2 \cdot \mathbf{1}\{\text{all } x_i = 0\}$. Since $\mathbb{E}\chi_i = 0$, $\mathbb{E}[f\chi_i] = -2\mathbb{E}[\chi_i \mathbf{1}\{\text{all } x = 0\}] = -2(1 - q)^k(-v) = 2(1-q)^{k-1}(1-q)v = 2(1-q)^{k-1}\tau$. Summing over i gives $\mathbb{E}|S| = 2k(1-q)^{k-1}\tau$. The comparisons: (i) $4(1-q)^3 \le 2\sqrt{5}(1-q)^4$ iff $1 - q \ge \frac{2}{\sqrt{5}}$; (ii) $T_{k+1} \le T_k$ iff $\sqrt{k+1}(1-q) \le \sqrt{k}$ iff $1 - q \le \sqrt{k/(k+1)}$, which for $k = 5$ is $q \ge q_6$, and for $k \ge 6$ follows from $1 - q \le \sqrt{5/6} \le \sqrt{k/(k+1)}$; (iii) $2\tau < 2\sqrt{5}(1 - q)^4\tau$ iff $5(1 - q)^8 > 1$, and $2\sqrt{2}(1 - q)\tau < 2\sqrt{5}(1 - q)^4\tau$ iff $5(1 - q)^6 > 2$; both hold for $u \ge U_-$ by (6.3). □

6.2.3 Splitting off the two largest coefficients

Let $|\alpha|_2 = 1$ and $L = \sum \alpha_i \chi_i$. Changing the sign of α and permuting coordinates does not change $\mathbb{E}|L|$. So we may assume

$$a_1 := \alpha_1 = \max_i |\alpha_i| > 0, \qquad a_2 := |\alpha_2| = \max_{i \ge 2} |\alpha_i|, \qquad |\alpha_3| \ge |\alpha_4| \ge \cdots,$$

and we put $s = \operatorname{sgn} \alpha_2 \in \{1, -1\}$ ($s = 1$ if $\alpha_2 = 0$),

$$r = \sqrt{a_1^2 + a_2^2} \in (0, 1], \qquad b = \sqrt{1 - r^2}.$$

If $r < 1$, let $\beta_i = \alpha_i/b$ for $i \ge 3$ and $M = \sum_{i\ge3} \beta_i\chi_i$. Then

$$L = a_1\chi_1 + s\,a_2\chi_2 + bM, \qquad \sum_{i\ge3}\beta_i^2 = 1, \qquad m := \max_{i\ge3}|\beta_i| = \frac{|\alpha_3|}{b} \le \min\Big(1, \frac{a_2}{b}\Big),$$

and M is independent of (χ_1, χ_2). We use half-angle coordinates for (a_1, a_2):

$$a_1 = r\,c(t), \quad a_2 = r\,d(t), \qquad c(t) = \frac{1-t^2}{1+t^2}, \quad d(t) = \frac{2t}{1+t^2}, \qquad t = \frac{a_2}{r+a_1}.$$

Since $0 \le a_2 \le a_1$, the angle θ with $\tan\theta = a_2/a_1$ is in $[0, \pi/4]$ and $t = \tan(\theta/2) \in [0, \sqrt{2}-1]$. We fix $T_8 = \frac{20711}{50000} = 0.41422 \ge \sqrt{2}-1$ (indeed $(T_8+1)^2 \ge 2$). On $[0,1]$, c is decreasing and d is increasing in t, both are ≥ 0, and $c^2 + d^2 = 1$. Thus every unit α gives a point

$$(u, t, r, s) \in [U_-, U_+] \times [0, T_8] \times (0, 1] \times \{1, -1\} \qquad (u \in [u_5, u_6]).$$

We put $A_S = \frac{1}{4}$. If $a_1 \le A_S$ we use the one-coordinate route of Section 6.5; otherwise $r \ge a_1 > A_S$ and we use the two-coordinate route of Sections 6.6–6.8.

6.3 Exact evaluations

6.3.1 Two coordinates

Lemma 6.5 (two-coordinate value)**.** *Let $q \le \frac{1}{2}$, $c, d \ge 0$, $s \in \{1, -1\}$, and $X = c\chi_1 + s\,d\chi_2$. List the atoms of X as $(\chi_1, \chi_2) = (u,u), (u,-v), (-v,u), (-v,-v)$, with probabilities $p = (q^2,\ q(1-q),\ q(1-q),\ (1-q)^2)$ and values x_j. Then $p_j x_j = \tau g_j$ with*

$$g = \big(q(c+sd),\ (1-q)c - s\,q\,d,\ -q\,c + s(1-q)d,\ -(1-q)(c+sd)\big), \tag{6.4}$$

and

$$\mathbb{E}|X| = 2\tau\max\{c,\ d,\ [s=1]\,(1-q)(c+d)\}$$

(the last entry is present only for $s = 1$). Consequently $\mathbb{E}|X| \le \max(2\tau, T_2)\sqrt{c^2+d^2}$, and if $u \ge U_-$ and $(c,d) \ne 0$, then $\mathbb{E}|X| < T_5\sqrt{c^2+d^2}$.

Proof. The identities $p_j x_j = \tau g_j$ follow from (6.1); for example $q(1-q)(cu - sdv) = (1-q)\tau c - q\tau sd$. Since $\mathbb{E}X = 0$, $\mathbb{E}|X| = 2\mathbb{E}X_+ = 2\tau\sum_j (g_j)_+$. For $s = 1$: $g_1 \ge 0 \ge g_4$, so $\mathbb{E}X_+/\tau = q(c+d) + ((1-q)c - qd)_+ + ((1-q)d - qc)_+$. If both middle terms are nonnegative this equals $(1-q)(c+d)$, and then $(1-q)(c+d) - c = (1-q)d - qc \ge 0$ and similarly $\ge d$. If only the first is nonnegative it equals $q(c+d) + (1-q)c - qd = c$, and $(1-q)(c+d) - c = (1-q)d - qc < 0$, while $c \ge d$ (otherwise $(1-q)d - qc \ge (1-2q)c \ge 0$). The case where only the second is nonnegative is symmetric. Both negative would give $(1-q)(c+d) < q(c+d)$, impossible for $q \le \frac{1}{2}$ unless $c = d = 0$. In all cases $\mathbb{E}X_+/\tau = \max\{c, d, (1-q)(c+d)\}$. For $s = -1$: $g_2 \ge 0 \ge g_3$. If $c \ge d$ then $g_1 \ge 0 \ge g_4$ and $\mathbb{E}X_+/\tau = q(c-d) + (1-q)c + qd = c$. If $c < d$ then $g_1 < 0 < g_4$ and $\mathbb{E}X_+/\tau = (1-q)c + qd + (1-q)(d-c) = d$. So $\mathbb{E}X_+/\tau = \max(c,d)$.

For the bound let $\rho = \sqrt{c^2+d^2}$. Then $\max(c,d) \le \rho$ and $(1-q)(c+d) \le \sqrt{2}(1-q)\rho$, so $\mathbb{E}|X| \le \max(2\tau\rho, 2\sqrt{2}(1-q)\tau\rho) = \max(2\tau, T_2)\rho$. For $u \ge U_-$ and $\rho > 0$ this is $< T_5\rho$ by Lemma 6.4(iii). □

6.3.2 Bits, OR functions and the OR region

For $n \geq 1$, $f : \{0,1\}^n \to [-1,1]$ and $x_i = \mathbf{1}\{\chi_i = u\}$ put $\Delta_i(f) = \mathbb{E}[f \mid x_i = 1] - \mathbb{E}[f \mid x_i = 0]$, a polynomial in q. Then, by (6.1),

$$\mathbb{E}[f\chi_i] = qu\,\mathbb{E}[f \mid x_i = 1] - (1-q)v\,\mathbb{E}[f \mid x_i = 0] = \tau\,\Delta_i(f). \tag{6.5}$$

For $c \in \mathbb{R}^n$ write $G_n(c) = \mathbb{E}|c_1\chi_1 + \cdots + c_n\chi_n|$. For a set $S \subseteq \{1,\dots,n\}$ let $\mathrm{OR}_S = 2 \cdot \mathbf{1}\{\exists i \in S : x_i = 1\} - 1$. By the computation in the proof of Lemma 6.4,

$$\Delta_i(\mathrm{OR}_S) = 2(1-q)^{|S|-1} \ (i \in S), \qquad \Delta_i(\mathrm{OR}_S) = 0 \ (i \notin S). \tag{6.6}$$

(For $i \in S$: $\mathbb{E}[\mathrm{OR}_S \mid x_i = 1] = 1$ and $\mathbb{E}[\mathrm{OR}_S \mid x_i = 0] = 1 - 2(1-q)^{|S|-1}$; for $i \notin S$, OR_S does not depend on x_i.)

Lemma 6.6 (OR-region identity)**.** *Let $n \geq 1$, $q \in (0,1)$ and $c \in \mathbb{R}^n$ with $c_i > 0$ and $c_i > q\sum_{l=1}^n c_l$ for every i. Then*

$$G_n(c) = 2\tau(1-q)^{n-1}\sum_{i=1}^n c_i \ \leq \ 2\sqrt{n}\,(1-q)^{n-1}\tau\,|c|.$$

In particular $G_5(c) \leq T_5|c|$, with equality if and only if $c_1 = \cdots = c_5$; and for $q \geq q_6$, $G_6(c) \leq T_6|c| \leq T_5|c|$, where $G_6(c) = T_5|c|$ holds if and only if $q = q_6$ and $c_1 = \cdots = c_6$.

Proof. Let $S = \sum_l c_l\chi_l$. If all $x_l = 0$ then $S = -v\sum_l c_l < 0$. Otherwise pick i with $x_i = 1$. Every l with $x_l = 1$ contributes $c_l u$ instead of $-c_l v$, a gain of $c_l(u+v) > 0$, so $S \geq c_i u - v\sum_{l\neq i} c_l = c_i(u+v) - v\sum_l c_l$. By (6.1), $u + v = (1+u^2)/u = v/q$, so $S \geq \frac{v}{q}\big(c_i - q\sum_l c_l\big) > 0$. Hence $|S| = \mathrm{OR}_{\{1,\dots,n\}} \cdot S$, and by (6.5) and (6.6), $G_n(c) = \sum_i c_i\mathbb{E}[\mathrm{OR}\,\chi_i] = \tau\sum_i c_i \cdot 2(1-q)^{n-1}$. The inequality is Cauchy–Schwarz, $\sum_i c_i \leq \sqrt{n}|c|$, with equality iff all c_i are equal. For $n = 5$ the bound is $T_5|c|$. For $n = 6$ it is $T_6|c|$, and $T_6 \leq T_5$ for $q \geq q_6$ with equality iff $q = q_6$ (Lemma 6.4(ii)). So $G_6(c) = T_5|c|$ forces equality in both steps, i.e. $c_1 = \cdots = c_6$ and $q = q_6$; conversely these give equality. □

6.3.3 Three and four bits for $k = 5$

Lemma 6.7 (three-bit lemma for $k = 5$)**.** *Let $q \in [q_6, q_5]$ and $c \in \mathbb{R}^3$, $c \neq 0$. Then $G_3(c) < T_5\,|c|$.*

Lemma 6.8 (four-bit lemma for $k = 5$)**.** *Let $q \in [q_6, q_5]$ and $c \in \mathbb{R}^4$. Then $G_4(c) \leq T_5\,|c|$. For $c \neq 0$ equality holds if and only if $q = q_5$ and c is a positive multiple of $\pm(e_1 + e_2 + e_3 + e_4)$.*

Proof of Lemmas 6.7 and 6.8. Let $n \in \{3,4\}$, $X = c\cdot\chi$ and $f^* = \operatorname{sgn} X$ (with $\operatorname{sgn} 0 = 1$), a function of $(x_1,\dots,x_n)$ with values ± 1. By (6.5) and Cauchy–Schwarz,

$$G_n(c) = \mathbb{E}[f^*X] = \tau\sum_i c_i\Delta_i(f^*) \leq \tau|c|\,|\Delta(f^*)|.$$

For $f : \{0,1\}^n \to \{-1,1\}$ put $H_f(q) = 20(1-q)^8 - \sum_{i=1}^n \Delta_i(f)^2$, a polynomial with integer coefficients. *Claims* (finite exact computations, Section 6.9, part G):

(C1) ($n = 3$, all 2^8 functions) $H_f > 0$ on $[q_6, q_5]$.

(C2) ($n = 4$, all 2^{16} functions) $H_f \geq 0$ on $[q_6, q_5]$; no H_f vanishes identically; $H_f(q_5) = 0$ exactly for $f = \pm\mathrm{OR}_{\{1,2,3,4\}}$, and these two H_f are > 0 on $[q_6, q_5)$; every other H_f is > 0 on $[q_6, q_5]$.

Given the claims, $|\Delta(f)| \le 2\sqrt{5}(1-q)^4$ for all f, so $G_n(c) \le \tau|c| \cdot 2\sqrt{5}(1-q)^4 = T_5|c|$ on $[q_6, q_5]$. If equality holds with $c \neq 0$, then both inequalities are equalities: $H_{f^*}(q) = 0$, and c is a positive multiple of $\Delta(f^*) \neq 0$ (equality in Cauchy–Schwarz with $\sum_i c_i\Delta_i(f^*) > 0$). By the claims, $n = 4$, $q = q_5$ and $f^* = \pm\mathrm{OR}_{\{1,2,3,4\}}$, so $\Delta(f^*) = \pm 2(1-q)^3(1,1,1,1)$ by (6.6). In particular equality never holds for $n = 3$. Conversely, at q_5 the vector $c = \pm(1,1,1,1)$ gives $G_4(c) = T_4|c| = T_5|c|$ by Lemma 6.4 ($q_5 < \frac{1}{4}$).

How the claims are checked. For each f, $\Delta_i(f) = \sum_{x:x_i=1}(f(x) - f(x-e_i))\prod_{l\neq i} q^{x_l}(1-q)^{1-x_l}$ is computed as an integer polynomial, and the distinct polynomials H_f are tested (39 for $n = 3$, 1 630 for $n = 4$). Let $g_5(q) = 5q^2 - 10q + 1$ and $g_6(q) = 6q^2 - 12q + 1$, with roots q_5 and q_6 in $(0,1)$ ($5(1-q)^2 = 4$, resp. $6(1-q)^2 = 5$); both are decreasing on $[0,1]$, and g_5 is irreducible over $\mathbb{Q}$ (its discriminant 80 is not a square). Take rationals $q_6^- < q_6$ and $q_5^+ > q_5$ from rational bounds of $\sqrt{5/6}$ and $\sqrt{4/5}$, with $g_6(q_6^-) > 0$ and $g_5(q_5^+) < 0$ (and $q_6^+ < q_5^-$ for the companion bounds). For $H_f \not\equiv 0$: either $g_5 \mid H_f$, $H_f = g_5 Q$, where Q has no root in $[q_6^-, q_5^+]$ (Sturm) and $Q(q_6^-) > 0$; then $Q > 0$ on $[q_6, q_5]$, and $H_f = g_5 Q \ge 0$ there with equality only at q_5, since $g_5 > 0$ on $[0, q_5)$. Or $g_5 \nmid H_f$, and H_f has no root in $[q_6^-, q_5^+]$ and $H_f(q_6^-) > 0$, so $H_f > 0$ on $[q_6, q_5]$. Since g_5 is irreducible, $H_f(q_5) = 0$ iff $g_5 \mid H_f$. The verifier checks that no H_f vanishes identically, that no H_f with $n = 3$ is divisible by g_5, and that the functions with $n = 4$ and $g_5 \mid H_f$ are exactly the two truth tables of $\pm\mathrm{OR}_{\{1,2,3,4\}}$. As a check of (6.6): $H_{\mathrm{OR}_{\{1,2,3\}}} = 20(1-q)^8 - 12(1-q)^4 = 4(1-q)^4\big(5(1-q)^4 - 3\big) > 0$ (as $(1-q)^2 \ge \frac{4}{5}$ for $q \le q_5$), and $H_{\mathrm{OR}_{\{1,2,3,4\}}} = 20(1-q)^8 - 16(1-q)^6 = 4(1-q)^6 g_5(q)$. □

Remark 6.9. Lemmas 6.7 and 6.8 also follow from RQ-C's result C6 ($R_n(q) = 2\tau\sqrt{\max_{k\le n} k(1-q)^{2k-2}}$ for $q \le \frac{1}{2}$ and $n \le 7$, audited VALID as A.5, A.5b), since $T_k < T_5$ for $k \le 3$ and $T_4 \le T_5$ on $[q_6, q_5]$. Our check is independent of it. The four-bit lemma is false for $q > q_5$, where $(e_1 + e_2 + e_3 + e_4)/2$ gives $T_4 > T_5$, and the bound $G_6 \le T_5|c|$ of Lemma 6.6 is false for $q < q_6$, where $(e_1 + \cdots + e_6)/\sqrt{6}$ gives $T_6 > T_5$. The ends of $[q_6, q_5]$ enter the proof through the four-bit lemma ($q \le q_5$) and through $G_n \le T_n|c| \le T_5|c|$ for $n \ge 6$ in the OR region ($q \ge q_6$, Lemmas 6.6 and 6.4(ii)), both used in the near-sphere bounds of Section 6.8; the box computations cover the slightly larger range $u \in [U_-, U_+]$, and their conclusions are used only for $u \in [u_5, u_6]$.

6.4 Moments of the remainder

Lemma 6.10 (cumulants)**.** *Let $w = u^2 + v^2$ and $d = u - v$. The cumulants of χ are $\kappa_1 = 0$, $\kappa_2 = 1$ and $\kappa_j = d^{[j \text{ odd}]} G_j(w)$ for $3 \le j \le 10$, where*

$$G_3 = 1, \qquad G_4 = w - 4,$$
$$G_5 = w - 10, \qquad G_6 = w^2 - 26w + 64,$$
$$G_7 = w^2 - 56w + 244, \qquad G_8 = w^3 - 120w^2 + 1188w - 2176,$$
$$G_9 = w^3 - 246w^2 + 4044w - 11080, \qquad G_{10} = w^4 - 502w^3 + 14604w^2 - 86728w + 126976.$$

Proof. By (6.1), $m_k = \mathbb{E}\chi^k = qu^k + (1-q)(-v)^k = (u^k + (-1)^k u^{2-k})/(1+u^2)$. The cumulants are determined by the recursion $\kappa_n = m_n - \sum_{k=1}^{n-1}\binom{n-1}{k-1}\kappa_k m_{n-k}$. For example $m_3 = u - v$, $m_4 = w - 1$, so $\kappa_3 = d$ and $\kappa_4 = m_4 - 3 = w - 4$. The identities for $j \le 10$ are verified symbolically (sympy, part A1 of the verifier: the difference of the two sides simplifies to 0 as a rational function of u). □

Lemma 6.11 (moments from cumulants)**.** *Let $M = \sum \beta_i\chi_i$ (finite sum) with $\sum \beta_i^2 = 1$ and power sums $p_j = \sum_i \beta_i^j$. Then M has cumulants $K_1 = 0$, $K_2 = 1$, $K_j = \kappa_j p_j$, and $\mathbb{E}M^n = \mu_n(K_3, \ldots, K_n)$*

for $n \le 10$, where $\mu_0 = 1$ and

$$\mu_n = \sum_{k=2}^{n} \binom{n-1}{k-1} K_k \, \mu_{n-k} \qquad (K_2 = 1).$$

Each μ_n is a polynomial in $K_3, \dots, K_{10}$ with nonnegative integer coefficients; we write $\mu_n = \sum_e N_n(e) \prod_{j=3}^{10} K_j^{e_j}$ over exponent vectors $e = (e_3, \dots, e_{10})$. The term with $e = 0$ is the Gaussian moment: $N_n(0) = (n-1)!!$ for even n and 0 for odd n.

Proof. Cumulants of independent sums add and $K_j(\beta\chi) = \beta^j \kappa_j$, so $K_j(M) = \kappa_j p_j$, with $K_1 = 0$ and $K_2 = \sum \beta_i^2 = 1$. The recursion is the moment–cumulant relation $m_n = \sum_{k=1}^{n} \binom{n-1}{k-1} K_k m_{n-k}$ with $K_1 = 0$. The value at $K_3 = \cdots = K_{10} = 0$ is the n-th moment of a standard Gaussian. (Part A2 of the verifier checks the recursion against the Gaussian moments and against $\mathbb{E}\chi^n$ at $u = \frac{5}{2}$ for $n \le 10$.) □

Lemma 6.12 (power sums)**.** *Let $\sum \beta_i^2 = 1$, $\max |\beta_i| \le m \le 1$ and $\rho = \sqrt{p_4}$. Then $0 \le \rho \le m$, $|p_3| \le \rho$, $|p_j| \le m^{j-4}\rho^2$ for $5 \le j \le 10$, and $p_j \ge \rho^{j-2}$ for even $j \ge 4$.*

Proof. $p_4 \le m^2 \sum \beta_i^2 = m^2$. Cauchy–Schwarz gives $p_3^2 = (\sum \beta_i \beta_i^2)^2 \le p_2 p_4 = p_4$. For $j \ge 5$, $|p_j| \le \sum |\beta_i|^{j-4} \beta_i^4 \le m^{j-4} p_4$. For even $j \ge 4$, Jensen's inequality for the probability weights β_i^2 and the convex function $x \mapsto x^{(j-2)/2}$ gives $p_j = \sum \beta_i^2 (\beta_i^2)^{(j-2)/2} \ge (\sum \beta_i^2 \beta_i^2)^{(j-2)/2} = \rho^{j-2}$. □

Lemma 6.13 (sign information)**.** *Let $\sum \beta_i^2 = 1$, $m = \max |\beta_i|$, and suppose $\beta_{i_0} = -m$ for some i_0. If $m \ge m_c \in (0, 1]$, then $p_3 \le \varphi(m_c) := -m_c^3 + (1 - m_c^2)^{3/2}$. Moreover $\varphi(m) < 0$ iff $2m^2 > 1$.*

Proof. For $i \ne i_0$, $|\beta_i| \le (\sum_{i \ne i_0} \beta_i^2)^{1/2} = \sqrt{1 - m^2}$. Hence $p_3 = -m^3 + \sum_{i \ne i_0} \beta_i^3 \le -m^3 + \sqrt{1-m^2} \sum_{i \ne i_0} \beta_i^2 = \varphi(m)$, and $\varphi'(m) = -3m^2 - 3m\sqrt{1-m^2} \le 0$, so $\varphi(m) \le \varphi(m_c)$. Finally $\varphi(m) < 0$ iff $(1-m^2)^{3/2} < m^3$ iff $1 - m^2 < m^2$. □

Cumulant enclosures. For $1 \le u_1 \le u \le u_2$: $d = u - 1/u$ and $w = u^2 + u^{-2}$ are increasing and $d \ge 0$, so $d \in [d^-, d^+] = [u_1 - \frac{1}{u_1}, u_2 - \frac{1}{u_2}]$ and $w \in [w^-, w^+] = [u_1^2 + u_1^{-2}, u_2^2 + u_2^{-2}]$. Let $[G_j^-, G_j^+] \supseteq G_j([w^-, w^+])$ be the following enclosure: bisect $[w^-, w^+]$; on a subinterval where G_j' has no root (exact Sturm count) the range of G_j is spanned by its two end values; a subinterval that still contains a root of G_j' after a fixed number of bisections (24 in the generator, 30 in the verifier) is enclosed by interval Horner evaluation; $[G_j^-, G_j^+]$ is the hull of these pieces. (This matters: G_9' vanishes at a point with $u \approx 2.926$, inside the range.) Then $\kappa_j \in [\kappa_j^-, \kappa_j^+]$, where this is $[G_j^-, G_j^+]$ for even j and the interval product $[d^-, d^+] \cdot [G_j^-, G_j^+]$ for odd j.

Definition 6.14 (objective bound)**.** Let $D \le 10$, $c = (c_0, \dots, c_D) \in \mathbb{Q}^{D+1}$, $1 < u_1 < u_2$ rationals, $m^* \in (0, 1]$, $p^* < 0$ optional, and Θ a target. Put $L_e = \sum_n c_n N_n(e)$ and $A = L_0 = \sum_{n \text{ even}} c_n (n-1)!!$. For every $e \ne 0$ with $L_e \ne 0$ let $[C_e^-, C_e^+]$ be the interval product $L_e \prod_j [\kappa_j^-, \kappa_j^+]^{e_j}$, and put

$$u_e = e_3 + 2 \sum_{j \ge 4} e_j, \qquad U_e = \prod_{j \ge 5} (m^*)^{(j-4)e_j}.$$

Call e *even* if e_j is even for every odd j. For even e let $(\ell_e, l_e) = (0, 0)$ if $e_j > 0$ for some odd j, and $(\ell_e, l_e) = (1, \sum_{j \text{ even}} (j-2)e_j)$ otherwise. Define the term bounds

(T0) if p^* is given, $e = (1, 0, \dots, 0)$ (i.e. the monomial p_3) and $C_e^- \ge 0$: replace A by $A + C_e^- p^*$, and $b_e = 0$;

(T1) otherwise, if e is not even: $b_e(\rho) = \max(|C_e^-|, |C_e^+|)\, U_e\, \rho^{u_e}$;

(T2) if e is even and $C_e^+ \le 0$: $b_e(\rho) = C_e^+\, \ell_e\, \rho^{l_e}$;

(T3) if e is even and $C_e^+ > 0$: $b_e(\rho) = C_e^+\, U_e\, \rho^{u_e}$.

We say that c *satisfies the objective bound for* $(u_1, u_2, m^*, p^*, \Theta)$ if $h(\rho) = \Theta - A - \sum_e b_e(\rho) > 0$ for all $\rho \in [0, m^*]$.

Lemma 6.15 (expectation bound)**.** *Suppose c satisfies the objective bound for $(u_1, u_2, m^*, p^*, \Theta)$ and let $P(y) = \sum_n c_n y^n$. Then $\mathbb{E}P(M) < \Theta$ for every $u \in [u_1, u_2]$ and every $M = \sum \beta_i \chi_i$ with $\sum \beta_i^2 = 1$, $\max|\beta_i| \le m^*$ and, if p^* is given, $p_3 \le p^*$.*

Proof. By Lemma 6.11, $\mathbb{E}P(M) = \sum_n c_n \mu_n = L_0 + \sum_{e \neq 0} C_e p^e$ with $C_e = L_e \prod_j \kappa_j^{e_j} \in [C_e^-, C_e^+]$ and $p^e = \prod_j p_j^{e_j}$. Let $\rho = \sqrt{p_4} \in [0, m^*]$. By Lemma 6.12, $|p^e| \le \rho^{e_3} (\rho^2)^{e_4} \prod_{j \ge 5} (m^{*\,j-4} \rho^2)^{e_j} = U_e \rho^{u_e}$; if e is even then $p^e \ge 0$ (odd power sums appear to even powers, and $p_j \ge 0$ for even j); and if moreover $e_j = 0$ for all odd j, then $p^e \ge \prod_{j \text{ even}} \rho^{(j-2)e_j} = \rho^{l_e}$. Hence: in case (T0), $p_3 \le p^* < 0$ and $C_e \ge C_e^- \ge 0$ give $C_e p_3 \le C_e p^* \le C_e^- p^*$; in case (T1), $C_e p^e \le |C_e||p^e| \le b_e(\rho)$; in case (T2), $C_e \le C_e^+ \le 0$ and $p^e \ge \ell_e \rho^{l_e} \ge 0$ give $C_e p^e \le C_e^+ p^e \le C_e^+ \ell_e \rho^{l_e}$; in case (T3), $p^e \ge 0$ gives $C_e p^e \le C_e^+ p^e \le C_e^+ U_e \rho^{u_e}$. Summing, $\mathbb{E}P(M) \le \Theta - h(\rho) < \Theta$. □

6.5 The one-coordinate route ($a_1 \le \frac{1}{4}$)

Here we split off only $a = a_1$: $L = a\chi_1 + b_1 M_1$ with $b_1 = \sqrt{1 - a^2}$ and $M_1 = \sum_{i \ge 2} (\alpha_i / b_1) \chi_i$, whose coefficients are at most $\min(1, a/b_1)$ in absolute value. For $y \in \mathbb{R}$,

$$\mathbb{E}|a\chi + y| = 2\tau a + 2R_a(y) - (1 - 2q)y, \qquad R_a(y) = \max\{0,\ (1-q)(y - av),\ q(-y - au)\}$$

(BF3, Lemma 9.4; Lemma 3 of `MAIN_RESULT`, audited VALID). Indeed $\mathbb{E}|a\chi + y| = q|au + y| + (1-q)|y - av|$ equals $2\tau a - (1-2q)y$ for $-au \le y \le av$ (using $qau = (1-q)av = \tau a$), y for $y > av$, and $-y$ for $y < -au$, and so does the right-hand side. Conditioning on M_1 and using $\mathbb{E}M_1 = 0$,

$$\mathbb{E}|L| = 2\tau a + 2\mathbb{E}R_a(b_1 M_1), \qquad \text{so} \qquad \mathbb{E}|L| < T_5 \iff \mathbb{E}R_a(b_1 M_1) < \tau\big(\sqrt{5}(1-q)^4 - a\big).$$

A *cell* is $[u_1, u_2] \times [\underline{a}, \overline{a}]$ with rationals $1 < u_1 < u_2$ and $0 \le \underline{a} < \overline{a} \le A_S$. Let $\bar{b}$ be a rational upper bound of $\sqrt{1 - \underline{a}^2}$, $\bar{m} = \min\{1, \overline{a}/\beta\}$ with β a rational lower bound of $\sqrt{1 - \overline{a}^2}$, and

$$\bar{\ell}_1(y) = \frac{u_2^2}{1 + u_2^2}\Big(\bar{b}y - \frac{\underline{a}}{u_2}\Big), \quad \bar{\ell}_2(y) = \frac{1}{1 + u_1^2}\big(-\bar{b}y - \underline{a}u_1\big), \quad \Theta_1 = \tau(u_2)\Big(\sqrt{5}^{\,-}\Big(\frac{u_1^2}{1 + u_1^2}\Big)^4 - \overline{a}\Big).$$

A *cell certificate* is $c \in \mathbb{Q}^{D+1}$, $D \le 10$, with $P(y) = \sum c_n y^n$ such that (V1) $P > 0$, (V2) $P > \bar{\ell}_1$, (V3) $P > \bar{\ell}_2$ on $\mathbb{R}$, and (V4) c satisfies the objective bound for $(u_1, u_2, \bar{m}, -, \Theta_1)$.

Lemma 6.16. *If a cell with $u_1 \ge U_-$ has a certificate, then $\mathbb{E}|L| < T_5$ for every $u \in [u_1, u_2]$ and every unit α with $\underline{a} \le \max_i |\alpha_i| \le \overline{a}$.*

Proof. For $u \in [u_1, u_2]$, $a \in [\underline{a}, \overline{a}]$ and $b_1 = \sqrt{1 - a^2}$ we have $R_a(b_1 y) = \max\{0, \ell_1, \ell_2\}$ with $\ell_1 = \frac{u^2}{1+u^2}(b_1 y - \frac{a}{u})$ and $\ell_2 = \frac{1}{1+u^2}(-b_1 y - au)$. If $\ell_1(y) > 0$ then $y > 0$ and $0 < b_1 y - \frac{a}{u} \le \bar{b}y - \frac{\underline{a}}{u_2}$, and $\frac{u^2}{1+u^2} \le \frac{u_2^2}{1+u_2^2}$, so $\ell_1(y) \le \bar{\ell}_1(y)$. If $\ell_2(y) > 0$ then $y < 0$ and $0 < -b_1 y - au \le -\bar{b}y - \underline{a}u_1$, and $\frac{1}{1+u^2} \le \frac{1}{1+u_1^2}$, so $\ell_2(y) \le \bar{\ell}_2(y)$. So by (V1)–(V3), $R_a(b_1 y) < P(y)$ for all y, and $\mathbb{E}R_a(b_1 M_1) \le$

$\mathbb{E}P(M_1)$. Since $a/\sqrt{1-a^2}$ is increasing, the coefficients of M_1 are at most $\bar{m}$ in absolute value. By Lemma 6.15, $\mathbb{E}P(M_1) < \Theta_1$. Finally $\Theta_1 \le \tau(u)(\sqrt{5}(1-q)^4 - a)$, because $\tau(u) \ge \tau(u_2)$, $(1-q)^4 \ge (\frac{u_1^2}{1+u_1^2})^4$, $\sqrt{5}^- \le \sqrt{5}$, $a \le \bar{a}$, and the bracket is positive: $w_-^4 \ge 5^{-1/2} > \frac{2}{5}$ by (6.3) and $\sqrt{5}^- \ge 2$, so $\sqrt{5}^-(\frac{u_1^2}{1+u_1^2})^4 \ge \sqrt{5}^- w_-^4 > \frac{4}{5} > \frac{1}{4} \ge \bar{a}$ (the verifier also asserts $\Theta_1 > 0$ for every cell). □

6.6 The two-coordinate route: vertex certificates

6.6.1 The functions F_x, nested patches and peeling

Let $k \ge 2$ and a sign vector $\sigma \in \{1,-1\}^k$ with $\sigma_1 = 1$. For $x \in \mathbb{R}^{k+1}$ and $y \in \mathbb{R}$ put

$$F_x(y) = \mathbb{E}\Big|\sum_{i=1}^{k} \sigma_i x_i \chi_i + x_{k+1}\, y\Big|,$$

where $\chi_1, \dots, \chi_k$ are i.i.d. normalised q-biased bits. We use $\sigma = (1, s, \varsigma_1, \dots, \varsigma_{k-2})$, where ς_i are the signs of peeled coefficients (Lemma 6.18); the data use $k \le 5$.

Lemma 6.17. *For fixed q and y, the map $x \mapsto F_x(y)$ is convex and positively homogeneous of degree one. Consequently, if $x = \sum_l \nu_l V_l$ with $\nu_l \ge 0$, then $F_x(y) \le \sum_l \nu_l F_{V_l}(y)$.*

Proof. $F_x(y)$ is the expectation of the absolute value of a linear function of x, i.e. a seminorm of x. A seminorm N satisfies $N(\sum \nu_l V_l) \le \sum \nu_l N(V_l)$ for $\nu_l \ge 0$. □

The *patches* are the maps, for $j \ge 0$ and $k = 2 + j$,

$$p_k(t, r, \mu_1, \dots, \mu_j) = \big(rc(t),\, rd(t),\, b_0\mu_1,\, \dots,\, b_{j-1}\mu_j,\, b_j\big), \qquad b_0 = \sqrt{1-r^2}, \quad b_i = b_{i-1}\sqrt{1-\mu_i^2},$$

for $t \in [0,1]$ and $r, \mu_1, \dots, \mu_j \in [0,1]$. Thus

$$p_2(t,r) = (rc, rd, b_0), \quad p_3(t,r,\mu_1) = (rc, rd, b_0\mu_1, b_1), \quad p_4(t,r,\mu_1,\mu_2) = (rc, rd, b_0\mu_1, b_1\mu_2, b_2),$$

and so on. Their values are unit vectors with nonnegative entries: $b_{i-1}^2\mu_i^2 + b_i^2 = b_{i-1}^2$, so $|p_k|^2 = r^2c^2 + r^2d^2 + b_0^2 = 1$.

Peeling. Let $N = \sum_{i \in I} \gamma_i \chi_i$ be a finite sum with $\sum \gamma_i^2 = 1$, and $\mu(N) = \max_i |\gamma_i|$. If $\mu = \mu(N) < 1$ and $\gamma_{i^*} = \varsigma\mu$ with $\varsigma \in \{1,-1\}$, the *peeled remainder* is $N^\flat = \sum_{i \in I \setminus \{i^*\}} (\gamma_i/\sqrt{1-\mu^2})\chi_i$. Then

$$N = \varsigma\mu\chi_{i^*} + \sqrt{1-\mu^2}\, N^\flat, \qquad \sum_{i \ne i^*} \frac{\gamma_i^2}{1-\mu^2} = 1, \qquad \mu(N^\flat) \le \min\Big(1, \frac{\mu}{\sqrt{1-\mu^2}}\Big), \tag{6.7}$$

and $N^\flat$ is independent of χ_{i^*}: indeed $\sum_{i \ne i^*} \gamma_i^2 = 1 - \mu^2$, and each $|\gamma_i|$ is at most μ and at most $\sqrt{1-\mu^2}$. If $\mu(N) = 1$, then $N = \varsigma\chi_{i^*}$ (all other coefficients vanish).

Lemma 6.18 (conditional expectation)**.** *Consider a point with $r < 1$ and remainder M, and let $j \ge 0$. Put $M^{(0)} = M$ and, for $i = 1, \dots, j$, let $\mu_i = \mu(M^{(i-1)})$, attained by the coefficient $\varsigma_i\mu_i$ of χ_{l_i}, and $M^{(i)} = (M^{(i-1)})^\flat$ if $\mu_i < 1$.*

(i) If $\mu_1,\dots,\mu_j<1$, then $\mathbb{E}|L|=\mathbb{E}F_{p_{2+j}(t,r,\mu_1,\dots,\mu_j)}(M^{(j)})$ with $\sigma=(1,s,\varsigma_1,\dots,\varsigma_j)$, the bits being $\chi_1,\chi_2,\chi_{l_1},\dots,\chi_{l_j}$; here $M^{(j)}$ is independent of these bits, $\sum$(coefficients of $M^{(j)})^2=1$, and $\mu(M^{(j)})\le\min(1,\mu_j/\sqrt{1-\mu_j^2})$ if $j\ge1$.

(ii) If $j\ge1$, $\mu_1,\dots,\mu_{j-1}<1$ and $\mu_j=1$, then $L=a_1\chi_1+sa_2\chi_2+\sum_{i<j}\varsigma_i b_{i-1}\mu_i\chi_{l_i}+\varsigma_j b_{j-1}\chi_{l_j}$, and $F_{p_{2+j}(t,r,\mu_1,\dots,\mu_j)}(y)=\mathbb{E}|L|$ for every $y\in\mathbb{R}$ (with the same σ).

Proof. $L=a_1\chi_1+sa_2\chi_2+b_0M^{(0)}$ with $(a_1,a_2)=(rc(t),rd(t))$, and by (6.7), if $\mu_i<1$, $b_{i-1}M^{(i-1)}=\varsigma_i b_{i-1}\mu_i\chi_{l_i}+b_iM^{(i)}$. By induction $L=a_1\chi_1+sa_2\chi_2+\sum_{i\le j}\varsigma_i b_{i-1}\mu_i\chi_{l_i}+b_jM^{(j)}$, where the bits are distinct and independent of $M^{(j)}$; conditioning on $M^{(j)}$ gives (i), and the bound on $\mu(M^{(j)})$ is (6.7). In (ii), $M^{(j-1)}=\varsigma_j\chi_{l_j}$, which gives the formula for L; the last entry of p_{2+j} is $b_j=b_{j-1}\sqrt{1-1}=0$, so $F_{p_{2+j}}(y)$ does not depend on y and equals $\mathbb{E}|L|$. □

6.6.2 Vertex sets and the cone lemma

Definition 6.19 (vertex set)**.** Let $X=\prod_{i=1}^{k}[\xi_i^-,\xi_i^+]$ be a box of patch parameters $(t,r,\mu_1,\dots,\mu_j)$, $k=2+j$, and $p=p_k$. A *vertex set for X* is a vector $n_0\in\mathbb{Q}^{k+1}$ and 2^k vectors $V_\epsilon\in\mathbb{Q}^{k+1}$, indexed by $\epsilon\in\{0,1\}^k$, such that:

(P1) $|n_0|^2\ge1$ and $V_\epsilon\cdot n_0=|n_0|^2$ for all ϵ;

(P2) (parallelepiped) $V_\epsilon=V_0+\sum_i\epsilon_iE_i$ with $E_i=V_{e_i}-V_0$;

(P3) (facets) for each i and $\delta\in\{0,1\}$ the 2^{k-1} vertices with $\epsilon_i=\delta$ span a linear subspace of dimension k; let $h_{i,\delta}$ be a normal vector of it, oriented so that $h_{i,\delta}\cdot\bar c>0$ for the centre $\bar c=V_0+\frac12\sum_iE_i$ (and $h_{i,\delta}\cdot\bar c\ne0$ is required);

(P4) (enclosure) $h_{i,\delta}\cdot p(\xi)\ge0$ for all i,δ and all $\xi\in X$.

Lemma 6.20 (cone lemma)**.** *Let $(n_0,(V_\epsilon))$ be a vertex set for X. Then for every $\xi\in X$ there are $\nu_\epsilon\ge0$ with $p(\xi)=\sum_\epsilon\nu_\epsilon V_\epsilon$ and $\sum_\epsilon\nu_\epsilon\le1/|n_0|\le1$.*

Proof. First, $V_0,E_1,\dots,E_k$ is a basis of $\mathbb{R}^{k+1}$. Indeed $E_i\cdot n_0=0$ by (P1) and $V_0\cdot n_0=|n_0|^2\ne0$, so $V_0\notin\operatorname{span}\{E_i\}$. By (P2) the face $\{\epsilon_i=0\}$ spans $S_i=\operatorname{span}(V_0,\{E_j\}_{j\ne i})$, which has dimension k by (P3); hence the k vectors $V_0,\{E_j\}_{j\ne i}$ are linearly independent. Moreover $\bar c-V_0-\frac12\sum_{j\ne i}E_j=\frac12E_i$ and $h_{i,0}\cdot\bar c\ne0$ with $h_{i,0}\perp S_i$, so $E_i\notin S_i$. Thus the $k+1$ vectors are independent.

Let $z\in\mathbb{R}^{k+1}$ with $h_{i,\delta}\cdot z\ge0$ for all i,δ, and write $z=\lambda V_0+\sum_i\mu_iE_i$. Since $h_{i,0}\perp S_i$, $h_{i,0}\cdot z=\mu_i\,h_{i,0}\cdot E_i$, and $h_{i,0}\cdot\bar c=\frac12h_{i,0}\cdot E_i>0$; so $\mu_i\ge0$. The face $\{\epsilon_i=1\}$ spans $\operatorname{span}(V_0+E_i,\{E_j\}_{j\ne i})$, so $h_{i,1}\cdot E_j=0$ $(j\ne i)$ and $h_{i,1}\cdot V_0=-h_{i,1}\cdot E_i$; then $h_{i,1}\cdot\bar c=-\frac12h_{i,1}\cdot E_i>0$, so $h_{i,1}\cdot V_0>0$, and $h_{i,1}\cdot z=(\lambda-\mu_i)\,h_{i,1}\cdot V_0$; so $\mu_i\le\lambda$. If $\lambda=0$ then $z=0$. Otherwise $z/\lambda=V_0+\sum_i\theta_iE_i$ with $\theta_i=\mu_i/\lambda\in[0,1]$, which is a point of the parallelepiped $\operatorname{conv}\{V_\epsilon\}$, i.e. a convex combination $\sum\omega_\epsilon V_\epsilon$ (take $\omega_\epsilon=\prod_i\theta_i^{\epsilon_i}(1-\theta_i)^{1-\epsilon_i}$). So $z=\sum\nu_\epsilon V_\epsilon$ with $\nu=\lambda\omega\ge0$ and $\sum\nu_\epsilon=\lambda$. Finally $z\cdot n_0=\lambda|n_0|^2$, so $\lambda=z\cdot n_0/|n_0|^2\le|z|/|n_0|$.

By (P4), $z=p(\xi)$ satisfies the hypothesis, and $|p(\xi)|=1$. □

Condition (P4) is checked without subdivision: the minimum of a linear functional over a parameter box of a patch is the end of a short chain of one-variable minimisations.

Lemma 6.21 (facet minima)**.** *For $\alpha,\beta\in\mathbb{R}$ and $-1\le x^-<x^+\le1$ let $g(x)=\alpha x+\beta\sqrt{1-x^2}$ and $\mathfrak{m}(\alpha,\beta;x^-,x^+)=\min_{x\in[x^-,x^+]}g(x)$.*

(i) If $\beta \geq 0$, then $\mathfrak{m}(\alpha, \beta; x^-, x^+) = \min(g(x^-), g(x^+))$.

(ii) If $\beta < 0$, put $R = \sqrt{\alpha^2 + \beta^2}$ and $x^* = -\alpha/R$. Then $\mathfrak{m}(\alpha, \beta; x^-, x^+) = -R$ if $x^- \leq x^* \leq x^+$, and $\mathfrak{m}(\alpha, \beta; x^-, x^+) = \min(g(x^-), g(x^+))$ otherwise.

(iii) $\mathfrak{m}(\alpha, \beta; x^-, x^+)$ is nondecreasing in β, and also in α if $x^- \geq 0$.

Let $k = 2 + j$ with $j \geq 0$, let $X = [t^-, t^+] \times [r^-, r^+] \times \prod_{i=1}^{j} [\mu_i^-, \mu_i^+]$ with $0 \leq t^- < t^+ \leq 1$, $0 \leq r^- < r^+ \leq 1$ and $0 \leq \mu_i^- < \mu_i^+ \leq 1$, and let $h \in \mathbb{R}^{k+1}$. Put $W_j = h_{k+1}$, $W_{i-1} = \mathfrak{m}(h_{i+2}, W_i; \mu_i^-, \mu_i^+)$ for $i = j, j-1, \ldots, 1$, $A = \mathfrak{m}(h_1, h_2; c(t^+), c(t^-))$ and $G = \mathfrak{m}(A, W_0; r^-, r^+)$. Then

$$\min_{\xi \in X} h \cdot p_k(\xi) = G.$$

If in this recursion each value of $\mathfrak{m}$ is replaced by a lower bound of it (and the later steps are applied to these lower bounds), the result is a lower bound of G.

Proof. (i) The function $x \mapsto \sqrt{1 - x^2}$ is concave on $[-1, 1]$, so for $\beta \geq 0$ the function g is concave, and the minimum of a concave function over an interval is attained at an endpoint.

(ii) For $\beta < 0$ the function g is convex. By the Cauchy–Schwarz inequality, $g(x) \geq -R\,|(x, \sqrt{1-x^2})| = -R$ for all $x \in [-1, 1]$. Moreover $R > 0$, $|x^*| \leq 1$ and $\sqrt{1 - x^{*2}} = |\beta|/R = -\beta/R$, so $g(x^*) = -\alpha^2/R - \beta^2/R = -R$. Thus x^* is a minimum point of g on $[-1, 1]$. If $x^* \in [x^-, x^+]$, the minimum over $[x^-, x^+]$ is $-R$. Otherwise $[x^-, x^+]$ lies in $[-1, x^*]$ or in $[x^*, 1]$, where the convex function g is nonincreasing, respectively nondecreasing, so the minimum is attained at an endpoint.

(iii) For every $x \in [-1, 1]$, $g(x)$ is nondecreasing in β because $\sqrt{1 - x^2} \geq 0$, and nondecreasing in α if $x \geq 0$. Minima over x of pointwise nondecreasing families are nondecreasing.

Now the patch. Put $w_j = h_{k+1}$ and $w_{i-1}(\mu_i, \ldots, \mu_j) = h_{i+2}\mu_i + \sqrt{1 - \mu_i^2}\; w_i(\mu_{i+1}, \ldots, \mu_j)$ for $i = j, \ldots, 1$. Since $b_i = b_{i-1}\sqrt{1 - \mu_i^2}$, we have $b_{i-1} w_{i-1} = h_{i+2}\, b_{i-1}\mu_i + b_i w_i$, and therefore

$$h \cdot p_k(t, r, \mu_1, \ldots, \mu_j) = r\,\big(h_1 c(t) + h_2 d(t)\big) + b_0\, w_0(\mu_1, \ldots, \mu_j), \qquad b_0 = \sqrt{1 - r^2}.$$

First, $\min w_{i-1} = W_{i-1}$, the minimum being over $\mu_l \in [\mu_l^-, \mu_l^+]$ for $l \geq i$. This holds for $i - 1 = j$, since $w_j = h_{k+1} = W_j$. If it holds for i, then for fixed μ_i the minimum of w_{i-1} over $\mu_{i+1}, \ldots, \mu_j$ is $h_{i+2}\mu_i + \sqrt{1 - \mu_i^2}\, W_i$, because the weight $\sqrt{1 - \mu_i^2}$ is nonnegative and w_i does not depend on μ_i. Minimising over $\mu_i \in [\mu_i^-, \mu_i^+]$ gives $\mathfrak{m}(h_{i+2}, W_i; \mu_i^-, \mu_i^+) = W_{i-1}$.

Second, c is a decreasing bijection of $[t^-, t^+]$ onto $[c(t^+), c(t^-)]$, and $d(t) = \sqrt{1 - c(t)^2}$ for $t \in [0, 1]$ (because $c^2 + d^2 = 1$ and $d \geq 0$). Hence $\min_{t \in [t^-, t^+]} (h_1 c(t) + h_2 d(t)) = \mathfrak{m}(h_1, h_2; c(t^+), c(t^-)) = A$.

Third, for fixed r the two brackets depend on disjoint sets of parameters and have the nonnegative weights r and b_0, so the minimum over t and μ is $rA + \sqrt{1 - r^2}\, W_0$. Minimising over $r \in [r^-, r^+]$ gives G.

The last statement follows from (iii) by induction along the recursion: in the steps for W_{i-1} the replaced value enters as β, and in the step for G the values A and W_0 enter as α and β, with $x = r \geq r^- \geq 0$. □

Checking (P4). (P4) holds if and only if $G(h_{i,\delta}) \geq 0$ for all $2k$ facet normals. A rational lower bound of G is computed by the recursion of Lemma 6.21 in exact rational arithmetic: an endpoint value $g(x^\pm)$ is bounded below using a rational lower bound of $\sqrt{1 - (x^\pm)^2}$ if $\beta \geq 0$ and a rational

upper bound if $\beta < 0$; the value $-R$ is bounded below by $-R^+$ with $R^+ \geq R$ rational; and the condition $x^- \leq x^* \leq x^+$ is decided exactly. For rationals p, q the sign of $p - qR$ is: ≥ 0 if $p \geq 0 \geq q$; < 0 if $p \leq 0 \leq q$ and $(p,q) \neq (0,0)$; the sign of $p^2 - q^2R^2$ if $p, q > 0$; and the sign of $q^2R^2 - p^2$ if $p, q < 0$. Then $x^- \leq x^*$ if and only if $p - qR \geq 0$ for $(p,q) = (-\alpha, x^-)$, and $x^* \leq x^+$ if and only if $p - qR \leq 0$ for $(p,q) = (-\alpha, x^+)$. (P4) is accepted if the lower bound is ≥ 0 for every facet normal.

6.6.3 Vertex envelopes and vertex certificates

Fix a u-interval $[u_1, u_2]$ with $u_1 > 1$. For a vertex $V \in \mathbb{Q}^{k+1}$ let $\gamma = (\sigma_1 V_1, \ldots, \sigma_k V_k)$ and $b_V = V_{k+1}$. The atoms of $\sum_i \gamma_i \chi_i$ are indexed by $\omega \in \{u, -v\}^k$, with probability $\pi_\omega = \prod_i q^{[\omega_i = u]}(1-q)^{[\omega_i = -v]}$ and value $y_\omega = \sum_i \gamma_i \omega_i$, and by (6.1)

$$\pi_\omega y_\omega = \tau \sum_i \gamma_i \, (\pm 1)_i \prod_{l \neq i} q^{[\omega_l = u]}(1-q)^{[\omega_l = -v]}, \qquad (\pm 1)_i = +1 \text{ if } \omega_i = u, \ -1 \text{ otherwise.}$$

Using $q \in [\frac{1}{1+u_2^2}, \frac{1}{1+u_1^2}]$, $1 - q \in [\frac{u_1^2}{1+u_1^2}, \frac{u_2^2}{1+u_2^2}]$ and $\tau \in [\tau(u_2), \tau(u_1)]$, interval arithmetic gives rational enclosures $\pi_\omega y_\omega \in [\eta_\omega^-, \eta_\omega^+]$ and $\pi_\omega \in [\pi_\omega^-, \pi_\omega^+]$, valid for all $u \in [u_1, u_2]$. Put $[\beta_\omega^-, \beta_\omega^+] = [\min(\pi_\omega^- b_V, \pi_\omega^+ b_V), \max(\pi_\omega^- b_V, \pi_\omega^+ b_V)]$.

Definition 6.22 (vertex envelope)**.** $\Phi_V(y) = \sum_\omega \max(\eta_\omega^+ + \beta_\omega^+ y, \ -\eta_\omega^- - \beta_\omega^- y)$ for $y \geq 0$, and $\Phi_V(y) = \sum_\omega \max(\eta_\omega^+ + \beta_\omega^- y, \ -\eta_\omega^- - \beta_\omega^+ y)$ for $y < 0$.

Lemma 6.23 (envelope)**.** *$F_V(y) \leq \Phi_V(y)$ for all $y \in \mathbb{R}$ and all $u \in [u_1, u_2]$. On each closed half-line, Φ_V is continuous and piecewise linear, with breakpoints among the points where the two lines of one summand cross.*

Proof. $F_V(y) = \sum_\omega \pi_\omega |y_\omega + b_V y| = \sum_\omega |\pi_\omega y_\omega + \pi_\omega b_V \, y|$ and $|z| = \max(z, -z)$. For $y \geq 0$: $\pi_\omega y_\omega + \pi_\omega b_V y \leq \eta_\omega^+ + \beta_\omega^+ y$ and $-\pi_\omega y_\omega - \pi_\omega b_V y \leq -\eta_\omega^- - \beta_\omega^- y$, since $\pi_\omega b_V \in [\beta_\omega^-, \beta_\omega^+]$ (whatever the sign of b_V). For $y < 0$ the roles of $\beta^\pm$ are exchanged. □

Definition 6.24 (vertex certificate)**.** Let X be a parameter box, σ a sign vector, $[u_1, u_2]$ a u-interval, $m^* \in (0, 1]$ a cap, and $p^* < 0$ optional. A *vertex certificate for* $(X, \sigma, [u_1, u_2], m^*, p^*)$ is a vertex set $(n_0, (V_\epsilon))$ for X and coefficient vectors $c^{(\epsilon)} \in \mathbb{Q}^{D+1}$, $D \leq 10$, with $P_\epsilon(y) = \sum_n c_n^{(\epsilon)} y^n$, such that for every ϵ: (W1) $P_\epsilon(y) > \Phi_{V_\epsilon}(y)$ for all $y \in \mathbb{R}$; and (W2) $c^{(\epsilon)}$ satisfies the objective bound for $(u_1, u_2, m^*, p^*, T^-(u_1, u_2))$.

(W1) is checked as follows: on each half-line, Φ_V coincides on each interval between consecutive breakpoints with one line $\lambda_0 + \lambda_1 y$ (one choice of line per summand); for every such line, $P_\epsilon - \lambda_0 - \lambda_1 y$ is shown to be positive on all of $\mathbb{R}$ by Sturm sequences.

Lemma 6.25 (vertex certificate lemma)**.** *Let a vertex certificate for $(X, \sigma, [u_1, u_2], m^*, p^*)$ be given. Let $\mathcal{Z}$ be the class of random variables $Z = \sum \beta_i \chi_i'$ (finite sums of i.i.d. copies of χ, independent of $\chi_1, \ldots, \chi_k$) with $\sum \beta_i^2 = 1$, $\max |\beta_i| \leq m^*$ and, if p^* is given, $p_3 \leq p^*$. Then for every $u \in [u_1, u_2]$, every $\xi \in X$ and every $Z \in \mathcal{Z}$,*

$$\mathbb{E} F_{p(\xi)}(Z) < T^-(u_1, u_2) \leq T_5(u).$$

Proof. By Lemma 6.20, $p(\xi) = \sum \nu_\epsilon V_\epsilon$ with $\nu \geq 0$ and $\sum \nu_\epsilon \leq 1$. By Lemmas 6.17 and 6.23 and (W1), for every y, $F_{p(\xi)}(y) \leq \sum_\epsilon \nu_\epsilon F_{V_\epsilon}(y) \leq \sum_\epsilon \nu_\epsilon P_\epsilon(y)$. Taking expectations over Z, $\mathbb{E} F_{p(\xi)}(Z) \leq \sum_\epsilon \nu_\epsilon \mathbb{E} P_\epsilon(Z)$. By (W1) and Lemma 6.23, $\mathbb{E} P_\epsilon(Z) > \mathbb{E} F_{V_\epsilon}(Z) \geq 0$, and by (W2) and Lemma 6.15, $\mathbb{E} P_\epsilon(Z) < T^-$. Since $\sum \nu_\epsilon \leq 1$ and $\max_\epsilon \mathbb{E} P_\epsilon(Z) \geq 0$, $\sum_\epsilon \nu_\epsilon \mathbb{E} P_\epsilon(Z) \leq \max_\epsilon \mathbb{E} P_\epsilon(Z) < T^-$. Finally $T^- \leq T_5(u)$ by (6.2). □

Two members of $\mathcal{Z}$ are used repeatedly: $Z = N^{-1/2}(\chi'_1 + \cdots + \chi'_N)$ with $N^{-1/2} \le m^*$ (no p^*), and, if $m^* = 1$, $Z = \chi'_1$ (no p^*).

6.6.4 Boxes

A *box* is $B = [u_1, u_2] \times [t_1, t_2] \times [r_1, r_2]$ with rationals $1 < u_1 < u_2$, $0 \le t_1 < t_2 \le 1$, $0 \le r_1 < r_2 \le 1$, together with a sign s. Let b^- be a rational lower bound of $\sqrt{1 - r_2^2}$ ($b^- = 0$ if $r_2 = 1$), and define $\bar{m}(B) = 1$ if $b^- = 0$ or $r_2 d(t_2) \ge b^-$, and $\bar{m}(B) = r_2 d(t_2)/b^-$ otherwise. Then $\bar{m}(B) \in (0, 1]$ and $m \le \min(1, a_2/b) \le \bar{m}(B)$ at every point of B with $r < 1$, because $a_2 = rd(t) \le r_2 d(t_2)$ and $b \ge b^-$. A box of kind lpv carries a vertex certificate for $([t_1, t_2] \times [r_1, r_2], (1, s), [u_1, u_2], \bar{m}(B), -)$. A box of kind small satisfies $r_2 c(t_1) \le A_S$, so $a_1 = rc(t) \le A_S$ on it.

Lemma 6.26. *At every point of an lpv box with $r < 1$, $\mathbb{E}|L| < T_5$.*

Proof. By Lemma 6.18 ($j = 0$), $\mathbb{E}|L| = \mathbb{E}F_{p_2(t,r)}(M)$, and $M \in \mathcal{Z}$ since $m \le \bar{m}(B)$. Apply Lemma 6.25. □

6.7 Near $(e_1 + e_2)/\sqrt{2}$: the near-circle lemma

Lemma 6.27 (tail bound)**.** *Let $y \in \mathbb{R}$, $b \ge 0$ and let Z be a random variable with $\mathbb{E}Z = 0$ and $\mathbb{E}Z^4 < \infty$. Then*

$$\mathbb{E}|y + bZ| \le |y| + \min\Big(b\,\mathbb{E}|Z|,\ \frac{27}{128}\,\frac{b^4 \mathbb{E}Z^4}{|y|^3}\Big),$$

where for $y = 0$ the minimum is read as its first entry. The same convention is used below whenever this bound is applied at a point where $y = 0$.

Proof. The first bound is the triangle inequality. For the second ($y \ne 0$), $|y + z| - |y| - \operatorname{sgn}(y) z = 2(-\operatorname{sgn}(y) z - |y|)_+ \le 2(|z| - |y|)_+$, and $\mathbb{E}[\operatorname{sgn}(y) bZ] = 0$. For $x \ge 0$ and $\eta > 0$, $(x - \eta)_+ \le \frac{27}{256} x^4/\eta^3$: the maximum of $(x - \eta)/x^4$ over $x > \eta$ is at $x = \frac{4}{3}\eta$ and equals $\frac{27}{256}\eta^{-3}$. Hence $\mathbb{E}|y + bZ| - |y| \le 2 \cdot \frac{27}{256}\, b^4 \mathbb{E}Z^4/|y|^3$. □

Lemma 6.28 (near-circle tests)**.** *Let B be a box with $r_1 > 0$ and $u_1 \ge U_-$. Let y_j ($j = 1, \dots, 4$) be the atoms of $c\chi_1 + sd\chi_2$, so that the atoms of $a_1\chi_1 + sa_2\chi_2$ are ry_j. Let $\eta_j \ge 0$ be a lower bound of $|y_j|$ on B, p_j^+ an upper bound of p_j, b^+ an upper bound of $\sqrt{1 - r_1^2}$, and $E_4 = 3 + \max(0, w^+ - 4)\,\bar{m}(B)^2$. Let $T^- = T^-(u_1, u_2)$.*

(A) If all $\eta_j > 0$ and $\frac{27}{128} E_4 (b^+)^2 \frac{1 + r_2}{r_1^3} \sum_j p_j^+ \eta_j^{-3} < T^-$, then $\mathbb{E}|L| < T_5$ at every point of B with $r < 1$.

(B) Let G^+ be an upper bound of $\mathbb{E}|c\chi_1 + sd\chi_2| = \tau \sum_j |g_j|$ on B with $G^+ \le T^-$, and $e_j^+ = \min\big(b^+, \frac{27}{128}(b^+)^4 E_4/(r_1^3 \eta_j^3)\big)$ ($e_j^+ = b^+$ if $\eta_j = 0$). If $\sum_j p_j^+ e_j^+ < T^-(1 - r_2) + r_1(T^- - G^+)$, then $\mathbb{E}|L| < T_5$ at every point of B with $r < 1$.

Proof. At a point of B with $r < 1$, condition on (χ_1, χ_2) and apply Lemma 6.27 with $Z = M$. Here $\mathbb{E}M^4 = 3 + \kappa_4 p_4 \le E_4$ by Lemma 6.11, since $p_4 \le m^2 \le \bar{m}(B)^2$ and $\kappa_4 = w - 4 \le w^+ - 4$; also $\mathbb{E}|M| \le 1$. This gives $\mathbb{E}|L| \le rG + \sum_j p_j e_j$, where $G = \mathbb{E}|c\chi_1 + sd\chi_2|$ and $e_j = \min(b, \frac{27}{128} b^4 E_4/(r^3 |y_j|^3))$. (A) By Lemma 6.5 ($u \ge U_-$, $c^2 + d^2 = 1$), $G < T_5$. Since $1 - r = b^2/(1 + r)$ and $b > 0$, $\sum_j p_j e_j \le \frac{27}{128} \frac{b^4 E_4}{r^3} \sum_j \frac{p_j}{|y_j|^3} \le b^2 \cdot \frac{27}{128} E_4 (b^+)^2 \frac{1}{r_1^3} \sum_j \frac{p_j^+}{\eta_j^3} < \frac{b^2 T^-}{1 + r_2} \le T_5(1 - r)$. So $\mathbb{E}|L| < rT_5 + T_5(1 - r) = T_5$. (B) $\mathbb{E}|L| \le rG^+ + \sum_j p_j^+ e_j^+ < rG^+ + T^-(1 - r_2) + r_1(T^- - G^+) \le rG^+ + T^-(1 - r) + r(T^- - G^+) = T^- \le T_5$, using $r_1 \le r \le r_2$ and $T^- - G^+ \ge 0$. □

Boxes of kind ncA pass test (A) or test (B); boxes of kind ncB pass test (B).

6.8 Near the extremisers: the m-split

In our coordinates the extremisers are the following points (all with $s = 1$ and $t = \sqrt{2} - 1$, since $a_1 = a_2$; $\mu_1, \mu_2, \dots$ are the successive maxima of Lemma 6.18):

- $(e_1 + \cdots + e_5)/\sqrt{5}$, for every $q \in [q_6, q_5]$: $a_1 = a_2 = \frac{1}{\sqrt{5}}$, $b = \sqrt{3/5}$, $M = (\chi_3 + \chi_4 + \chi_5)/\sqrt{3}$, $\mu_1 = \frac{1}{\sqrt{3}}$, $\mu_2 = \frac{1}{\sqrt{2}}$, $\mu_3 = 1$;
- $(e_1 + e_2 + e_3 + e_4)/2$, at q_5: $a_1 = a_2 = \frac{1}{2}$, $b = \frac{1}{\sqrt{2}}$, $M = (\chi_3 + \chi_4)/\sqrt{2}$, $\mu_1 = \frac{1}{\sqrt{2}}$, $\mu_2 = 1$;
- $(e_1 + \cdots + e_6)/\sqrt{6}$, at q_6: $a_1 = a_2 = \frac{1}{\sqrt{6}}$, $b = \sqrt{2/3}$, $M = (\chi_3 + \cdots + \chi_6)/2$, $\mu_1 = \frac{1}{2}$, $\mu_2 = \frac{1}{\sqrt{3}}$, $\mu_3 = \frac{1}{\sqrt{2}}$, $\mu_4 = 1$.

Equality holds at these points, so no certificate with a strict bound can contain them. We split according to $m = \mu_1$ and the sign of a largest coefficient of M; inside some pieces we peel off that coefficient and split the next remainder in the same way. This gives a finite tree of *split nodes* (Definition 6.30). The points above are reached at the leaves, where the remainder is used up ($b_j = 0$) and the near-sphere bound (Lemma 6.29) is exact.

Positive peeling. At a point with $r < 1$ we use the peeling of Lemma 6.18, with $M^{(0)} = M$ and $\mu_i = \mu(M^{(i-1)})$, and we put

$$a_{i+2} = b_{i-1}\mu_i, \qquad b_i = b_{i-1}\sqrt{1 - \mu_i^2} \qquad (b_0 = b),$$

so that $(a_1, a_2, a_3, \dots, a_{j+2}, b_j) = p_{2+j}(t, r, \mu_1, \dots, \mu_j)$. Let $j \geq 1$ and let $I_1, \dots, I_j \subset (0, 1]$ be intervals. The point is *positively peeled through* $I_1, \dots, I_j$ if $\mu_1, \dots, \mu_{j-1} < 1$ and, for $i = 1, \dots, j$, $\mu_i \in I_i$ and $M^{(i-1)}$ has the coefficient $+\mu_i$ at some χ_{l_i}, which is the coefficient peeled off ($\varsigma_i = +1$). Then, by Lemma 6.18, the indices $l_1, \dots, l_j \geq 3$ are distinct (each peeling removes the peeled coordinate), and

$$L = a_1\chi_1 + sa_2\chi_2 + \sum_{i=1}^{j} a_{i+2}\chi_{l_i} + b_j M^{(j)},$$

where the last term is absent if $\mu_j = 1$ (then $b_j = 0$). For $j = 0$ every point with $r < 1$ counts as positively peeled (through the empty list). Throughout, $E_4' = 3 + \max(0, \kappa_4)$; for any remainder $N = \sum \gamma_i \chi_i$ with $\sum \gamma_i^2 = 1$, $\mathbb{E}N^4 = 3 + \kappa_4 \sum \gamma_i^4 \leq E_4'$ by Lemma 6.11 (as $0 \leq \sum \gamma_i^4 \leq 1$), and $\mathbb{E}|N| \leq 1$.

6.8.1 Near-sphere bounds

Lemma 6.29 (near-sphere bound)**.** *Let $j \geq 1$, $n = j + 2$, and consider a point that is positively peeled through $I_1, \dots, I_j$. Let $Y_n = a_1\chi_1 + sa_2\chi_2 + \sum_{i=1}^{j} a_{i+2}\chi_{l_i}$, with atoms y_l and probabilities p_l ($l = 1, \dots, 2^n$), and $r_n = |(a_1, \dots, a_n)| = \sqrt{1 - b_j^2}$. Then*

$$\mathbb{E}|L| \leq \mathbb{E}|Y_n| + \sum_l p_l \min\Big(b_j,\ \frac{27}{128}\frac{b_j^4 E_4'}{|y_l|^3}\Big). \tag{6.8}$$

Suppose moreover that $q \in [q_6, q_5]$, that all $y_l \neq 0$, that $\frac{27}{128} E_4' \, b_j^2 (1 + r_n) \sum_l p_l |y_l|^{-3} < T_5$, and, if $n \geq 5$, that $s = 1$ and $a_i > q \sum_{i'=1}^n a_{i'}$ for $i = 1, \dots, n$. Then $\mathbb{E}|L| < T_5$ if $b_j > 0$. If $b_j = 0$, then $\mathbb{E}|L| = \mathbb{E}|Y_n| \leq T_5$, and equality holds only if $s = 1$, $a_1 = \cdots = a_n = n^{-1/2}$, and either $n = 5$, or $n = 4$ and $q = q_5$, or $n = 6$ and $q = q_6$.

Proof. If $\mu_j = 1$ then $b_j = 0$ and $L = Y_n$. Otherwise $L = Y_n + b_j M^{(j)}$ with $M^{(j)}$ independent of the n bits of Y_n; conditioning on these bits and applying Lemma 6.27 with $Z = M^{(j)}$ gives (6.8).

Now assume the extra hypotheses and let $c = (a_1, s a_2, a_3, \dots, a_n)$, so that $\mathbb{E}|Y_n| = G_n(c)$ and $|c| = r_n$. All a_i are positive: $a_1 > 0$; $a_{i+2} = b_{i-1}\mu_i > 0$, because $b_0 = b > 0$, $b_i > 0$ for $i < j$ (as $\mu_i < 1$) and $\mu_i > 0$; and $a_2 \geq |\alpha_{l_1}| = a_3$. We show $G_n(c) \leq T_5 r_n$, with equality only if $s = 1$, all a_i are equal, and (n, q) is as in the statement. For $n = 3$ this is Lemma 6.7, with strict inequality. For $n = 4$ it is Lemma 6.8: equality forces $q = q_5$ and c to be a positive multiple of $\pm(1, 1, 1, 1)$; as $c_1 = a_1 > 0$ the sign is $+$, so $s = 1$ and all a_i are equal. For $n \geq 5$ we have $s = 1$, and $c = (a_1, \dots, a_n)$ satisfies the hypothesis of Lemma 6.6, so $G_n(c) = 2\tau(1-q)^{n-1} \sum_i a_i \leq T_n r_n$, with equality iff all a_i are equal; and $T_n \leq T_5$ for $q \geq q_6$ by Lemma 6.4(ii), with equality iff $n = 5$, or $n = 6$ and $q = q_6$ (for $n \geq 7$, $T_n \leq T_7 < T_6 \leq T_5$, since $T_7 < T_6$ iff $1 - q < \sqrt{6/7}$, and $1 - q \leq \sqrt{5/6}$).

If $b_j > 0$, the hypothesis and $1 - r_n = b_j^2/(1 + r_n)$ give $\sum_l p_l \frac{27}{128} \frac{b_j^4 E_4'}{|y_l|^3} < T_5 \frac{b_j^2}{1 + r_n} = T_5(1 - r_n)$, hence $\mathbb{E}|L| < T_5 r_n + T_5(1 - r_n) = T_5$ by (6.8). If $b_j = 0$, then $r_n = 1$ and $\mathbb{E}|L| = \mathbb{E}|Y_n| = G_n(c) \leq T_5$, with equality only as stated. □

Piece tests (A_n)**,** (B_n)**.** Let B be a box with sign s and $b^- > 0$, let $j \geq 1$, $n = j + 2$, and $I_i = [\mu_i^-, \mu_i^+] \subset (0, 1]$ for $i = 1, \dots, j$. On $B \times I_1 \times \cdots \times I_j$ we enclose $a_1 = rc(t) \in [r_1 c(t_2), r_2 c(t_1)]$, $a_2 = rd(t) \in [r_1 d(t_1), r_2 d(t_2)]$, $b_0^2 \in [(b^-)^2, (b^+)^2]$ with b^+ a rational upper bound of $\sqrt{1 - r_1^2}$, and recursively

$$b_i^2 \in \big[(b_{i-1}^2)^-(1 - (\mu_i^+)^2),\ (b_{i-1}^2)^+(1 - (\mu_i^-)^2)\big], \qquad a_{i+2} = b_{i-1}\mu_i \in \big[b_{i-1}^- \mu_i^-,\ b_{i-1}^+ \mu_i^+\big],$$

where $b_{i-1}^\pm$ are the square roots of the bounds of b_{i-1}^2; and $r_n \leq r_n^+ := \min(1, \sqrt{1 - (b_j^2)^-})$. The 2^n atoms y_l, the probabilities p_l and the products $p_l y_l = \tau \sum_i (\pm c_i) \prod_{i' \neq i} \Pr[\cdot]$ (by $qu = (1-q)v = \tau$, as in Lemma 6.5; $c = (a_1, s a_2, a_3, \dots, a_n)$) are enclosed in interval arithmetic over $u \in [u_1, u_2]$. Let η_l be a lower bound of $|y_l|$, p_l^+ an upper bound of p_l, $|p_l y_l|^+$ an upper bound of $|p_l y_l|$, b_j^+ an upper bound of $\sqrt{(b_j^2)^+}$, $a_i^\pm$ the bounds of a_i, $q^+ = \frac{1}{1 + u_1^2}$, $E_4'^+ = 3 + \max(0, w^+ - 4)$ and $T^- = T^-(u_1, u_2)$. The piece $(B; I_1, \dots, I_j)$ passes

- test (A_n) if all $\eta_l > 0$; if $n \geq 5$, also $s = 1$ and $a_i^- > q^+ \sum_{i'=1}^n a_{i'}^+$ for $i = 1, \dots, n$; and $\frac{27}{128} E_4'^+ (b_j^2)^+ (1 + r_n^+) \sum_l p_l^+ \eta_l^{-3} < T^-$;
- test (B_n) if $\sum_l \big(|p_l y_l|^+ + p_l^+ \min\big(b_j^+, \frac{27}{128}((b_j^2)^+)^2 E_4'^+ / \eta_l^3\big)\big) < T^-$, where the second entry of the minimum is omitted if $\eta_l = 0$.

Consider a point of B that is positively peeled through $I_1, \dots, I_j$. All quantities above lie in their enclosures, $E_4' \leq E_4'^+$ (as $\kappa_4 = w - 4$ and $w \leq w^+$), and $T^- \leq T_5(u)$ by (6.2). In (A_n) with $n \geq 5$, $\sum_{i'} a_{i'}^+ > 0$, so $a_i \geq a_i^- > q^+ \sum_{i'} a_{i'}^+ \geq q \sum_{i'} a_{i'}$. Hence: if the piece passes (A_n) and $q \in [q_6, q_5]$, the hypotheses of Lemma 6.29 hold, so $\mathbb{E}|L| < T_5$ if $b_j > 0$, and $\mathbb{E}|L| \leq T_5$ with equality only as in Lemma 6.29 if $b_j = 0$. If the piece passes (B_n), then $\mathbb{E}|L| < T_5$ by (6.8) alone, since $\mathbb{E}|Y_n| = \sum_l |p_l y_l|$ (this holds for every $u \in [u_1, u_2]$ and either sign s).

6.8.2 Split nodes

For a box B with sign s and intervals $I_1, \dots, I_l \subset (0,1]$ ($l \ge 0$) put $X_l = [t_1,t_2]\times[r_1,r_2]\times I_1 \times \cdots \times I_l$ (parameters of the patch p_{2+l}) and $\sigma_l = (1, s, 1, \dots, 1) \in \{1,-1\}^{2+l}$. For $\mu \in (0,1]$ let $\kappa(\mu) = \min(1, \mu/\sqrt{1-\mu^2})$, with $\kappa(1) = 1$. It is nondecreasing, and by (6.7), $\mu(M^{(i)}) \le \kappa(\mu_i)$ whenever $\mu_i < 1$. A rational $\kappa' \ge 0$ satisfies $\kappa' \ge \kappa(\mu)$ iff $\kappa' \ge 1$, or $\mu < 1$ and $\kappa'^2(1-\mu^2) \ge \mu^2$.

Definition 6.30 (split node)**.** Let B be a box with sign s and $r_2 < 1$ (so $b^- > 0$), let $l \ge 0$, $I_1, \dots, I_l \subset (0,1]$, and $\hat\kappa \in (0,1]$. A *split node of level l on $(B; I_1, \dots, I_l)$ with range $\hat\kappa$* consists of a rational *cut* $m_c \in (0,1]$, a vertex certificate $\mathcal{C}$ for $(X_l, \sigma_l, [u_1,u_2], m_c, -)$, and two finite families of intervals $[n_1,n_2] \subset (0,1]$, the *plus pieces* and the *minus pieces*, each family covering $[m_c, \hat\kappa]$. Each plus piece is of one of the following types:

- (A_{l+3}) or (B_{l+3}): the piece $(B; I_1, \dots, I_l, [n_1,n_2])$ passes this test;
- TC^+: a rational cap $\kappa' \in (0,1]$ with $\kappa' \ge \kappa(n_2)$, and a vertex certificate for $(X_l \times [n_1,n_2],\ (\sigma_l, 1),\ [u_1,u_2],\ \kappa',\ -)$;
- TCN: a rational $\kappa' \in (0,1]$ with $\kappa' \ge \kappa(n_2)$, and a split node of level $l+1$ on $(B; I_1, \dots, I_l, [n_1,n_2])$ with range κ' (its *child*);
- TCS: a TCN piece whose child, with cut m_c' and range κ', has exactly one minus piece, $[m_c', \kappa']$, of type SG with cap κ', and only plus pieces of type (A_{l+4}) or (B_{l+4}).

Each minus piece is of one of the following types:

- SG: a rational p^* with $2n_1^2 > 1$ and $\varphi(n_1) \le p^* < 0$, a rational cap $\kappa' \in (0,1]$ with $\kappa' \ge \min(n_2, \hat\kappa)$, and a vertex certificate for $(X_l, \sigma_l, [u_1,u_2], \kappa', p^*)$;
- TC^-: a rational cap $\kappa' \in (0,1]$ with $\kappa' \ge \kappa(n_2)$, and a vertex certificate for $(X_l \times [n_1,n_2],\ (\sigma_l, -1),\ [u_1,u_2],\ \kappa',\ -)$.

The *height* of a node is 0 if it has no TCN piece (including TCS), and otherwise one more than the largest height of its children.

A TCS piece is stored compactly: its cap κ', the cut m_c', the value p'^*, the two vertex certificates (cap m_c'; cap κ' with p'^*) and the sub-pieces. In the notation of Theorem 5, $\mathsf{TC4}$, $\mathsf{TC4S}$ and $\mathsf{SG3}$ are the pieces $\mathsf{TC}^\pm$, TCS and SG of a node of level one.

Lemma 6.31 (split node lemma)**.** *Let $\mathcal{N}$ be a split node of level l on $(B; I_1, \dots, I_l)$ with range $\hat\kappa$. Consider a point of B with $q \in [q_6, q_5]$ that is positively peeled through $I_1, \dots, I_l$, with $\mu_l < 1$ if $l \ge 1$, and with $\mu_{l+1} = \mu(M^{(l)}) \le \hat\kappa$. Then $\mathbb{E}|L| \le T_5$. Equality forces $s = 1$ and $\alpha = n^{-1/2}(e_1 + e_2 + e_{l_1} + \cdots + e_{l_{n-2}})$ for distinct $l_1, \dots, l_{n-2} \ge 3$, where $n = 5$, or $n = 4$ and $q = q_5$, or $n = 6$ and $q = q_6$.*

Proof. Induction on the height of $\mathcal{N}$. By Lemma 6.18(i) with $j = l$ (for $l = 0$: $L = a_1\chi_1 + sa_2\chi_2 + bM$), $\mathbb{E}|L| = \mathbb{E}F_{p_{2+l}(\xi)}(M^{(l)})$ with $\xi = (t, r, \mu_1, \dots, \mu_l) \in X_l$ and the sign vector σ_l. Write $\mu = \mu_{l+1}$.

Case $\mu \le m_c$. $M^{(l)}$ belongs to the class $\mathcal{Z}$ of $\mathcal{C}$ (cap m_c), and Lemma 6.25 gives $\mathbb{E}|L| < T_5$.

Case $\mu \ge m_c$, and $M^{(l)}$ has the coefficient $+\mu$ at some $\chi_{l_{l+1}}$. We peel it ($\varsigma_{l+1} = +1$). As $\mu \in [m_c, \hat\kappa]$, μ lies in a plus piece $[n_1,n_2]$, and the point is positively peeled through $I_1, \dots, I_l, [n_1,n_2]$.

- (A_{l+3}) or (B_{l+3}): by Lemma 6.29 and the consequences of the piece tests (with $j = l+1$, $n = l+3$), $\mathbb{E}|L| < T_5$, except for (A_{l+3}) with $b_{l+1} = 0$, where $\mathbb{E}|L| \le T_5$. In that case $L = Y_n$, i.e. $\alpha = a_1e_1 + sa_2e_2 + \sum_{i=1}^{l+1} a_{i+2}e_{l_i}$, and equality forces $s = 1$, all $a_i = n^{-1/2}$, and (n,q) as in the statement.

- TC^+: if $\mu < 1$, Lemma 6.18(i) with $j = l+1$ gives $\mathbb{E}|L| = \mathbb{E}F_{p_{3+l}(\xi,\mu)}(M^{(l+1)})$ with the sign vector $(\sigma_l, 1)$, where $(\xi, \mu) \in X_l \times [n_1, n_2]$ and $\mu(M^{(l+1)}) \le \kappa(\mu) \le \kappa(n_2) \le \kappa'$; so $M^{(l+1)}$ is in the class of the certificate, and Lemma 6.25 gives $\mathbb{E}|L| < T_5$. If $\mu = 1$, then $n_2 = 1$ and $\kappa' = 1$, and $F_{p_{3+l}(\xi,1)}(y) = \mathbb{E}|L|$ for every y (Lemma 6.18(ii)); with $Z = \chi'$ (in the class, cap 1), $\mathbb{E}|L| = \mathbb{E}F_{p_{3+l}(\xi,1)}(Z) < T_5$.
- TCN (in particular TCS), with child $\mathcal{N}'$ of cut m_c' and range κ': if $\mu = 1$, then $F_{p_{3+l}(\xi,1)}(y) = \mathbb{E}|L|$ for every y, with the sign vector σ_{l+1}, and $Z = N^{-1/2}(\chi_1' + \cdots + \chi_N')$ with $N^{-1/2} \le m_c'$ is in the class of the certificate of $\mathcal{N}'$ (patch parameters X_{l+1}, sign vector σ_{l+1}, cap m_c'); so $\mathbb{E}|L| = \mathbb{E}F_{p_{3+l}(\xi,1)}(Z) < T_5$. If $\mu < 1$, the point is positively peeled through $I_1, \dots, I_l, [n_1, n_2]$ with $\mu_{l+1} < 1$, and $\mu_{l+2} \le \kappa(\mu) \le \kappa(n_2) \le \kappa'$; the induction hypothesis for $\mathcal{N}'$ (whose height is smaller) gives $\mathbb{E}|L| \le T_5$, with equality only as stated.

Case $\mu \ge m_c$, and $M^{(l)}$ has no coefficient $+\mu$. Then it has the coefficient $-\mu$ at some $\chi_{l_{l+1}}$, and $\mu \in [m_c, \hat{\kappa}]$ lies in a minus piece $[n_1, n_2]$.

- SG: by Lemma 6.13 (applied to $M^{(l)}$ with $n_1 \le \mu$ in place of m_c), $p_3(M^{(l)}) \le \varphi(n_1) \le p^*$; and $\mu \le \min(n_2, \hat{\kappa}) \le \kappa'$. So $M^{(l)}$ is in the class of the certificate, and Lemma 6.25 gives $\mathbb{E}|L| < T_5$.
- TC^-: exactly as for TC^+, peeling the coefficient $-\mu$ ($\varsigma_{l+1} = -1$, sign vector $(\sigma_l, -1)$): $\mathbb{E}|L| < T_5$.

□

6.8.3 The m-split boxes

Definition 6.32 (m-split box)**.** An m-split box (kind ms) is a box B with sign s and $r_2 < 1$, together with a split node of level 0 on B with range $\min(1, \bar{m}(B))$.

Lemma 6.33 (m-split lemma)**.** *Let B be an m-split box. At every point of B with $r < 1$ and $q \in [q_6, q_5]$ we have $\mathbb{E}|L| \le T_5$. Equality forces $s = 1$ and $\alpha = n^{-1/2}(e_1 + e_2 + e_{l_1} + \cdots + e_{l_{n-2}})$ for distinct $l_1, \dots, l_{n-2} \ge 3$, where $n = 5$, or $n = 4$ and $q = q_5$, or $n = 6$ and $q = q_6$.*

Proof. Every point with $r < 1$ is positively peeled through the empty list, and $\mu_1 = m \le \min(1, a_2/b) \le \min(1, \bar{m}(B))$ (Section 6.6). Apply Lemma 6.31 with $l = 0$. □

6.9 Computer verification

All scripts and outputs are in the repository (`scripts/`, `outputs/`). Floating point (HiGHS linear programming via scipy, numpy) is used only to *find* certificates. Every *verification* is exact or uses outward-rounded interval arithmetic.

6.9.1 Data

The list of data files is `outputs/k5_manifest.json` ($U_- = \frac{29106}{10000}$, $U_+ = \frac{3236855}{1000000}$, $T_8 = \frac{20711}{50000}$, $A_S = \frac{1}{4}$); md5 sums are in `outputs/k5_MD5SUMS.txt`.

- One-coordinate cells: `outputs/k5/one_0.json`, …, `one_3.json` ($u \in [U_-, 3]$, $[3, \frac{31}{10}]$, $[\frac{31}{10}, \frac{16}{5}]$, $[\frac{16}{5}, U_+]$; 234, 232, 245 and 150 cells, 861 in all, all with degree-ten certificates), covering $u \in [U_-, U_+]$ and $a \in [0, \frac{1}{4}]$.

- Two-coordinate boxes: `outputs/k5/m_i.json` ($s = -1$, $i = 0, \dots, 32$) and `outputs/k5/p_i.json` ($s = +1$, $i = 0, \dots, 23$), on the u-slabs $[U_-, \frac{292}{100}]$, $[\frac{292}{100}, \frac{293}{100}]$, $\dots$, $[\frac{322}{100}, \frac{323}{100}]$, $[\frac{323}{100}, U_+]$ (slab i is the $(i+1)$-st). For $s = +1$ the slabs $i = 24, \dots, 32$, next to u_6, are split into equal u-subslabs, with files `outputs/k5/p_is0.json`, `p_is1.json`, $\dots$: four subslabs for $i = 24, \dots, 30$ and eight for $i = 31, 32$; there is no file `p_i.json` for these i. For each sign the boxes cover $[U_-, U_+] \times [0, T_8] \times [\frac{1}{4}, 1]$. Each file records $K = 5$, $A_S = \frac{1}{4}$ and the maximal level 2 of TCN nodes. Each box record has its kind and data: small, lpv (n_0, the vertices and one coefficient vector per vertex), ncA/ncB, and ms (the split node: m_c, a cap, $\mathcal{C}$ and the pieces; each piece records its interval and type and, according to the type, its cap, p^* value, vertex certificates, sub-pieces, or child node). Only the kinds lpv and ms occur in the data (Table 6.1).

sign	lpv	ncA/ncB	ms	small	total
$s = +1$	3804	0	4303	0	8107
$s = -1$	1059	0	0	0	1059

Table 6.1: Two-coordinate boxes for Theorem 6. Widths range from 0.00086 to 0.01 in u, from 0.013 to 0.1 in t and from 0.023 to 0.094 in r. The ms boxes carry split nodes of height 0 (2017 boxes), 1 (809), 2 (1348) and 3 (129), where, as in Definition 6.30, a TCS piece counts as a TCN piece. Besides the children of the TCS pieces, which are stored with them, there are 4303 nodes of level 0, 4873 of level 1 and 3958 of level 2. Cuts: level 0 $\frac{2}{5}$ (1335), $\frac{7}{20}$ (1330), $\frac{9}{20}$ (1034), $\frac{1}{2}$ (592), $\frac{3}{10}$ (10), $\frac{3}{4}$ (2); level 1 $\frac{1}{2}$ (1281), $\frac{11}{20}$ (1094), $\frac{13}{20}$ (902), $\frac{9}{20}$ (825), $\frac{3}{5}$ (771); level 2 $\frac{13}{20}$ (3913), $\frac{3}{5}$ (45). Pieces: level 0: minus 2 SG, 4301 TC; plus 5445 TC, 4873 TCN, 58 TCS; level 1: minus 4873 TC; plus 127 (A4), 5768 TC, 3958 TCN, 1400 TCS; level 2: minus 3958 TC; plus 1431 (A5), 6240 TC, 396 TCS. Every TCS piece has $m_c' = \frac{17}{20}$; the sub-pieces are 58 (A4) at level 0, 1769 (A5) at level 1, 644 (A6) at level 2. There are 52 292 vertex-certificate sets (4863 in lpv boxes, 47 429 in split nodes) with 784 616 vertices; 9168 of them have two patch parameters, 14 735 three, 17 399 four and 10 990 five. The polynomials of 24 326 vertices have degree 10, all others degree 6.

6.9.2 Generation

`scripts/run_k5.sh` writes the 105 jobs (101 two-coordinate jobs: the plus slabs $i = 0, \dots, 23$, the 44 plus u-subslabs and the 33 minus slabs; and 4 one-coordinate jobs) to `outputs/k5/jobs_all.txt`. A two-coordinate job is `python3 cover6.py u1 u2 s out.json` ν `4 8 16` with the environment `RQ_K=5 RQ_AS=1/4 RQ_MSD=5 RQ_MAXLEV=2 RQ_WTCN=1/16` and the lists of cuts `RQ_MCS0` $= \frac{9}{10}, \frac{17}{20}, \frac{4}{5}, \frac{3}{4}, \frac{1}{2}, \frac{9}{20}, \frac{2}{5}, \frac{3}{5}, \frac{7}{20}, \frac{3}{10}$ (root nodes), `RQ_MCSN` $= \frac{13}{20}, \frac{3}{5}, \frac{11}{20}, \frac{1}{2}, \frac{9}{20}, \frac{2}{5}$ (children of TCN pieces) and `RQ_MCST` $= \frac{17}{20}, \frac{4}{5}, \frac{3}{4}$ (TCS pieces). It bisects $[u_1, u_2] \times [0, T_8] \times [\frac{1}{4}, 1]$ adaptively (ν initial u-intervals, 4 initial t-intervals, 8 r-intervals, depth ≤ 16) and on each box tries, in order: small; the near-circle tests (`nearcircle.py`); a vertex certificate (`cert5.py`); from depth 5 on, a split node of level 0 (`cover6.try_ms`). In a node of level l with range $\hat\kappa$ the cut m_c is the first value $m_c < \hat\kappa$ of the list for which $\mathcal{C}$ exists and both sides can be covered; each side is covered by bisecting $[m_c, \hat\kappa]$ (depth at most 4 at level 0 and 3 below, at most 10 pieces). A plus piece is tried as $(\mathrm{A}_{l+3})/(\mathrm{B}_{l+3})$ (generator-side tests `nsphere3.py`, `cert4.py` and `cover6.check_piece_n` for $n = 3$, 4, ≥ 5), then TC^+ with $\kappa' = \kappa(n_2)$ (rounded up), then TCS (cuts from `RQ_MCST`, sub-pieces by bisection, depth at most 6, at most 24), and, if $l + 1 \le 2$ and the piece has width at most $\frac{1}{16}$, TCN with range $\kappa(n_2)$ (rounded up); a minus piece as SG (if $2n_1^2 > 1$, with cap $\min(n_2, \hat\kappa)$) and then TC^-. Vertex sets with two

or three patch parameters come from `cert5.py` and those with four or five from `cert6.py` (n_0 a rational approximation of the patch point at the centre with $|n_0| \geq 1$; the polytope is a box in an exactly orthogonal rational basis of $n_0^{\perp}$ containing the gnomonic projection of a grid of the patch with a relative margin; its corners are the vertices). The cone check is the exact test of Lemma 6.21 (`sphmin.py`). The coefficient vectors come from a discretised moment linear program (degree 6, or 10 if degree 6 fails), rounded to rationals and repaired; (W1), (W2) and (P1)–(P4) are checked exactly before a record is accepted. One-coordinate cells come from `cover_lp10.py` (degree-ten certificates), run with `RQ_LPFALLBACK=1`: if the HiGHS simplex method stops without a solution, the linear program is solved again by the interior-point method and with other reference points u of the cell. This changes only where a candidate comes from. Without it, the job for $u \in [3, \frac{31}{10}]$ left two cells unproved ($u \in [3 + \frac{254}{10240}, 3 + \frac{256}{10240}]$, $a \in [\frac{351}{2048}, \frac{352}{2048}]$; the simplex method failed there at every depth); the other three one-coordinate files are byte-identical with and without it. No box or cell of the final data failed.

The slabs were started with $\nu = 1$. The plus slabs in $[\frac{315}{100}, U_+]$, next to u_6, progressed too slowly and were replaced by the u-subslabs listed above (each again with $\nu = 1$); the whole-slab runs were stopped before they ended and left no data. Two runs started on RQ-A's machine while RQ-C was finishing the same jobs (the plus slabs $i = 14, 15$) were killed within minutes and left no data either; RQ-C's files are used. Jobs were run by `scripts/k5_sched.py` (queue `outputs/k5/queue.txt`) on RQ-A's machine and, for 54 of the 105 files (the $s = -1$ slabs, the plus slabs $i = 10, \ldots, 23$ and the subslabs `p_24s0`, ..., `p_24s3`, `p_25s1`, `p_25s2`, `p_25s3`), by RQ-C with an unmodified copy of `scripts/` (md5 sums of the copied scripts in `outputs/k5/RQC_SCRIPTS_MD5SUMS.txt`; delivered files and their md5 sums in `outputs/k5/RQC_MD5SUMS.txt`, logs in `outputs/k5/logs/*.rqc.log`). The copy differs from the final `scripts/` in six files, none of which a two-coordinate job runs: `run_k5.sh` (the job list, in which $p_{24}, \ldots, p_{32}$ were whole slabs, and `RQ_LPFALLBACK` for the one-coordinate jobs), `cover_lp10.py` (the fallback), the verifier `verify_k5.py` and its negative tests `break_tests_k5.py`, `build_main_md.py` and `mirror.sh`. The generators of the two-coordinate jobs (`cover6`, `cert4`, `cert5`, `cert6`, `sphmin`, `nearcircle`, `nsphere3` and their imports) are identical. Generation is not part of the proof: all files are checked in the same way by the verifier. The 101 two-coordinate jobs took 65.6 hours in total (40.1 hours for the 44 subslabs; the longest job, p_{23}, took 135 minutes), and the four one-coordinate jobs took 2 to 3.5 minutes each.

6.9.3 Independent verification

`python3 verify_k5.py` re-checks everything from the data files, and all parts pass (output `outputs/verify_k5_ABCDEFG.txt`; 4449 seconds on 8 cores, 9.8 hours of CPU time, almost all of it in part D). It shares no code with the generators (`cert2c`, `cert4`, `cert5`, `cert6`, `sphmin`, `cover6`, `cover_lp10`, `tenmom`, `nsphere3`, `nearcircle`, `exactcert`, `fourbit`, `bitlemma_k4`, `bitlemma_k5`). It reuses the exact helpers of `verify_k4.py` (the verifier of Theorem 5: exact facet minima of nested patches, vertex-certificate domination, interval helpers), of `verify_k3b.py` (the verifier of Theorem 4: moment polynomials, objective bound, facet normals, atom enclosures, envelopes, cap and φ checks, interval coverage, symbolic part A) and the Sturm-sequence, integer-square-root and tiling helpers of `verify_all.py` (the verifier of Theorem 1, audited in A.6). It replaces the range enclosure of the polynomials G_j of `verify_k3b.py`, whose bisection does not terminate when G_j' has a root inside the range (for $k = 5$, G_9' vanishes at $w \approx 8.68$, i.e. $u \approx 2.926$), by its own: exact endpoint values on subintervals without a root of G_j' (Sturm), and interval Horner evaluation on subintervals of length 2^{-30} times the range that still contain one. Its parts:

A. Symbolic identities (sympy). Lemma 6.10: the cumulants of χ, computed from its moments,

are $d^{[j \text{ odd}]}G_j(w)$ for $j = 3, \dots, 10$. Lemma 6.11: the recursion reproduces the Gaussian moments, and also the moments of χ at $u = \frac{5}{2}$, up to order ten.

B. Coverage (exact). $U_- \le u_5$ (checked as $U_-^2 \le 4$ or $(U_-^2 - 4)^2 \le 20$); $U_+ \ge u_6$ (checked as $U_+^2 \ge 5$ and $(U_+^2 - 5)^2 \ge 30$); (6.3); and $T_8 \ge \sqrt{2} - 1$. The cells tile $[U_-, U_+] \times [0, \frac{1}{4}]$. For each sign the boxes tile $[U_-, U_+] \times [0, T_8] \times [\frac{1}{4}, 1]$: they lie in the region, have pairwise disjoint interiors and total volume equal to the volume of the region (a closed subset of full measure is dense, so it is the whole region). Every box has the sign of its file and one of the kinds small, lpv, ncA, ncB, ms, so that one of the parts B, D, E, F checks it. Every small box satisfies $r_2 c(t_1) \le A_S$. Every file has $K = 5$ and $A_S = \frac{1}{4}$, and no file lists a failed box or cell.

C. One-coordinate cells: (V1)–(V3) by Sturm sequences; $\Theta_1 > 0$; (V4) strictly (Definition 6.14 re-implemented: the polynomials μ_n from the recursion, the monomial bounds, and a Sturm count of the roots of h on $[0, \bar{m}]$ together with $h(0) > 0$).

D. Vertex certificates of every node of every split tree: all lpv records; in every node $\mathcal{C}$; in every $\mathsf{TC}^{\pm}$, SG and TCS piece its certificates. (P1) and (P2) exactly; (P3) by exact Gaussian elimination (rank k of each facet, normal vector, orientation by the centre); (P4) by the recursion of Lemma 6.21 as described after it, in an implementation of its own (exact sign decisions, integer square-root bounds, no rounding of intermediate values); (W1) on every linear piece of every vertex envelope (Definition 6.22, recomputed from the atom enclosures over $[u_1, u_2]$); (W2) strictly with the target $T^-(u_1, u_2)$. The patch parameters, sign vector, cap and p^* value of each certificate are taken from the structure: X_l (or $X_l \times [n_1, n_2]$) and σ_l (or $(\sigma_l, \pm 1)$) from the position in the tree; $\bar{m}(B)$ (recomputed exactly) for lpv; the cut m_c of the node for $\mathcal{C}$; for TCS the recorded m_c', and the recorded cap κ' with the recorded p'^*; and the recorded cap $\kappa' \in (0, 1]$ (and $p^* < 0$ for SG) for the others.

E. Near-circle boxes: mpmath interval arithmetic (120 bits), tests (A)/(B) strictly, with the target $T^-(u_1, u_2)$ of Lemma 6.28, enclosed in interval arithmetic.

F. Split trees: for every ms box $r_2 < 1$ and a recorded root cap $\ge \min(1, \bar{m}(B))$; recursively, for every node: $0 < m_c < \kappa \le 1$ for its recorded cap κ (the range at the root is $\min(1, \bar{m}(B))$, below a TCN piece $[n_1, n_2]$ it is κ, and $\kappa \ge \kappa(n_2)$ is checked as $\kappa \ge 1$ or $\kappa^2(1 - n_2^2) \ge n_2^2$); the plus pieces and the minus pieces each cover $[m_c, \hat{\kappa}]$; every near-sphere piece of a node of level l is of type $(\mathrm{A}_{l+3})/(\mathrm{B}_{l+3})$ and passes one of the two tests (mpmath, strict; (A_n) with $n \ge 5$ includes $s = 1$ and the OR-region condition); the cap condition $\kappa' \ge \kappa(n_2)$ of $\mathsf{TC}^{\pm}$ and TCS; for TCS, $m_c' < \kappa'$, the φ condition of (m_c', p'^*), the cover of $[m_c', \kappa']$ by the sub-pieces, and the sub-pieces of type $(\mathrm{A}_{l+4})/(\mathrm{B}_{l+4})$ passing their tests; for SG, the φ condition of (n_1, p^*) ($0 < n_1 \le 1$, $2n_1^2 > 1$, $p^* < 0$, and $p^* \ge \varphi(n_1)$, checked as $p^* + n_1^3 \ge 0$ and $(p^* + n_1^3)^2 \ge (1 - n_1^2)^3$) and $\kappa' \ge \min(n_2, \hat{\kappa})$.

G. The claims (C1) and (C2) of Lemmas 6.7 and 6.8, for all 2^8 and all 2^{16} functions, exactly as described there, including the list of equality cases ($\pm$OR of four bits at q_5 only; none for three bits).

The generator side has its own exact check of the bit lemmas (`scripts/bitlemma_k5.py`, output `outputs/bitlemma_k5.txt`, same result).

Negative tests. `python3 break_tests_k5.py` corrupts random samples of records (seed 13) and runs the check functions of `verify_k5.py` on them (26 seconds; output `outputs/break_tests_`

k5.txt). Every corruption below is rejected in every case. On 40 lpv boxes: lowering the constant term of one vertex polynomial by $\frac{1}{20}$ (domination fails), raising it by 1 (the objective bound fails), shrinking the polytope by 10% about its centre (the cone check fails) and moving one vertex by 10^{-6} (the hyperplane/parallelepiped check fails). On 40 split nodes of any level: removing one plus piece or one minus piece (coverage fails). On 25 ms boxes: lowering the root cap below $\min(1, \bar{m}(B))$, with the pieces clipped to the new cap (the top check fails). At 60 split nodes: replacing the cap of a TC, TCS or TCN piece $[n_1, n_2]$ with $n_2 < 1$ by n_2 (112 cases; the cap check $\kappa' \geq \kappa(n_2)$ fails). For both SG pieces of the data: lowering p^* to $\varphi(n_1) - \frac{1}{100}$ (the φ check fails) and lowering the cap below $\min(n_2, \hat{\kappa})$ (the cap check fails). On 25 TCS pieces: widening the lowest near-sphere sub-piece from $[o_1, o_2]$ to $[\frac{o_1}{4}, o_2]$ (the near-sphere test fails). On 25 near-sphere pieces: changing the number of coordinates in the label (the type check fails). On 25 (A_5) and (A_6) pieces of boxes with $s = 1$: re-checking them with $s = -1$ (test (A_n), $n \geq 5$, must not pass, since the OR-region identity needs $s = 1$). On 25 nested split nodes: lowering the cut m_c by $\frac{1}{50}$ without adding pieces (coverage fails), and, for the 21 of them where the TCN piece $[n_1, n_2]$ of the node has $2n_2^2 < 1$ and there is room above m_c, lowering the cap of the node to a rational number between m_c and $\kappa(n_2) - 10^{-4}$, with the pieces clipped (the cap check fails). On 25 ms boxes: lowering the constant term of one vertex polynomial, in a vertex set of any level, by $\frac{1}{20}$ (domination fails). On 40 nested polytopes with three to five patch parameters: shrinking by $\frac{1}{2}$ about the centre (the cone check fails). Removing one box from the tiling, for each sign. On 30 one-coordinate cells: raising the constant term of the certificate by 1 (the objective bound fails). On 40 boxes: relabelling the kind as LPV, as the kind followed by a space, as nc, as the empty string and as msplit (200 cases; part B rejects them). Four sanity checks (not corruptions) hold: on the same 40 lpv boxes the recomputed cap $\bar{m}(B)$ is at least $\min(1, a_2/b)$ on the box; the 40 unmodified box records pass the per-box check of part B; and for 20 nested vertex sets the exact facet minima of the cone check are at most the minima of $h \cdot p$ over a sample of the patch (11^k points for $k \leq 4$ patch parameters, 6^5 for $k = 5$; up to $10^{-12}|h|_\infty$ for the rounding of the sample), and, for the 13 sets with $k \leq 4$, within $10^{-3}|h|_\infty$ of them.

6.9.4 Reproducing

```
pip install numpy scipy sympy mpmath
cd scripts
python3 verify_k5.py          # parts A-G, about 75 minutes on 8 cores
python3 break_tests_k5.py     # negative tests, about 30 seconds
python3 bitlemma_k5.py        # bit lemmas (generator-side check)
bash run_k5.sh                # regenerate all data (66 job-hours)
```

6.10 Proof of Theorem 6

(a) By Lemma 6.3 let $q \in [q_6, q_5]$, i.e. $u \in [u_5, u_6] \subseteq [U_-, U_+]$. Reduce α as in Section 6.2.3.

(1) $a_1 = 1$: $\alpha = e_1$ and $\mathbb{E}|L| = 2\tau < T_5$ (Lemma 6.4(iii)).

(2) $a_1 \leq \frac{1}{4}$: (u, a_1) lies in a cell, and Lemma 6.16 gives $\mathbb{E}|L| < T_5$.

(3) $a_1 > \frac{1}{4}$ and $r = 1$: $L = a_1\chi_1 + sa_2\chi_2$, and Lemma 6.5 gives $\mathbb{E}|L| < T_5$.

(4) $a_1 > \frac{1}{4}$ and $r < 1$: (u, t, r) lies in a box of the cover for the sign s (part B), since $t \in [0, \sqrt{2} - 1] \subseteq [0, T_8]$ and $r \geq a_1 > \frac{1}{4}$. It is not a small box, since $a_1 > A_S$. If it is lpv,

Lemma 6.26 gives $\mathbb{E}|L| < T_5$. If it is ncA or ncB, Lemma 6.28 gives $\mathbb{E}|L| < T_5$. If it is ms, Lemma 6.33 gives $\mathbb{E}|L| \le T_5$.

So $\mathbb{E}|L| \le T_5$ always, and $(e_1 + \cdots + e_5)/\sqrt{5}$ attains T_5 (Lemma 6.4, $q < \frac{1}{5}$). Hence $R(q) = T_5(q)$. For $q \in [1 - q_5, 1 - q_6]$ use Lemma 6.3: $R(q) = R(1 - q) = 2\sqrt{5}\, q^4\tau$.

(b) Equality can occur only in the ms case of (4). By Lemma 6.33, after the reduction, $\alpha = n^{-1/2}(e_1 + e_2 + e_{l_1} + \cdots + e_{l_{n-2}})$ with distinct $l_i \ge 3$, where $n = 5$, or $n = 4$ and $q = q_5$, or $n = 6$ and $q = q_6$. Undoing the reduction (global sign and permutation) gives the list in (b). Conversely, each listed vector attains T_5 at the stated q (Lemma 6.4): $(e_{i_1} + \cdots + e_{i_5})/\sqrt{5}$ gives T_5 for $q < \frac{1}{5}$; $(e_i + e_j + e_k + e_l)/2$ gives $T_4 = T_5$ at q_5 ($q_5 < \frac{1}{4}$); and $(e_{i_1} + \cdots + e_{i_6})/\sqrt{6}$ gives $T_6 = T_5$ at q_6 ($q_6 < \frac{1}{6}$). For $q \ge \frac{1}{2}$ use Lemma 6.3.

(c) For $q < q_6 < \frac{1}{6}$, $R(q) \ge \mathbb{E}|\chi_1 + \cdots + \chi_6|/\sqrt{6} = T_6(q) > T_5(q)$ by Lemma 6.4 and (ii). For $q_5 < q < \frac{1}{4}$, $R(q) \ge T_4(q) > T_5(q)$ by Lemma 6.4 and (i). For $\frac{1}{4} \le q \le \frac{1}{2}$, $R(q) \ge \mathbb{E}|\chi_1| = 2\tau$, and $2\tau > 2\sqrt{5}(1 - q)^4\tau$ because $5(1 - q)^8 \le 5(\frac{3}{4})^8 < 1$. □

6.11 Remarks

1. **The $k = 5$ regime is closed.** $R(q) = 2\sqrt{5}\,(1-q)^4\sqrt{q(1-q)}$ holds exactly on $[q_6, q_5]$, which is the largest possible interval (Corollary 6.1). Both ends are ties: at q_5 with $(e_1+e_2+e_3+e_4)/2$, at q_6 with $(e_1 + \cdots + e_6)/\sqrt{6}$. Given Theorem 5, Corollary 6.2 confirms the conjecture $R(q) = 2\tau \max_k \sqrt{k}\,\hat{q}^{\,k-1}$ (BF3, Stone; RQ-C's Conjecture S) on $[q_6, 1-q_6]$. The next regime, $k = 6$ on $[q_7, q_6]$ with $q_7 = 1 - \sqrt{6/7}$, is not treated here.

2. **Range of the computations.** The boxes and cells cover $u \in [U_-, U_+]$, slightly more than $[u_5, u_6]$. Outside $[u_5, u_6]$ the four-bit lemma (for $q > q_5$) or the bound $T_6 \le T_5$ (for $q < q_6$) fails, so the tests (A_4) and (A_6) would claim too much there, and the bit lemmas behind (A_3) and (A_4) are verified only on $[q_6, q_5]$ ((A_5) holds for every q, by the OR-region identity and Cauchy–Schwarz); this is why Lemmas 6.29, 6.31 and 6.33 and the proof of Theorem 6 use the data only for $q \in [q_6, q_5]$.

3. **From $k = 4$ to $k = 5$.** The structure of the proof does not depend on k: the one- and two-coordinate routes, the vertex certificates and the split nodes are the same, with the target T_k. What depends on k is the input at the leaves of the split trees: the near-sphere bound with n coordinates needs $G_n(c) \le T_k|c|$, which for $n < k$ is a bit lemma ($\sum_i \Delta_i(f)^2 \le 4k(1-q)^{2k-2}$ for all f on n bits, checked here by enumeration for $n \le 4$; RQ-C's C6 covers $n \le 7$), and for $n \ge k$ in the OR region is Lemma 6.6 with $T_n \le T_k$.

4. **Where the method is tight.** Split nodes are used in 4303 of the 8107 boxes with $s = +1$ and in none with $s = -1$. Their trees have height at least one in 2286 boxes, height two in 1348 and height three in 129 (heights as in Definition 6.30, where a TCS piece counts as a TCN piece). The trees of height three are those with a TCS piece at level two; they are exactly the 129 boxes with six-coordinate pieces. The near-sphere pieces follow the three extremisers. Four-coordinate pieces occur only for $u \le 3.09$ (123 boxes; $(e_1 + \cdots + e_4)/2$ ties at u_5). Six-coordinate pieces occur only for $u \ge 3.13$ (129 boxes; $(e_1 + \cdots + e_6)/\sqrt{6}$ ties at u_6). Five-coordinate pieces occur on the whole range (930 boxes), as $(e_1 + \cdots + e_5)/\sqrt{5}$ is extremal for every q of the regime (Table 6.1).

5. **Status.** Audited VALID by RQ-AUD (A.37, 2026-10-22 22:58 UTC), with no fix. A.37's cosmetic remark r1 is applied (23:04 UTC): Table 6.1 and Remark 4 now count heights as

in Definition 6.30. Nothing else was changed. Refereed VALID by RQ-REF2 (2026-10-23 01:05 UTC), with no fixes, together with Theorem 5 of `MAIN_RESULT_K4`, which Corollary 6.2 uses; after that report only this item was changed. The computer steps have been run twice (generator and independent verifier), the verifier rejects corrupted data (negative tests above), and the referee re-did every computer step with its own exact programs.

Part II

Poissonisation: the reduction of $(0, q_5]$ to a q-free inequality

Chapter 7

Level-one form, Poissonisation, and the reduction of $(0, q_5]$ to one inequality for infinitely divisible laws (RQ-B, Sections 1–4 and 6; RQ-A, U.1–U.3)

Source of Sections 7.1–7.5: RQ-B, `rq/MAIN_RESULT.tex` (md5 `e41938426653fabb413484e593485ccf`), "The L^1–L^2 constant $R(q)$ of biased bits for small q: Poissonization, the limit $q \to 0$, an explicit bound, and exact values conditional on an infinitely divisible Khintchine inequality", by "RQ-B (hard-math attack on $R(q)$, regime $q < 1 - 1/\sqrt{2}$)", dated October 22, 2026. This is the file RQ-REF3 refereed. RQ-B's `rq/MAIN_RESULT.md` (md5 `b47f294573d030edf79f8022a14d0346`) has the same content; its Sections 1–10 are Sections 2–11 of the `.tex` and its Section 13 is Section 12 of the `.tex`, and the team cites RQ-B's results by the `.md` numbers.

Source of Section 7.6: RQ-A, `CLAIMS.md`, Section U (see the box there).

Reproduced: the setting and notation of RQ-B's Section 1 (Definition 1.1, Conjectures C0 and C5), from Section 2 Theorem 2.1 with its proof and the paragraph defining q_K, g, $C(q)$ and (7.1), Sections 3 and 4 complete (Lemma 3.1, Theorem 4.1, Remarks 4.2–4.3, Theorem 4.4 with its proof, Remark 4.5), and Proposition 6.2 with its proof. Each omission is marked in the text. The omitted parts are not used by the chain.

Audit: A.7a (Lemma 7.5; VALID WITH FIXES on 22 October for a typo, which RQ-B fixed before A.10; re-rated VALID on 23 October, 07:48 UTC), A.10 (Theorem 4.1 = A.10a, VALID; Proposition 6.2 = part of A.10c, VALID; Theorem 7.4 re-proved correctly, it is Stone's theorem), A.26 (Theorem 7.9(a)–(e) = RQ-A U.1–U.2; VALID, NEW; fix f1 to U.3), and A.40 (the composition).

Referee: RQ-REF3, link 1, VALID ("by hand; constants re-checked exactly"): Lemma 7.5, Theorem 7.6 and Theorem 7.9(a)–(d), which the report identifies with RQ-A U.1–U.3. Report `REFEREE.md`, md5 `6ac713c05dd3a1b74e71d5c959ac0ceb`, FINAL, 03:09 UTC on 23 October.

Use in the Main Theorem: Theorem 7.4 in Step 2; Theorem 7.9(a)–(b) and (d), with Lemma 7.5 and Theorem 7.6, in Steps 3–4.

Transcription: RQ-B's theorem counter is numbered within sections; here the items are numbered $7.n$ in order, and each carries a tag with its numbers in RQ-B's `.tex` and `.md`. Labels are prefixed by `ch07:`. The headings of Sections 7.1 and 7.5 are those of this document. Three cross-references to parts that are not reproduced (RQ-B's Remark 9.7, Section 11 and Theorem 6.1) are written out as text. Four editorial footnotes in Sections 7.1–7.5: two at those rewritten references, one on the symbol q_0, and one on the status of the inequality ID$^*(C)$ (Appendix C).

7.1 Setting and notation

[RQ-B tex Section 1 "Setting, notation, and summary", without the summary]

By $\chi \mapsto -\chi$, $R(q) = R(1-q)$; we take $q \in (0, 1/2]$. Put $\tau = \sqrt{q(1-q)}$, $u = \sqrt{(1-q)/q}$, $v = \sqrt{q/(1-q)}$ (so $\chi \in \{u, -v\}$, $qu = (1-q)v = \tau$), and $\chi = (X-q)/\tau$ with $X \sim \text{Bernoulli}(q)$. Define

$$s = s(q) = \ln \tfrac{1}{1-q}, \qquad M(q) = \max_{k \geq 1} 2\sqrt{kq}\,(1-q)^{k-1/2},$$

$$B(q) = \sqrt{\frac{2q}{e(1-q)s}}, \qquad q_k^* = 1 - e^{-1/(2k)} \quad (k = 1, 2, \dots).$$

Definition 7.1 (Kolmogorov measures and R_{ID})**.** [RQ-B tex Definition 1.1] For a finitely supported probability measure $K = \sigma^2\delta_0 + \sum_{j=1}^m w_j \delta_{a_j}$ ($a_j \neq 0$, $w_j > 0$) let

$$Z_K = \sigma G + \sum_{j=1}^m a_j \Big(N_j - \frac{w_j}{a_j^2}\Big), \qquad G \sim N(0,1),\ N_j \sim \text{Poisson}(w_j/a_j^2),$$

all independent; $\mathbb{E}Z_K = 0$ and $\mathbb{E}Z_K^2 = K(\mathbb{R}) = 1$. Let $R_{\mathrm{ID}} = \sup_K \mathbb{E}|Z_K|$. Since a Gaussian is an L^2-limit of compensated Poisson variables with small jumps, the supremum is the same without the atom at 0; by L^2 approximation of Lévy–Itô decompositions it is also $\sup \mathbb{E}|Z|/\|Z\|_2$ over all mean-zero, finite-variance, infinitely divisible Z.

Conjecture 7.2 (C0, main conjecture in the regime)**.** [RQ-B tex Conjecture 1.2] *$R(q) = M(q)$ for $q \leq 1 - 1/\sqrt{2}$.*

Conjecture 7.3 (C5, infinitely divisible Khintchine inequality)**.** [RQ-B tex Conjecture 1.3] *$R_{\mathrm{ID}} = \sqrt{2/e}$; i.e. $\mathbb{E}|Z| \leq \sqrt{2/e}\,\|Z\|_2$ for every mean-zero infinitely divisible Z. Equivalently, $\mathbb{E}|\int h\, d(\eta - \mathrm{Leb})| \leq \sqrt{2/e}\,\|h\|_{L^2(\mathbb{R}_+)}$ for a unit-rate Poisson process η. Equality holds for $Z = a(N_{1/2} - \frac{1}{2})$.*

[Not reproduced here: RQ-B tex Section 1, the paragraph "Summary" (a list of the results of RQ-B's paper).]

7.2 Equal coefficients

Theorem 7.4. [RQ-B tex Theorem 2.1; md Theorem 1] *Let $q \in (0, 1/2]$ and $k \geq 1$ with $kq < 1$. Then*

$$\frac{\mathbb{E}|\chi_1 + \cdots + \chi_k|}{\sqrt{k}} = 2\sqrt{kq}\,(1-q)^{k-1/2}.$$

The maximum of the right-hand side over all $k \geq 1$ is attained at $k = \lfloor 1/(q(2-q))\rfloor$, which satisfies $kq < 1$; $k-1$ and k are both maximal exactly when $q = 1 - \sqrt{(k-1)/k}$. Consequently $R(q) \geq M(q)$, and $M(q) \to \sqrt{2/e}$ as $q \to 0$.

Proof. Let $S = X_1 + \cdots + X_k$, so $\sum_i \chi_i = (S - kq)/\tau$. Since $0 < kq < 1$ and $S \in \{0, 1, \dots\}$, $S - kq < 0$ iff $S = 0$. As $\mathbb{E}(S - kq) = 0$, $\mathbb{E}|S - kq| = 2\mathbb{E}(kq - S)_+ = 2kq(1-q)^k$, hence $\mathbb{E}|\sum \chi_i|/\sqrt{k} = 2kq(1-q)^k/(\tau\sqrt{k}) = 2\sqrt{kq}(1-q)^{k-1/2}$. With $h(k) = \sqrt{k}(1-q)^k$ we have $h(k+1)/h(k) = \sqrt{1 + 1/k}\,(1-q) \geq 1$ iff $k \leq (1-q)^2/(q(2-q)) = 1/(q(2-q)) - 1$, so h increases up to $k^* = \lfloor 1/(q(2-q))\rfloor$ and decreases afterwards, with $h(k-1) = h(k)$ iff $(1-q)^2 = (k-1)/k$. Also $k^* q \leq 1/(2-q) < 1$. For the limit, $2\sqrt{kq}(1-q)^{k-1/2} = 2\sqrt{q/(1-q)}\sqrt{k}\,e^{-ks}$, $\max_{\kappa > 0} \sqrt{\kappa} e^{-\kappa s} = (2es)^{-1/2}$ at $\kappa = 1/(2s)$, an integer within 1 of $1/(2s)$ gives $\sqrt{k}e^{-ks} = (2es)^{-1/2}(1 + o(1))$, and $q/((1-q)s) \to 1$. □

[Not reproduced here: RQ-B tex Remark 2.2 (de Moivre's formula for $kq \geq 1$; RQ-B notes that it is not used).]

For $K \geq 2$ let $q_K = 1-\sqrt{(K-1)/K}$ (the tie of $K-1$ and K equal coefficients; $q_4 = 1-\sqrt{3}/2$), let $g(x) = 2\sqrt{x}\,e^{-x}$ $(x \geq 0)$, $C(q) = \max_{k\geq 1} g(ks)$, and $r_1 = 2(3/2)^{3/2}e^{-3/2} = 0.819833$ (Remark 7.8). Since $(1-q)^k = e^{-ks}$,

$$M(q) = 2\sqrt{\tfrac{q}{1-q}} \max_{k\geq 1} \sqrt{k}\, e^{-ks} = \sqrt{\tfrac{q}{(1-q)s}}\, C(q). \tag{7.1}$$

[Not reproduced here: RQ-B tex Theorem 2.3 (equal coefficients, every k; md Theorem 1.2), its proof, and Remark 2.4. The chain does not use them.]

7.3 Level-one form

For $f : \{0,1\}^n \to [0,1]$ and the product Bernoulli(q) measure, let $\Delta_i(f) = \mathbb{E}[f \mid x_i = 1] - \mathbb{E}[f \mid x_i = 0]$ and $D(f) = \sum_i \Delta_i(f)^2$.

Lemma 7.5. [RQ-B tex Lemma 3.1; md Lemma 2.1] $R(q)^2 = 4q(1-q)\sup_{n,f} D(f)$.

Proof. $\mathbb{E}[f\chi_i] = \frac{q}{\tau}(\mathbb{E}[f \mid x_i = 1] - \mathbb{E}f) = \frac{q(1-q)}{\tau}\Delta_i(f) = \tau\Delta_i(f)$. Given α, let $L = \sum \alpha_i\chi_i$ and $f = 1\{L > 0\}$; since $\mathbb{E}L = 0$, $\mathbb{E}|L| = 2\mathbb{E}[fL] = 2\tau\sum_i \alpha_i\Delta_i(f) \leq 2\tau\|\alpha\|_2\sqrt{D(f)}$. Conversely, given f with $D(f) > 0$, put $\alpha_i = \Delta_i(f)$ and $L = \sum \alpha_i\chi_i$: $\tau D(f) = \mathbb{E}[fL] \leq \mathbb{E}L_+ = \mathbb{E}|L|/2 \leq R(q)\sqrt{D(f)}/2$. □

7.4 Poissonization

Theorem 7.6. [RQ-B tex Theorem 4.1; md Theorem 3] *For every $q \in (0, 1/2]$, with $s = \ln\frac{1}{1-q}$,*

$$R(q)^2 \leq R_{\mathrm{ID}}^2\, \frac{q}{(1-q)\,s}.$$

Proof. Fix $f : \{0,1\}^n \to [0,1]$. Let $N_1, \ldots, N_n$ be i.i.d. Poisson(s) and $x_i = 1\{N_i \geq 1\}$; the x_i are i.i.d. Bernoulli$(1-e^{-s})$ = Bernoulli(q). Put $F(N) = f(x(N)) \in [0,1]$. For $N \sim$ Poisson(s) and bounded g, $\mathbb{E}[(N-s)g(N)] = s\mathbb{E}[g(N+1) - g(N)]$; applying this to N_i conditionally on $(N_j)_{j\neq i}$,

$$\mathbb{E}[F(N)(N_i - s)] = s\,\mathbb{E}[F(N + e_i) - F(N)].$$

Now $x(N + e_i)$ is $x(N)$ with coordinate i set to 1. Hence $F(N+e_i) - F(N) = 0$ if $N_i \geq 1$, and $= f(x^{i\leftarrow 1}) - f(x^{i\leftarrow 0})$ if $N_i = 0$, an event of probability $e^{-s} = 1-q$ independent of $(x_j)_{j\neq i}$. Therefore $\mathbb{E}[F(N+e_i) - F(N)] = (1-q)\Delta_i(f)$. Let $I = \sum_i \Delta_i(f)(N_i - s)$; this is Z_K up to scaling, with $\mathbb{E}I = 0$ and $\mathbb{E}I^2 = sD(f)$, so $\mathbb{E}|I| \leq R_{\mathrm{ID}}\sqrt{sD(f)}$. Using $0 \leq F \leq 1$,

$$s(1-q)D(f) = \mathbb{E}[FI] \leq \mathbb{E}I_+ = \tfrac{1}{2}\mathbb{E}|I| \leq \tfrac{1}{2}R_{\mathrm{ID}}\sqrt{sD(f)}.$$

Thus $D(f) \leq R_{\mathrm{ID}}^2/(4s(1-q)^2)$, and Lemma 7.5 gives $R(q)^2 \leq 4q(1-q)R_{\mathrm{ID}}^2/(4s(1-q)^2)$. □

Remark 7.7. [RQ-B tex Remark 4.2; md Remark 3.2] Since $s > q$, this improves the convex-order bound $R(q) \leq R_{\mathrm{ID}}/\sqrt{1-q}$.

Remark 7.8 (Atomic Poisson inequality). [RQ-B tex Remark 4.3; md Remark 3.3] The proof only tests F against sums of i.i.d. Poisson(s) variables. Let $A(s) = \max_{k\ge 1} \mathbb{E}|N_{ks} - ks|/\sqrt{ks}$ ($N_\lambda \sim$ Poisson(λ)) and consider

$$\mathrm{APC}(s): \qquad \mathbb{E}\Big|\sum_i g_i(N_i - s)\Big| \le A(s)\sqrt{s\textstyle\sum_i g_i^2} \quad (N_i \text{ i.i.d. Poisson}(s),\ g \in \mathbb{R}^n).$$

The same proof gives $R(q)^2 \le qA(s)^2/((1-q)s)$ under APC(s).

Values of $A(s)$. For $N \sim$ Poisson(λ) and $m = \lfloor\lambda\rfloor$, $\mathbb{E}(\lambda - N)_+ = \lambda \Pr(N \le m) - \lambda \Pr(N \le m-1) = \lambda \Pr(N = m)$, so

$$\mathbb{E}|N_\lambda - \lambda|/\sqrt{\lambda} = f_m(\lambda) := 2\lambda^{m+1/2}e^{-\lambda}/m! \qquad (m \le \lambda < m+1),$$

continuous at the integers. As $(\ln f_m)' = (m+\frac12)/\lambda - 1$, the maximum of f_m on $[m, m+1)$ is at $\lambda = x := m + \frac12$, with value $r_m = 2x^x e^{-x}/m!$. We claim $r_{m+1} < r_m$ for $m \ge 1$. Since $r_{m+1}/r_m = (x+1)(1+1/x)^x/(e(x+\frac12))$, the claim reads $x\ln(1+1/x) < 1 + \ln(1-y)$ with $y = 1/(2x+2) \in (0, \frac15]$. The Padé bound $\ln(1+t) \le t(6+t)/(6+4t)$ for $t \ge 0$ (the difference vanishes at $t=0$ and has derivative $4t^3/((6+4t)^2(1+t)) \ge 0$) gives, with $t = 1/x$, $x\ln(1+1/x) \le 1 - 3/(6x+4) = 1 - y/(1-\frac23 y)$; and $g(y) = \ln(1-y) + y/(1-\frac23 y) > 0$ for $0 < y < \frac34$, because $g(0) = 0$ and $g'(y) = \frac{y}{3}(1-\frac43 y)/((1-y)(1-\frac23 y)^2) > 0$. Hence for $\lambda \ge 1$ the ratio is at most $r_1 = 2(3/2)^{3/2}e^{-3/2} = 0.819833 < 0.82$. For $\lambda < 1$ it equals $2\sqrt{\lambda}e^{-\lambda}$, which is unimodal with peak at $\lambda = \frac12$ and exceeds 0.82 at $\lambda = 0.32$ (0.82154) and $\lambda = 0.74$ (0.82086), hence on $[0.32, 0.74]$. (The four constants are checked in interval arithmetic, and the three derivative identities symbolically, by `numerics/remark33_check.py`.)

If $s \le 0.42$, some multiple ks lies in $[0.32, 0.74]$ (an interval of length 0.42), so the maximum defining $A(s)$ is attained with $ks < 1$, and with $e^{-ks} = (1-q)^k$, $qA(s)^2/((1-q)s) = \max_{k:\, ks<1} 4kq(1-q)^{2k-1} \le M(q)^2$. Since $s(q) \le 0.42$ iff $q \le 1 - e^{-0.42} = 0.34295$, *APC($s(q)$) implies C0 at q for every $q \le 0.3429$*, which contains the regime $q < q_0$.[1] Numerically APC holds (`numerics/apc_test.py`: $n \le 6$, $s \in \{0.15, \dots, 0.35\}$; ascent converges to equal coefficients, with value $A(s)$ to 10^{-15}).

Theorem 7.9 (configuration-wise Poissonization; a q-free condition, uniform in k)**.** [RQ-B tex Theorem 4.4; md Theorem 3.4] *Let $q \in (0, 1/2]$, $s = s(q)$, and g, $C(q)$ as in* (7.1). *For $f : \{0,1\}^n \to [0,1]$ with $D(f) > 0$ let $\beta = \Delta(f)/\sqrt{D(f)}$ (a unit vector) and*

$$K_f = \sum_{i:\, \beta_i \ne 0} \beta_i^2\, \delta_{\beta_i/\sqrt{s}},$$

a probability measure on $\mathbb{R}\setminus\{0\}$. For $\theta > 0$ and a measure K put $\lambda_+(K) = \int_{[\theta,\infty)} x^{-2}K(dx)$ and $\lambda_-(K) = \int_{(-\infty,-\theta]} x^{-2}K(dx)$ (the expected numbers of jumps of Z_K of size $\ge\theta$, resp. $\le -\theta$).

(a) $2\tau\sqrt{D(f)} \le \sqrt{q/((1-q)s)}\ \mathbb{E}|Z_{K_f}|$.

(b) $\lambda_\pm(K_f) = s\,k_\pm$ *with the integers* $k_\pm = \#\{i : \pm\beta_i \ge \theta\sqrt{s}\}$, *and for every integer* $k \ge 1$, $\sqrt{q/((1-q)s)}\, g(ks) = T_k(q) = 2\sqrt{kq}(1-q)^{k-1/2}$ *(and $g(0) = 0$).*

[1] Editorial note. Here $q_0 = 1 - 1/\sqrt{2}$, which is q_2 in the notation of this document. RQ-B's `.tex` uses q_0 without defining it; its `.md` uses q0 for this value.

(c) If for every f (it suffices: for a maximiser f_n^* of D over functions of n bits, for every n) there is $\theta = \theta(f) > 0$ with

$$\mathbb{E}|Z_{K_f}| \le \max\big(g(\lambda_+(K_f)),\, g(\lambda_-(K_f)),\, C(q)\big) \tag{7.2}$$

($\lambda_\pm$ taken at $\theta(f)$), then $R(q) = M(q)$.

(d) (RQ-A's q-free formulation.) For $C > 0$ let $\mathrm{ID}^*(C)$ be the statement: for every finitely supported probability measure K on $\mathbb{R}\setminus\{0\}$ there is $\theta = \theta(K) > 0$ with

$$\mathbb{E}|Z_K| \le \max\big(g(\lambda_+(K)),\, g(\lambda_-(K)),\, C\big) \qquad (\lambda_\pm \text{ taken at } \theta(K)),$$

*and let (ID-θ, C) be the stronger statement with one θ for all K. If $\mathrm{ID}^*(C)$ holds, then $R(q) = M(q)$ for every $q \in (0, 1/2]$ with $C(q) \ge C$. For $K \ge 2$, $\min_{0<q\le q_K} C(q) = C_K := \sqrt{2/e}/(1+E_{K-1})$, attained at q_K; so $\mathrm{ID}^*(C_K)$ gives $R = M$ on $(0, q_K]$. In interval arithmetic $C_4 = 0.85334356\ldots$, $C_5 = 0.85510045\ldots$, $C_6 = 0.85598448\ldots$, i.e. $\sqrt{2/e} - C_K = 0.0044203$, 0.0026634, 0.0017794 (**numerics/uniform_k_constants.py**). A decimal C may replace C_K only if $C \le C_K$ (e.g. 0.8533435, 0.855100, 0.855984).*

(e) $\mathrm{ID}^*(C)$ with $C \le \sqrt{2/e}$ implies C5.

Proof. (a) This is the proof of Theorem 7.6 for the given f. With N_i i.i.d. Poisson(s) and $F = f(x(N))$, $I = \sum_i \Delta_i(f)(N_i - s)$ satisfies $\mathbb{E}I^2 = sD(f)$ and $s(1-q)D(f) = \mathbb{E}[FI] \le \mathbb{E}I_+ = \mathbb{E}|I|/2$. The variable $I/\sqrt{sD(f)} = \sum_i c_i(N_i - s)$, $c_i = \beta_i/\sqrt{s}$, is compensated compound Poisson; $c(N-s)$ with $N \sim$ Poisson(s) has Kolmogorov measure $sc^2\delta_c$, so $I/\sqrt{sD(f)}$ has Kolmogorov measure $\sum_i sc_i^2\delta_{c_i} = K_f$ (indices with $\beta_i = 0$ contribute nothing), i.e. it has the law of Z_{K_f}. Hence $\sqrt{D(f)} \le \mathbb{E}|Z_{K_f}|/(2(1-q)\sqrt{s})$ and $2\tau\sqrt{D(f)} \le \tau\mathbb{E}|Z_{K_f}|/((1-q)\sqrt{s}) = \sqrt{q/((1-q)s)}\,\mathbb{E}|Z_{K_f}|$.

(b) The atom of index i sits at $\beta_i/\sqrt{s}$ with mass β_i^2, so it contributes $(s/\beta_i^2)\beta_i^2 = s$ to λ_+ iff $\beta_i/\sqrt{s} \ge \theta$ (to λ_- iff $\beta_i/\sqrt{s} \le -\theta$). And $\sqrt{q/((1-q)s)} \cdot 2\sqrt{ks}\, e^{-ks} = 2\sqrt{kq}(1-q)^k/\sqrt{1-q}$ since $e^{-s} = 1-q$.

(c) By (a), (b) and (7.2), $2\tau\sqrt{D(f)} \le \max(T_{k_+}(q), T_{k_-}(q), M(q)) = M(q)$, with $T_0 := 0$ and $T_k \le M$ by the definition of M. By Lemma 7.5, $R(q) = 2\tau \sup_f \sqrt{D(f)} \le M(q)$, and $R \ge M$ by Theorem 7.4. For the parenthetical claim: D is continuous on the compact set $[0,1]^{2^n}$, so $R_n := 2\tau \max_f \sqrt{D(f)}$ over n-bit f is attained at some f_n^*, and $R(q) = \sup_n R_n$.

(d) Every K_f is a finitely supported probability measure on $\mathbb{R}\setminus\{0\}$, so $\mathrm{ID}^*(C)$ with $C \le C(q)$ gives (7.2) with $\theta(f) = \theta(K_f)$; (b) holds for every θ, so the proof of (c) applies. For the minimum: $C(q) = \sqrt{2/e}\, M(q)/B(q)$ by (7.1) and the definition of B; by Proposition 7.11, on $(0, q_K]$, the union of the bands $[q_{k+1}, q_k]$, $k \ge K$, the maximum of $B/M - 1$ is $\max_{k\ge K-1} E_k = E_{K-1}$, attained at q_K (E_k decreases). So $C(q) \ge C_K$ on $(0, q_K]$, with equality at q_K.

(e) $g \le g(\frac{1}{2}) = \sqrt{2/e}$, so $\mathrm{ID}^*(C)$ gives $\mathbb{E}|Z_K| \le \sqrt{2/e}$ for every compensated compound Poisson law with finitely many atoms. These laws are weakly dense among the mean-zero, variance-one ID laws, and $\mathbb{E}|Z_K|$ is continuous along weakly convergent K of mass 1 ($\mathbb{E}Z^2 = 1$ gives uniform integrability), so $R_{\mathrm{ID}} \le \sqrt{2/e}$. □

Remark 7.10 (on Theorem 7.9). [RQ-B tex Remark 4.5; md "Remarks on Theorem 3.4"] (1) With $R = M$ on $[q_4, 1-q_4]$ (RQ-A, Theorems 1–4, audited) and $R(q) = R(1-q)$, $\mathrm{ID}^*(C_4)$ *implies Conjecture S for every* $q \in (0,1)$; with RQ-A's $k = 4$ (resp. $k = 4, 5$) covers, $\mathrm{ID}^*(C_5)$ (resp. $\mathrm{ID}^*(C_6)$) suffices. All k enter only through the quantisation $\lambda_\pm \in s\mathbb{Z}$. The one-$\theta$ form (ID-θ, C) is false for every $\theta > \theta_{\max}(\eta)$ (RQ-C's C16; $\theta_{\max} = 0.9594$ for C_4), while $\mathrm{ID}^*(C)$ survives those examples. (2) (ID-θ, C) is tight along the Dirac family: for $a \ge \max(\theta, 1)$, $\mathbb{E}|Z_{\delta_a}| = g(1/a^2) = g(\lambda_+(\delta_a))$ (Remark 7.8 with $\lambda =$

$1/a^2 \le 1$). So it must be proved exactly near every δ_a with $g(1/a^2)$ close to C; away from the Dirac family it is C5 with the margin $\sqrt{2/e}-C$. Since $g(x) \ge C_4$ iff $x \in [3s(q_4), 4s(q_4)] = [0.4315, 0.5754]$, the exact part concerns δ_a, $a \in [a_4, b_4] = [1/\sqrt{4s(q_4)}, 1/\sqrt{3s(q_4)}] = [1.3183436, 1.5222920]$, and their reflections. (3) $\theta \le a_4 = 1/\sqrt{4s(q_4)} = 1.3183436$ is necessary for (ID-θ, C_4): for $a < \theta$, $\lambda_\pm(\delta_a) = 0$ while $\mathbb{E}|Z_{\delta_a}| = g(1/a^2) > C_4$ for $a \in (a_4, b_4)$. For $\theta \le 1$ the Diracs below θ are harmless: $\mathbb{E}|Z_{\delta_a}| \le r_1 < C_4$ for $a < 1$. (4) Status: (a)–(e) are proved; ID$^*(C)$ itself is open (it contains C5).[2] Remark 9.7 and Section 11 of RQ-B's paper[3] record why moment-cell certificates cannot supply the part away from the Dirac family.

[Not reproduced here: RQ-B tex Section 5 (Theorem 5.1, the limit $q \to 0$) and, from Section 6, Theorem 6.1 (exact values conditional on C5) with the numerical paragraph after it.]

7.5 Size of the window

[RQ-B tex Section 6 "Exact values conditional on C5", Proposition 6.2 only]

Proposition 7.11 (size of the window)**.** [RQ-B tex Proposition 6.2; md Proposition 5.1] *$B(q)/M(q) = 1/\max_{k\ge1} g(ks)$ with $g(x) = \sqrt{2ex}\,e^{-x}$. On the band $q \in [1-\sqrt{k/(k+1)}, 1-\sqrt{(k-1)/k}]$ where k is the maximiser of Theorem 7.4, $B/M-1$ vanishes only at q_k^* and is largest at the ends; at the tie $q = 1-\sqrt{k/(k+1)}$ it equals*

$$E_k = \frac{(1+1/k)^{k/2}}{\sqrt{e\,k\ln(1+1/k)}} - 1,$$

and E_k is decreasing in k. Hence $\sup_{0<q\le1-1/\sqrt{2}}(B/M-1) = E_1 = \sqrt{2/(e\ln2)} - 1 = 0.030279$, attained at $q = 1-1/\sqrt{2}$; the supremum over $(0, 1/4]$ is $E_2 = 0.010304$ and over $(0, 1/10]$ it is $E_5 = 0.002079$; $E_k \sim 1/(16k^2)$.

Proof. From the two displays in the proof of Theorem 6.1 of RQ-B's paper,[4] $B/M = (2es)^{-1/2}/\max_k \sqrt{k}e^{-ks} = 1/\max_k g(ks)$. By Theorem 7.4, k maximises $\sqrt{j}e^{-js}$ exactly for $s \in [s_k, s_{k-1}]$ with $s_k = \frac{1}{2}\ln(1+1/k)$ ($s_0 = \infty$). On that band $B/M = 1/g(ks)$, and $\log g(ks) = \frac{1}{2}\log(2eks) - ks$ is strictly concave in s with maximum 0 at $s = 1/(2k)$. So $B/M-1$ is largest at a band end. At $s = s_k$ the maximum is $g(x_k)$, $x_k = ks_k = \frac{k}{2}\ln(1+1/k)$, which gives E_k. Since $k\ln(1+1/k)$ increases to 1, x_k increases to $1/2$, and g increases on $(0, 1/2]$, so E_k decreases. The bands meeting $(0, 1-1/\sqrt{2}]$ are those with $k \ge 2$ (and the endpoint $s = s_1$), whose end values are E_j, $j \ge 1$. The values on $(0, 1/4]$ and $(0, 1/10]$ follow in the same way, since $q = 1/4$ and $q = 1/10$ are interior points of bands 2 and 5 with smaller values there (`numerics/constants_check.out`). □

[2] Editorial note. This is the status in RQ-B's text when it was written. The Claim in the proof of the Main Theorem (page xiii) proves the instance that the chain needs: the inequality with $\theta = \frac{17}{20}$ for every finitely supported probability measure K on $[-\frac{77}{50}, \frac{77}{50}]$.

[3] Editorial note. In the source these are cross-references to the labels `rem:slicelimits` and `sec:fail`, which print as Remark 9.7 and Section 11 of RQ-B's `MAIN_RESULT.tex` (limits of the slicing method; mechanisms that fail). These parts of RQ-B's paper are not reproduced here, and they are not Remark 9.7 or Section 11 of this document. The words "of RQ-B's paper" are editorial.

[4] Editorial note. In the source this is a cross-reference to the label `thm:cond`, which prints as Theorem 6.1 of RQ-B's `MAIN_RESULT.tex` (exact values conditional on C5; md Theorem 5). That theorem is not reproduced. The two displays in its proof are $B(q) = 2\sqrt{q/(1-q)}\max_{\kappa>0}\sqrt{\kappa}e^{-\kappa s}$ and $M(q) = 2\sqrt{q/(1-q)}\max_{k\in\mathbb{N}}\sqrt{k}e^{-ks}$. They hold for every q and do not use C5: the first is the definition of B in Section 7.1, since $\max_{\kappa>0}\sqrt{\kappa}e^{-\kappa s} = (2es)^{-1/2}$ (proof of Theorem 7.4), and the second is (7.1). The words "of RQ-B's paper" are editorial.

[Not reproduced here: RQ-B tex Sections 7–11 and 13–14. Section 12 is Chapter 10.]

7.6 RQ-A's formulation of the reduction: U.1–U.3

Source: RQ-A, `CLAIMS.md`, Section U, the notation paragraph and items U.1–U.3 (file md5 `67c3f27be651b187a3f5889ebcaa7827`; the file states that the text of U.1–U.3 is unchanged since audit A.26). Plain text, transcribed into LaTeX symbol by symbol; the proof of U.1 is set in a proof environment. The status paragraph that opens Section U of the file is replaced by this box.

Audit: A.26 (VALID, NEW, 22 October 16:14 UTC). Its fix f1 to U.3, applied by RQ-A at 16:33 UTC and recorded by RQ-AUD at 16:55 UTC, is contained in this text. Referee: RQ-REF3, link 1 (VALID), which names "Theorem 3.4 (a)–(d) = RQ-A U.1–U.3". Theorem 7.9 above is RQ-B's write-up of the same reduction.

Notation. $q \le 1/2$, $s = \ln(1/(1-q))$, $M(q) = 2\tau \max_k \sqrt{k}\,(1-q)^{k-1}$, $g(l) = 2\sqrt{l}\,e^{-l}$, $C(q) = M(q)\sqrt{(1-q)s/q} = \max_{k\ge1} g(ks) \le g(1/2) = \sqrt{2/e}$. For a Kolmogorov probability measure K on $\mathbb{R}$ (Z_K centred ID with $\mathbb{E}Z_K^2 = 1$, Lévy measure $x^{-2}K(dx)$) and $\theta > 0$: $\lambda_\theta^+(K) = \int_{[\theta,\infty)} x^{-2}\,dK$, $\lambda_\theta^-(K) = \int_{(-\infty,-\theta]} x^{-2}\,dK$. ID$^*(C)$: every finitely supported K has some $\theta > 0$ (allowed to depend on K) with

$$\mathbb{E}|Z_K| \le \max\bigl(g(\lambda_\theta^+(K)),\, g(\lambda_\theta^-(K)),\, C\bigr).$$

U.1 PROVED (reduction; first posted in `NOTES_FOR_TEAM.md`, 15:20 UTC). If ID$^*(C)$ holds, then $R(q) = M(q)$ for every $q \le 1/2$ with $C(q) \ge C$.

Written up by RQ-B as C19 = RQ-B MAIN_RESULT Theorem 3.4 (audit requested by RQ-B), with one θ for all K ("(ID-θ, C)").[5] The proof below is per configuration, so θ may depend on K (ID*); this matters because a fixed θ above $\theta_{\max}(\eta)$ makes the statement false (RQ-C C16: $\theta = 1.0$ fails for $C = C(q_4)$). RQ-A does not file U.1 separately.

Proof of U.1. Fix n and a maximiser α of $\mathbb{E}|L|$, $L = \sum \alpha_i\chi_i$, on the unit sphere of $\mathbb{R}^n$; $R_n = \mathbb{E}|L|$. Let $f = 1\{L > 0\}$, $\Delta_i = \Delta_i(f)$, $D = \sum \Delta_i^2$. Level-one form (RQ-B Lemma 2.1, audited):[6] $R_n = 2\tau\sum \alpha_i\Delta_i \le 2\tau\sqrt{D}$, and with $\beta = \Delta/\sqrt{D}$, $2\tau\sqrt{D} \le \mathbb{E}|\sum \beta_i\chi_i| \le R_n$; so $R_n = 2\tau\sqrt{D}$ (and $\beta = \alpha$). Poissonisation (the proof of RQ-B Theorem 3, audited A.7):[7] N_i i.i.d. Poisson(s), $x_i = 1\{N_i \ge 1\}$ (Bernoulli(q)), $F = f(x(N)) \in [0,1]$, $I = \sum \Delta_i(N_i - s)$; Stein–Chen gives $s(1-q)D = \mathbb{E}[FI] \le \mathbb{E}I_+ = \mathbb{E}|I|/2$. Here $I/\sqrt{sD} = Z_K$ with $K = \sum_i \beta_i^2\delta_{\beta_i/\sqrt{s}}$ (finitely supported, mass 1). Hence $R_n = 2\tau\sqrt{D} \le \sqrt{q/((1-q)s)}\,\mathbb{E}|Z_K|$. For every θ, $\lambda_\theta^+(K) = s\,\#\{i : \beta_i \ge \theta\sqrt{s}\}$ and $\lambda_\theta^-(K) = s\,\#\{i : \beta_i \le -\theta\sqrt{s}\}$ are integer multiples of s, so $g(\lambda_\theta^\pm(K)) \le \max(0, \max_k g(ks)) = C(q)$. By ID$^*(C)$ and $C \le C(q)$: $\mathbb{E}|Z_K| \le C(q)$, so $R_n \le \sqrt{q/((1-q)s)}\,C(q) = M(q)$. Taking sup over n, $R(q) \le M(q)$; $R(q) \ge M(q)$ by equal coefficients. □

[5] Editorial note. RQ-B's Theorem 3.4 (numbering of its `MAIN_RESULT.md`) is Theorem 7.9. RQ-C's claim C16 (audit A.29), cited next, is not reproduced; the chain uses the fixed $\theta = \frac{17}{20}$, which is below $\theta_{\max} = 1.0062780$ for $C = C_5$ (A.40, check J6).

[6] Editorial note. RQ-B's Lemma 2.1 is Lemma 7.5, its Theorem 3 is Theorem 7.6, and "equal coefficients" at the end of the proof is Theorem 7.4.

[7] Editorial note. The audit of RQ-B's Theorem 3 is A.10a (VALID, 22 October, 08:11 UTC). A.7 (06:59 UTC) audited RQ-B's claims C1–C4; its part A.7a is the level-one form, Lemma 7.5 (VALID WITH FIXES at 06:59 UTC for a typo, which RQ-B fixed before A.10a; re-rated VALID on 23 October, 07:48 UTC).

U.2 PROVED (elementary). $\min_{q\in(0,q_K]} C(q)$ is $C(q_K) = g((K-1)s_K)$, $s_K = \frac{1}{2}\ln(K/(K-1))$ (the dips of C are at the q_k, where $g((k-1)s_k) = g(ks_k)$, and $(k-1)s_k = \frac{1}{2}(k-1)\ln(1+1/(k-1))$ increases to $1/2$, where g is increasing). Values (mpmath, 30 digits, truncated): $C(q_4) = 0.8533435684\ldots$, $C(q_5) = 0.8551004554\ldots$, $C(q_6) = 0.8559844891\ldots$, i.e. $\eta_K = \sqrt{2/e} - C(q_K) = 0.0044203164\ldots$, $0.0026634294\ldots$, $0.0017793957\ldots$ for $K = 4, 5, 6$ ($\eta_K \sim \sqrt{2/e}/(16K^2)$ as $K \to \infty$); a margin η used in place of η_K must be $\geq \eta_K$ (e.g. 0.00443, 0.00267, 0.00178). Audited VALID as part of A.26.

U.3 CONDITIONAL corollaries. With MAIN-1..4 (audited): ID$^*(C(q_4))$ implies Conjecture S for all q; any decimal $C \leq 0.8533435$ may be used in place of $C(q_4)$ (C must not exceed $C(q_4)$; the earlier text used 0.853344, which is $C(q_4)$ rounded up and leaves q in $(0.13397376, q_4)$ uncovered: audit A.26, fix f1). With MAIN-5: ID$^*(C(q_5))$ suffices (e.g. $C = 0.855100$). With MAIN-6: ID$^*(C(q_6))$ suffices (e.g. $C = 0.855984$).[8] Remarks: C5 ($\mathbb{E}|Z_K| \leq \sqrt{2/e}$ for all K) is necessary for Conjecture S (RQ-B Theorem 4) and is implied by ID$^*(C)$ for any $C \leq \sqrt{2/e}$. ID* is tight on the Dirac curve ($K = \delta_x$, $x \geq 1$: $\mathbb{E}|Z_K| = g(1/x^2)$), so a proof must treat a band around it separately ("band lemma", RQ-D's T1) from the rest ("far region", C5 with margin η_K, RQ-B's certificates).[9]

[8] Editorial note. MAIN-1..4 are Theorems 1–4 (Chapters 1–4), MAIN-5 is Theorem 5 (Chapter 5) and MAIN-6 is Theorem 6 (Chapter 6). The proof of the Main Theorem uses the case "With MAIN-5": the constant is $C_5 = C(q_5)$, and the inequality is needed only at the measure $\tilde{K}$ of Theorem 8.1(f), with $\theta = \frac{17}{20}$.

[9] Editorial note. RQ-B's Theorem 4 (md numbering) is Theorem 5.1 of RQ-B's `MAIN_RESULT.tex`, which is not reproduced. RQ-D's band lemma is Theorem 9.13; RQ-B's far-region certificates are Chapter 10, and the heavy part of the far region is Theorem 9.16.

Part III

Localisation of maximisers

Chapter 8

Finite-q localisation of maximisers (RQ-C, claim C15)

Source: RQ-C, `CLAIMS.md`, claim C15 (file md5 `4b1e22a4fb96d0a383a1d8f5395edc06`, the version refereed by RQ-REF3). The source is plain text with Unicode mathematics. It is transcribed into LaTeX symbol by symbol: the claim header and the paragraph after it, the notation, the statement (a)–(g) (set as Theorem 8.1), the proof (a)–(g) and the numerical sanity checks. Bold source text is set in bold. Nothing is omitted.

Audit: A.28 (VALID, NEW, 22 October 16:14 UTC, no fix). Referee: RQ-REF3, link 2 (VALID, "by hand; constants re-checked exactly").

Use in the Main Theorem: part (f) with $A = \frac{77}{50}$ and $C = C_5$, and part (g) for $A'(q) \le A'(q_5)$.

> **Claim header in the source.** C15. Finite-q localisation of maximisers (step P0 of the uniform plan): at a maximiser, every jump satisfies $u|\alpha_i| \le \sqrt{2/(1-q)} \cdot (1 + o(1))$, so RQ-A's q-free target (ID-θ) is needed only for K supported in $[-A, A]$, any $A > A'(q) = \sqrt{2q/s}/(1-q)$. PROVED (elementary). **RQ-AUD: VALID, NEW** (A.28, 16:14 UTC, no fix)

This is the finite-q analogue of RQ-B's Lemma 8.2 and Proposition 8.3 (A.13), applied to the finite-q maximiser that RQ-A's reduction (RQ-A NOTES_FOR_TEAM 14:50 item 1 and 15:20; RQ-B Theorem 3 read at the maximiser) Poissonises. RQ-A's 14:50 plan item 4(a) asked for exactly this step.[1]

8.1 Notation

χ_i i.i.d., $\chi_i = u$ with probability q and $-v$ with probability $1-q$, $u = \sqrt{(1-q)/q}$, $v = 1/u$, $\tau = \sqrt{q(1-q)} = qu = (1-q)v$; $s = \ln(1/(1-q))$. For a unit $\alpha \in \mathbb{R}^n$ put $L = \alpha \cdot \chi$. $R_n = \max_{|\alpha|=1} \mathbb{E}|\alpha \cdot \chi|$ (attained), $R = R(q) = \sup_n R_n$; R_n is nondecreasing in n (append a zero coefficient), so $R_n \to R$, and $0 < R \le 1$.

[1] Editorial note. RQ-B's Lemma 8.2 and Proposition 8.3 (numbering of its `MAIN_RESULT.md`; Lemma 9.2 and Proposition 9.3 of its `MAIN_RESULT.tex`) concern maximisers of the infinitely divisible problem; they are not reproduced and not used. RQ-A's reduction is U.1 (Section 7.6), written up as Theorem 7.9(a)–(d); RQ-B's Theorem 3 is Theorem 7.6. The symbols g, Z_K, $\lambda_\pm$ and $M(q)$ below are those of Chapter 7.

8.2 Statement and proof

Theorem 8.1 (C15)**.** *Let $q \in (0,1)$, $n \geq 1$, $|\alpha| = 1$ with $\mathbb{E}|L| = R_n$, and put $\delta = R - R_n \geq 0$, $p_+ = P(L > 0)$, $p_- = P(L < 0)$.*

(a) $P(L = 0) = 0$ (so $p_+ + p_- = 1$), and $\mathbb{E}[\chi_i \operatorname{sgn} L] = R_n \alpha_i$ for every i.

(b) Let $L' = L - \alpha_i \chi_i$. If $\alpha_i > 0$, then $R_n u \alpha_i = 2(1-q)P(-\alpha_i u < L' < \alpha_i v) \leq 2p_-$. If $\alpha_i < 0$, then $R_n u|\alpha_i| = 2(1-q)P(-|\alpha_i| v < L' < |\alpha_i| u) \leq 2p_+$.

(c) For every $a > 0$: $\mathbb{E}[(L+a)^+; L < 0] \leq \delta/(2q) + Ra^2/(4(1-q))$, and $\mathbb{E}[(a-L)^+; L > 0] \leq \delta/(2q) + Ra^2/(4(1-q))$.

(d) $p_-^2 \leq R(R_n + \delta/q)/(2(1-q))$ and $p_+^2 \leq R(R_n + \delta/q)/(2(1-q))$; also $R_n^2 \leq 4p_+p_-$.

(e) Hence $\max_i u|\alpha_i| \leq \Lambda_n := \sqrt{2R(R_n + \delta/q)/(1-q)}\,/R_n$, and $\Lambda_n \to \sqrt{2/(1-q)}$ as $n \to \infty$.

(f) Use in the uniform plan. *Let f^* maximise $|\Delta(f)|$ over $f : \{0,1\}^n \to [0,1]$ and $\alpha^* = \Delta(f^*)/|\Delta(f^*)|$. Then $\mathbb{E}|\alpha^* \cdot \chi| = R_n$, so (a)–(e) apply to α^*, and the measure $\tilde{K} = \sum_i \alpha_i^{*2} \delta_{\alpha_i^*/\sqrt{s}}$ of RQ-A's reduction is supported in $[-\Lambda_n/(u\sqrt{s}), \Lambda_n/(u\sqrt{s})]$, where $\Lambda_n/(u\sqrt{s}) \to A'(q) := \sqrt{2/(1-q)}/(u\sqrt{s}) = \sqrt{2q/s}/(1-q)$. Consequently:* ***if, for some $A > A'(q)$ and some C with $C\sqrt{q/((1-q)s)} \leq M(q)$, every probability measure K on $[-A, A]$ satisfies RQ-A's (ID-θ), $\mathbb{E}|Z_K| \leq \max(g(\lambda_+(K)), g(\lambda_-(K)), C)$, then*** *$R(q) = M(q)$. The same holds for any other bound $\mathbb{E}|Z_K| \leq F(K)$ that is used only at $K = \tilde{K}$: it is needed only for K on $[-A, A]$.*

(g) $A'(q)$ is strictly increasing in q, so one $A > A'(q_K)$ serves every $q \leq q_K$: $A'(q) \to \sqrt{2}$ as $q \to 0$, and $A'(0.05) = 1.46976$, $A'(q_6) = 1.51455$, $A'(0.1) = 1.53085$, $A'(q_5) = 1.53804$, $A'(q_4) = 1.57599$.[2] *The bound is nearly attained: OR_k at $q = q_{k+1}$ (a maximiser there under Conjecture S, tied with OR_{k+1}) has $\tilde{K} = \delta_a$ with $a = 1/\sqrt{ks(q_{k+1})} = \sqrt{2/(k\ln(1+1/k))} = \sqrt{2}(1 + 1/(4k) + O(k^{-2})) > \sqrt{2}$, e.g. $a = 1.49690$ for $k = 4$ against $A'(q_5) = 1.53804$.* ***So a band/far-region split for $q \leq q_K$ must allow atoms beyond $\sqrt{2}$ (RQ-B's Theorem 8.5 uses $A = 99/70 = 1.41429$, which suffices at $q = 0$ by Proposition 8.3 but not at finite q): $A \geq 1.538$ for $q \leq q_5$, $A \geq 1.576$ for $q \leq q_4$.***[3]

Proof. (a) For $|t|$ small, $\varphi(t) := \mathbb{E}|L + t\chi_i| \leq R_n|\alpha + te_i| = R_n(1 + 2t\alpha_i + t^2)^{1/2} =: g(t)$, by maximality and homogeneity, with equality at $t = 0$. Comparing difference quotients (division by $t < 0$ reverses the inequality) gives $\varphi'_+(0) \leq g'(0) \leq \varphi'_-(0)$, while $\varphi'_-(0) \leq \varphi'_+(0)$ by convexity of φ. So $\varphi'_+(0) = \varphi'_-(0) = g'(0) = R_n\alpha_i$. By dominated convergence (difference quotients are bounded by $|\chi_i|$), $\varphi'_\pm(0) = \mathbb{E}[\chi_i \operatorname{sgn} L] \pm \mathbb{E}[|\chi_i|; L = 0]$. Hence $\mathbb{E}[|\chi_i|; L = 0] = 0$, so $P(L = 0) = 0$ as $|\chi_i| \geq \min(u, v) > 0$, and $\mathbb{E}[\chi_i \operatorname{sgn} L] = R_n\alpha_i$.

(b) L' is independent of χ_i and $qu = (1-q)v = \tau$, so $\mathbb{E}[\chi_i \operatorname{sgn} L] = \tau(\mathbb{E}\operatorname{sgn}(L' + \alpha_i u) - \mathbb{E}\operatorname{sgn}(L' - \alpha_i v))$. Let $\alpha_i > 0$. The function $\operatorname{sgn}(x + \alpha_i u) - \operatorname{sgn}(x - \alpha_i v)$ equals 2 on $(-\alpha_i u, \alpha_i v)$, 1 at the two endpoints and 0 elsewhere, and the endpoint events are null: $\{L = 0\} \supseteq \{\chi_i = u, L' =$

[2] Editorial note. In closed form $1 - q_5 = 2/\sqrt{5}$ and $s(q_5) = \frac{1}{2}\ln\frac{5}{4}$, so $A'(q_5) = \sqrt{5q_5/\ln\frac{5}{4}} = 1.538044391650755\ldots < \frac{77}{50}$. RQ-AUD (A.40, check J4, 256-bit Arb) and RQ-REF3 (exactly) checked this inequality.

[3] Editorial note. RQ-AUD, A.40 (sweep of the quoted figures, 23 October 03:30 UTC), a display remark with no fix: these two figures give $A'(q_5) = 1.538044\ldots$ and $A'(q_4) = 1.5759926\ldots$ to three places, the first truncated and the second rounded up. The requirement in (f) is $A > A'(q)$, and the chain uses $A = \frac{77}{50} > A'(q_5)$, which was checked exactly (A.28, A.40, RQ-REF3). RQ-B's Theorem 8.5 (numbering of its `MAIN_RESULT.md`; Theorem 9.6 of its `MAIN_RESULT.tex`) is the bound $R_{\mathrm{ID}} \leq \frac{867}{1000}$; it is not reproduced and not used.

$-\alpha_i u\} \cup \{\chi_i = -v, L' = \alpha_i v\}$, and $P(L=0)=0$ by (a). So $R_n\alpha_i = 2\tau P(-\alpha_i u < L' < \alpha_i v)$; multiply by u ($\tau u = 1-q$). On $\{\chi_i=-v\}$, which is independent of L' and has probability $1-q$, $L = L' - \alpha_i v < 0$ whenever $L' < \alpha_i v$; so $p_- \ge (1-q)P(-\alpha_i u < L' < \alpha_i v)$. For $\alpha_i < 0$ put $b = |\alpha_i|$: the same computation gives $R_n b = 2\tau P(-bv < L' < bu)$, and on $\{\chi_i = -v\}$, $L = L' + bv > 0$ whenever $L' > -bv$, so $p_+ \ge (1-q)P(-bv < L' < bu)$.

(c) Append an independent bit χ with coefficient β: $\mathbb{E}|L+\beta\chi| \le R_{n+1}\sqrt{1+\beta^2} \le R(1+\beta^2/2)$. For $a, b > 0$ and real x, $|x+a|-|x| = a(1-2\cdot 1\{x<0\}) + 2(x+a)^+ 1\{x<0\}$ and $|x-b|-|x| = b(1-2\cdot 1\{x>0\}) + 2(b-x)^+ 1\{x>0\}$. Let $\beta>0$, $a=\beta u$, $b=\beta v$, $H(a) = \mathbb{E}[(L+a)^+; L<0]$, $H^-(b) = \mathbb{E}[(b-L)^+; L>0]$. Using $P(L=0)=0$,

$$\begin{aligned}\mathbb{E}|L+\beta\chi| &= q\mathbb{E}|L+a| + (1-q)\mathbb{E}|L-b| \\ &= R_n + qa(2p_+ - 1) + (1-q)b(1-2p_+) + 2qH(a) + 2(1-q)H^-(b) \\ &= R_n + 2qH(a) + 2(1-q)H^-(b),\end{aligned}$$

as $qa = (1-q)b = \tau\beta$. Dropping $H^-(b) \ge 0$: $2qH(a) \le \delta + R\beta^2/2 = \delta + Rqa^2/(2(1-q))$, which is the first bound. For the second take $\beta < 0$ and $a = |\beta| u$: $\mathbb{E}|L+\beta\chi| = q\mathbb{E}|L-a| + (1-q)\mathbb{E}|L+|\beta|v| = R_n + 2qH^-(a) + 2(1-q)H(|\beta|v)$, and the same estimate.

(d) $\mathbb{E}L = 0$ and $\mathbb{E}|L| = R_n$ give $\mathbb{E}[L^-] = \mathbb{E}[L^+] = R_n/2$.[4] Since $(L+a)^+ \ge L + a$, $H(a) \ge ap_- - R_n/2$, so by (c) $ap_- - Ra^2/(4(1-q)) \le R_n/2 + \delta/(2q)$ for every $a>0$; at $a = 2(1-q)p_-/R$ this reads $(1-q)p_-^2/R \le (R_n + \delta/q)/2$. The bound for p_+ is the same with $H^-(a) \ge ap_+ - R_n/2$. Finally $R_n/2 = \mathbb{E}[L(1\{L>0\} - p_+)] \le (\mathbb{E}L^2)^{1/2}(p_+(1-p_+))^{1/2}$ by Cauchy–Schwarz, with $\mathbb{E}L^2 = 1$.

(e) Combine (b) and (d): $u|\alpha_i| \le 2\max(p_+, p_-)/R_n \le \Lambda_n$. As $n\to\infty$, $R_n \to R > 0$ and $\delta \to 0$, so $\Lambda_n \to \sqrt{2R^2/(1-q)}/R$.

(f) For every f with values in $[0,1]$ and every unit α', level-1 duality $\mathbb{E}[f\chi_i] = \tau\Delta_i(f)$ and $\mathbb{E}[\alpha'\cdot\chi] = 0$ give $\mathbb{E}|\alpha'\cdot\chi| = 2\mathbb{E}[(\alpha'\cdot\chi)^+] \ge 2\mathbb{E}[f\,\alpha'\cdot\chi] = 2\tau\,\alpha'\cdot\Delta(f)$, with equality for $f = 1\{\alpha'\cdot\chi > 0\}$. Hence $R_n = \max_{\alpha'}\mathbb{E}|\alpha'\cdot\chi| \le 2\tau\max_f|\Delta(f)| = 2\tau|\Delta(f^*)| = 2\tau\,\alpha^*\cdot\Delta(f^*) \le \mathbb{E}|\alpha^*\cdot\chi| \le R_n$. The atoms of $\tilde K$ are $\alpha_i^*/\sqrt{s}$ with $|\alpha_i^*| \le \Lambda_n/u$ by (e). For the implication: suppose $R > M(q)$. Since $R_n \to R$ and $\Lambda_n/(u\sqrt{s}) \to A'(q) < A$, there is n with $R_n > M(q)$ and $\operatorname{supp}\tilde K \subset [-A, A]$. RQ-A's reduction uses (ID-θ) only at $K = \tilde K$: $R_n \le \mathbb{E}|Z_{\tilde K}|\sqrt{q/((1-q)s)} \le \max(g(\lambda_+), g(\lambda_-), C)\sqrt{q/((1-q)s)} \le M(q)$, since $\lambda_\pm(\tilde K) = s\cdot\#\{i : \pm\alpha_i^* \ge \theta\sqrt{s}\}$ and $g(ks)\sqrt{q/((1-q)s)} = T_k(q) \le M(q)$. This contradicts $R_n > M(q)$.[5]

(g) $\frac{d}{dq}\ln(A'(q)^2) = 1/q - 1/((1-q)s) + 2/(1-q)$, which is positive iff $s(1+q) > q$; this holds because $s > q$. The OR_k atom: $\alpha = \mathbf{1}_k/\sqrt{k}$, so $\tilde K = \delta_{1/\sqrt{ks}}$, and $s(q_{k+1}) = \frac{1}{2}\ln(1+1/k)$. The numbers are evaluations of these closed forms. □

Sanity checks (NUMERICAL, float; `numerics/explore/p0_check.py`, output `p0_check.out`). The expansion in (c), including the term $2\tau\beta P(L=0)$ that appears when $P(L=0) > 0$, matches exact enumeration to $1.8\cdot10^{-15}$ on 200 random cases ($n \le 8$, $q \in [0.02, 0.45]$). At OR_k (the conjectured maximiser, $k = \lfloor 1/(q(2-q))\rfloor$) for $q \in \{0.3, 0.2, 0.15, 0.12, 0.1, 0.07, 0.05\}$: the identity in (b) holds to $7\cdot10^{-16}$; $p_-^2/(R^2/(2(1-q))) \in [0.80, 0.91]$, so (d) is nearly tight there; and $u\alpha_i = u/\sqrt{k}$ equals the first bound in (b), $2p_-/R_n$, exactly ($p_- = (1-q)^k$, $R_n = 2\tau\sqrt{k}(1-q)^{k-1}$).

[4] Editorial note. Here $L^- = \max(-L, 0)$ and $L^+ = \max(L, 0)$; in Chapter 1, x^- denotes $\min(x, 0)$.

[5] Editorial note. The first inequality of the last display is Theorem 7.9(a) (equivalently, the Poissonisation step of U.1) at $f = f^*$, for which $2\tau\sqrt{D(f^*)} = 2\tau|\Delta(f^*)| = R_n$ by the display before; the identities for $\lambda_\pm$ and $g(ks)$ are Theorem 7.9(b).

Part IV

The band and the heavy far region

Chapter 9

Flip formula, a comparison lemma for stop-loss terms, the band lemma near the Dirac curve, and the heavy part of the far region

(RQ-D)

Source: RQ-D, `MAIN_RESULT.tex` (md5 `ac0ecf4ff81feba53f6b8d8567a35a3b`), "RQ-D: flip formula, a comparison lemma for stop-loss terms, the band lemma near the Dirac curve, and the heavy part of the far region", by "RQ-D". The title page of the source adds "Draft — the status of every statement is in `CLAIMS.md`" and is dated by LaTeX's `\today`.

Refereed version: md5 `212c6f230b7bd8b8ef0c377b21f7c937`, the file RQ-REF3 refereed (Sections 1–7, that is, the whole paper). The source differs from it in two figures of Section 9.6.1, neither of them in a statement or a proof: one in the remark on the slope check (A.34's finding f1) and one in the paragraph on the controls. RQ-D corrected both at 05:35–05:36 UTC on 23 October. RQ-AUD checked the corrections at 06:58 UTC (A.34 addendum, check a34i) and wrote that this file "is the refereed 212c6f23… with the two corrected figures, so it is the version to quote in FULL_PROOF.pdf".

Audits: A.30 (Lemmas 9.1 and 9.3, claims D1–D2; VALID, Lemma 9.3 after fix f1, 22 October 17:23 UTC); A.32 (Lemmas 9.2, 9.4, 9.6–9.8, Proposition 9.9, Theorem 9.10, Corollary 9.11; VALID, 18:17 UTC); A.34 (Lemma 9.7(c), the options (O1)–(O5), Lemma 9.12, Theorem 9.13, Corollaries 9.14 and 9.15; VALID, 20:19 UTC; addendum of 23 October 03:02 UTC: finding f1, a slip in a remark of Section 9.6.1, text only; addendum of 04:51 UTC: the box-level record of the run for Theorem 9.13 replayed leaf by leaf, VALID; addenda of 06:58 and 07:48 UTC: RQ-D's text corrections checked, nothing open); A.38 (Lemmas 9.18–9.24, Theorem 9.16, Corollary 9.17; VALID, 22:51 UTC; its remark r3 settled at 23:25 UTC in this file). No fix to the mathematics except A.30's f1, which this file contains.

Referee: RQ-REF3, link 3, VALID: every lemma checked by hand; the certificates of Theorem 9.16 re-verified, and the computation of Theorem 9.13 re-done from scratch with RQ-REF3's own exact cover, every square certified. Report `REFEREE.md`, md5 `6ac713c05dd3a1b74e71d5c959ac0ceb`, FINAL, 03:09 UTC on 23 October.

Use in the Main Theorem: Step 4. Theorem 9.13 for $V_+ \geq \frac{4}{5}$ or $V_- \geq \frac{4}{5}$, and Theorem 9.16 for $\frac{1}{2} \leq V_\pm < \frac{4}{5}$; Corollaries 9.14 and 9.17 state the reductions. Theorem 9.10 and Corollaries 9.11 and 9.15 (the statements about C5) are not used by the chain.

Transcription: the whole paper, with the mechanical changes of Appendix C: labels prefixed by `ch09:`; Section n, item n and equation (n) become Section 9.n, item 9.n and $(9.n)$; the title becomes the chapter title; the abstract as a quoted block. Three editorial footnotes, all in Section 9.6.1: RQ-REF3's second robustness remark with its resolution (first paragraph, at the list of the run's output files), and the two corrected figures (the remark on the slope check, and the paragraph on the controls).

Abstract of the source paper. For the centred infinitely divisible laws Z_K (Kolmogorov measure K, $\mathbb{E}Z_K^2 = K(\mathbb{R}) = 1$) we prove $\mathbb{E}|Z_K| \leq \sqrt{2/e}$ on the band $\{K([1,\sqrt{2}]) \geq 9/10\} \cup \{K([-\sqrt{2},-1]) \geq 9/10\}$ of probability measures on $[-\sqrt{2},\sqrt{2}]$ (Theorem 9.10); by the audited support bound for maximisers this reduces C5 ($\sup_K \mathbb{E}|Z_K| = \sqrt{2/e}$) to the complementary far region (Corollary 9.11). In the form needed at finite q (the q-free condition ID* of the audited reduction, with $C_5 = g(2\ln\frac{5}{4})$) we prove the band lemma with $\theta = 0.85$, $A = 1.54$: $\mathbb{E}|Z_K| \leq \max(g(\lambda^+_{0.85}(K)), C_5)$ for every finitely supported probability K on $[-1.54, 1.54]$ with $K([0.85, 1.54]) \geq 4/5$, and the mirror statement (Theorem 9.13). So ID*, and with it Conjecture S for all q, reduces to $\mathbb{E}|Z_K| \leq C_5$ on the far region $\{K([0.85,1.54]) < 4/5,\ K([-1.54,-0.85]) < 4/5\}$ (Corollary 9.14). The proof of the band lemmas is not a moment argument: an exact identity (Lemma 9.3) isolates the extremal Poisson part, the residual enters only through two stop-loss terms, and these are bounded by a new comparison lemma (Lemma 9.4: pushing jumps to the right increases $\mathbb{E}\psi(Z_K)$ whenever ψ'' is nondecreasing) together with convexity bounds in the jump law. The final inequalities on four-parameter domains are checked in ball arithmetic. Sections 9.2–9.4 are written for a general threshold θ and support bound A, since the same tools are used for the finite-q band (Section 9.6). On the heavy part of that far

region, $\{\frac{1}{2} \le K([0.85, 1.54]) < \frac{4}{5}\}$ and its mirror, we prove $\mathbb{E}|Z_K| < C_5$ (Theorem 9.16). The positive edge is replaced by its chord law (a convex-order increase) and fixed on boxes of the two chord rates. The rest enters through a certified degree-16 moment bound (polynomial majorant, Lagrangian relaxation on cumulant cells). So ID* and C5 reduce to the light part $\{K([0.85, 1.54]) < \frac{1}{2},\ K([-1.54, -0.85]) < \frac{1}{2}\}$ (Corollary 9.17).

9.1 Setting

For $q \in (0,1)$ let $\chi_1, \chi_2, \dots$ be i.i.d. with $\mathbb{P}(\chi = \sqrt{(1-q)/q}) = q$ and $\mathbb{P}(\chi = -\sqrt{q/(1-q)}) = 1-q$, and $R(q) = \sup_{\alpha \neq 0} \mathbb{E}|\sum_i \alpha_i \chi_i| / \|\alpha\|_2$. Conjecture S: $R(q) = M(q) := 2\sqrt{q(1-q)} \max_{k \ge 1} \sqrt{k}\, \hat{q}^{\,k-1}$, $\hat{q} = \max(q, 1-q)$.

A *Kolmogorov measure* is a finite Borel measure K on $\mathbb{R}$; Z_K denotes the centred infinitely divisible random variable with

$$\log \mathbb{E} e^{itZ_K} = \int_{\mathbb{R}} \frac{e^{itx} - 1 - itx}{x^2}\, K(dx) \qquad \text{(the integrand is } -t^2/2 \text{ at } x = 0),$$

so $\mathbb{E}Z_K = 0$, $\mathbb{E}Z_K^2 = K(\mathbb{R})$, $K(\{0\})$ is the Gaussian variance and $x^{-2}K(dx)$ on $\mathbb{R} \setminus \{0\}$ is the Lévy measure. $Z_{K_1+K_2} \overset{d}{=} Z_{K_1} + Z_{K_2}$ with independent summands. For a finitely supported K,

$$Z_K = \sqrt{K(\{0\})}\, G + \sum_{x \in \operatorname{supp} K \setminus \{0\}} x\big(N_x - K(\{x\})/x^2\big),$$

with $G \sim N(0,1)$ and independent $N_x \sim \text{Poisson}(K(\{x\})/x^2)$. Throughout, N_λ denotes a Poisson(λ) variable ($N_0 = 0$) and G a standard Gaussian, independent of each other and of everything else. We write $g(\lambda) = 2\sqrt{\lambda}\, e^{-\lambda}$; $g(1/x^2) = \mathbb{E}|Z_{\delta_x}|$ for $x \ge 1$, and $\max g = g(1/2) = \sqrt{2/e}$. C5 is the statement $\mathbb{E}|Z_K| \le \sqrt{2/e}\, K(\mathbb{R})^{1/2}$ for all K.

9.2 Exact identities

Lemma 9.1 (flip formula)**.** *For $y \neq 0$ and $w \in \mathbb{R}$, $|y+w| = |y| + \operatorname{sgn}(y)\, w + 2\big(-\operatorname{sgn}(y)\, w - |y|\big)_+$. Consequently, if Y and W are independent, $\mathbb{E}|Y| + \mathbb{E}|W| < \infty$, $\mathbb{E}W = 0$ and $\mathbb{P}(Y = 0) = 0$, then $\mathbb{E}|Y+W| = \mathbb{E}|Y| + 2\,\mathbb{E}\big[(-\operatorname{sgn}(Y)\, W - |Y|)_+\big]$.*

Proof. Let $s = \operatorname{sgn}(y)$, so $y + w = s(|y| + sw)$. If $|y| + sw \ge 0$ then $|y+w| = |y| + sw$ and $(-sw - |y|)_+ = 0$. If $|y| + sw < 0$ then $|y+w| = -|y| - sw = |y| + sw + 2(-sw - |y|)$. Take expectations; $\mathbb{E}[\operatorname{sgn}(Y) W] = \mathbb{E}\operatorname{sgn}(Y)\, \mathbb{E}W = 0$. □

Lemma 9.2 (conditional form)**.** *Let Y, W be independent and integrable with $\mathbb{E}W = 0$, $\mathbb{E}W^2 = \rho^2 < \infty$, and put $\ell(y) = \mathbb{E}|y + W|$. Then $\mathbb{E}|Y+W| = \mathbb{E}\,\ell(Y)$; ℓ is convex and 1-Lipschitz; for every real y*

$$\ell(y) = y + 2\mathbb{E}(-W - y)_+ = -y + 2\mathbb{E}(W + y)_+, \qquad |y| \le \ell(y) \le \sqrt{y^2 + \rho^2}.$$

Proof. Fubini gives $\mathbb{E}|Y+W| = \mathbb{E}\ell(Y)$; convexity and the Lipschitz bound are inherited from $|\cdot|$. The two identities are $|x| = x + 2(-x)_+ = -x + 2x_+$ with $x = y + W$, together with $\mathbb{E}W = 0$. Jensen gives $\ell(y) \ge |y|$ and Cauchy–Schwarz $\ell(y) \le (\mathbb{E}(y+W)^2)^{1/2}$. □

Lemma 9.3 (OR-region identity with a residual)**.** *Let $K = K_S + K_R$ with $K_S \neq 0$ and K_R finite measures, K_S carried by $[\theta, \infty)$ for some $\theta > 0$, and put $\Lambda = \int x^{-2} dK_S$, $m = \int x^{-1} dK_S$, $V = K_S(\mathbb{R})$. Let $Y = Z_{K_S}$ and $W = Z_{K_R}$ be independent and N_S the number of jumps of Y. Then*

$Y = S_{N_S} - m$, where $N_S \sim \mathrm{Poisson}(\Lambda)$ and, given $N_S = n$, $S_n = J_1 + \cdots + J_n$ with J_i i.i.d. of law ν_S/Λ, $\nu_S(dx) = x^{-2}K_S(dx)$, carried by $[\theta, \infty)$. If moreover $\theta > m$ (every jump exceeds the compensator), then

$$\mathbb{E}|Z_K| = 2me^{-\Lambda} + 2e^{-\Lambda}\,\mathbb{E}(W - m)_+ + 2\,\mathbb{E}\big[(-W - Y)_+;\, N_S \geq 1\big],$$

and $2me^{-\Lambda} \leq \sqrt{V}\, g(\Lambda) \leq \sqrt{2/e}\,\sqrt{V}$, with equality in the first inequality iff K_S is a single atom, and in both iff $K_S = V\delta_{\sqrt{2V}}$.

Proof. ν_S is carried by $[\theta, \infty)$ and has mass $\Lambda \leq \theta^{-2}V < \infty$, so Y is compound Poisson with rate Λ, jump law ν_S/Λ and compensator $\int x\,\nu_S(dx) = m$. On $\{N_S = 0\}$, $Y = -m < 0$; on $\{N_S \geq 1\}$, $Y \geq \theta - m > 0$. Hence $\mathbb{P}(Y = 0) = 0$ (here $K_S \neq 0$ is used: $m > 0$) and, as $\mathbb{E}Y = 0$, $\mathbb{E}|Y| = 2\mathbb{E}Y_- = 2me^{-\Lambda}$. Lemma 9.1 with the independence of W and (Y, N_S) gives the identity. Cauchy–Schwarz gives $m^2 \leq \Lambda V$, with equality iff x^{-1} is K_S-a.e. constant, so $2me^{-\Lambda} \leq \sqrt{V}g(\Lambda)$; and $g \leq g(1/2) = \sqrt{2/e}$ with equality iff $\Lambda = 1/2$. A single atom $V\delta_x$ has $\Lambda = V/x^2$, which is $1/2$ iff $x = \sqrt{2V}$. □

9.3 A comparison lemma for stop-loss terms

For a function ψ and $x \in \mathbb{R}$ put $D_x\psi(z) = \int_0^1 (1-u)\,\psi''(z + ux)\,du$; for $x \neq 0$ this is $(\psi(z+x) - \psi(z) - x\psi'(z))/x^2$, and $D_0\psi = \psi''/2$.

Lemma 9.4 (comparison)**.** *Let $\psi : \mathbb{R} \to \mathbb{R}$ be C^1 with ψ' absolutely continuous and ψ'' nondecreasing and bounded. Let K be a finitely supported Kolmogorov measure and $T : \mathbb{R} \to \mathbb{R}$ a map with $T(x) \geq x$ on $\operatorname{supp} K$. Then $\mathbb{E}\psi(Z_K) \leq \mathbb{E}\psi(Z_{T_\# K})$.*

Proof. Step 1 (smooth ψ). Assume first $\psi \in C^2$ with ψ'' nondecreasing and $|\psi''| \leq M$. For a finitely supported Kolmogorov measure $L = \sigma^2\delta_0 + \sum_j w_j\delta_{x_j}$ ($x_j \neq 0$) and a square-integrable X independent of the Z's, put $\Phi(s) = \mathbb{E}\psi(X + Z_{sL})$, $s \geq 0$. Since $Z_{(s+\delta)L} \overset{d}{=} Z_{sL} + Y_\delta$ with $Y_\delta = Z_{\delta L}$ independent and $\mathbb{E}Y_\delta = 0$, Taylor's formula with integral remainder gives

$$\Phi(s+\delta) - \Phi(s) = \mathbb{E}\Big[Y_\delta^2 \int_0^1 (1-u)\,\psi''(X' + uY_\delta)\,du\Big], \qquad X' = X + Z_{sL}.$$

Write $Y_\delta = \sigma\sqrt{\delta}\,G - \delta c + \sum_j x_j N^{(j)}_{\delta\lambda_j}$ with $\lambda_j = w_j/x_j^2$, $c = \sum_j x_j\lambda_j$. On the event of no jump (probability $1 - \delta\sum\lambda_j + O(\delta^2)$) the contribution is $\delta\sigma^2\,\mathbb{E}\psi''(X')/2 + o(\delta)$, by bounded convergence and continuity of ψ''; on the event of exactly one jump, of size x_j (probability $\delta\lambda_j + O(\delta^2)$), it is $\delta\lambda_j x_j^2\,\mathbb{E}D_{x_j}\psi(X') + o(\delta)$; on the event E_2 of two or more jumps the integrand is at most $\frac{M}{2}Y_\delta^2$ and $\mathbb{E}[Y_\delta^2; E_2] \leq 3\big(\sigma^2\delta\,\mathbb{P}(E_2) + \delta^2c^2 + \mathbb{E}[(\sum_j |x_j| N^{(j)}_{\delta\lambda_j})^2; E_2]\big) = O(\delta^2)$ (Poisson moments). Hence Φ has the right derivative $\mathbb{E}\,(\mathcal{G}_L\psi)(X + Z_{sL})$ with $\mathcal{G}_L\psi = \sum_{x \in \operatorname{supp} L} L(\{x\})D_x\psi$, which is continuous in s (bounded continuous integrand, weakly continuous law), so $\Phi \in C^1$. Now let $K' = T_\# K$ and $\Psi(t) = \mathbb{E}\psi(Z_{(1-t)K} + Z'_{tK'})$ with independent summands, $t \in [0,1]$. Applying the above in each variable (the two partial derivatives are jointly continuous, for the same reason),

$$\Psi'(t) = \mathbb{E}\big[(\mathcal{G}_{K'}\psi - \mathcal{G}_K\psi)(Z_{(1-t)K} + Z'_{tK'})\big],$$
$$(\mathcal{G}_{K'}\psi - \mathcal{G}_K\psi)(z) = \sum_{x \in \operatorname{supp} K} K(\{x\})\big(D_{T(x)}\psi(z) - D_x\psi(z)\big) \geq 0,$$

because $y \mapsto D_y\psi(z) = \int_0^1 (1-u)\psi''(z+uy)du$ is nondecreasing when ψ'' is. So $\Psi(1) \geq \Psi(0)$.

Step 2 (general ψ). Let ϕ_ε be a smooth probability density supported in $[-\varepsilon, \varepsilon]$ and $\psi_\varepsilon = \psi * \phi_\varepsilon$. Then $\psi_\varepsilon \in C^\infty$, $\psi_\varepsilon'' = \psi'' * \phi_\varepsilon$ is nondecreasing and bounded, and $|\psi_\varepsilon(w) - \psi(w)| \leq \varepsilon \sup_{|v-w|\leq\varepsilon} |\psi'(v)| \leq \varepsilon C(1+|w|)$ since ψ' is Lipschitz. As $\mathbb{E}|Z| < \infty$, Step 1 for ψ_ε and $\varepsilon \to 0$ give the claim. □

Remark 9.5. The test functions used below are $\psi_{t,h}(w) = (w-t+h)_+^2/(4h)$, $h > 0$: they are C^1, $\psi_{t,h}'' = (2h)^{-1}\mathbf{1}\{w > t-h\}$ is nondecreasing, and $\psi_{t,h}(w) \geq (w-t)_+$ (for $w \geq t$ the difference is $(w-t-h)^2/(4h)$). The stop-loss function $(w-t)_+$ itself does not satisfy the hypothesis, and the conclusion fails for it: with $t = 0$, $K = \delta_{\sqrt{2}}$ and $T(x) = 2$, $\mathbb{E}(Z_K)_+ = \frac{1}{2}\mathbb{E}|Z_K|$ drops from $\frac{1}{2}\sqrt{2/e}$ to $\frac{1}{2}g(1/4) = \frac{1}{2}e^{-1/4}$.

(Not used below.) $\psi_{t,h}$ is the pointwise smallest ψ admissible in Lemma 9.4 with $\psi \geq (w-t)_+$ and $\psi(t+h) = h$, so the loss of this step cannot be reduced within the method. Proof, with $t = 0$: $\psi'(h) = 1$, and $\psi'' \geq 0$ because ψ is bounded below. Let $u^* < h$ be the largest zero of ψ' ($u^* = -\infty$ if there is none; then $\psi'(-\infty) = 0$). The measure $\mu = \psi''(v)\,dv$ on (u^*, h) has mass 1 and a nondecreasing density, and Taylor's formula gives $\psi(w) = \psi(u^*) + \mathbb{E}_\mu(w-V)_+$ for $w \in [u^*, h]$ and, at $w = h$, $\psi(u^*) = \mathbb{E}_\mu V$; so $\psi(w) = \mathbb{E}_\mu \max(V, w)$ and $\mathbb{E}_\mu V \geq 0$. Such a μ is a mixture of uniform laws on $[s, h]$, and for $V \sim U[s,h]$, $\mathbb{E}\max(V,w) = F_w(\frac{s+h}{2})$ with $F_w(x) = w + \frac{(h-w)^2}{4(h-x)}$ for $x \leq \frac{w+h}{2}$ and $F_w(x) = x$ otherwise, a C^1 convex nondecreasing function. Jensen gives $\psi(w) \geq F_w(\mathbb{E}_\mu V) \geq F_w(0) = \psi_{0,h}(w)$ for $w \in [\max(u^*, -h), h]$. To the left of u^*, ψ is nonincreasing and $\psi_{0,h}$ nondecreasing; $\psi_{0,h} = 0$ on $(-\infty, -h]$. For $w > h$: a probability density on $(-\infty, h)$ that is nondecreasing, bounded by $c = \psi''(h-)$ and has nonnegative mean forces $c \geq 1/(2h)$, so $\psi(w) \geq w + \frac{(w-h)^2}{4h} = \psi_{0,h}(w)$.

Lemma 9.6 (stop-loss bounds)**.** *Let $0 < \theta \leq A$, let K_R be a finitely supported Kolmogorov measure carried by $[-A, \theta)$, $a = K_R((0,\theta))$, $b = K_R([-A, 0])$, $\rho^2 = a + b$, $W = Z_{K_R}$, and*

$$W_B = \theta\big(N_{a/\theta^2} - a/\theta^2\big) + \sqrt{b}\,G, \qquad W_C = A\big(N_{b/A^2} - b/A^2\big) + \sqrt{a}\,G.$$

For $t \in \mathbb{R}$ and $h > 0$ put $\chi_h^B(t) = \frac{1}{2h}\mathbb{E}(W_B - t + h)_+^2$, $\chi_h^C(t) = \frac{1}{2h}\mathbb{E}(W_C - t + h)_+^2$. Then for every $t \in \mathbb{R}$:

(i) $2\mathbb{E}(W-t)_+ \leq \chi_h^B(t)$ *and* $2\mathbb{E}(-W-t)_+ \leq \chi_h^C(t)$;

(ii) $2\mathbb{E}(W-t)_+ \leq \sqrt{t^2+\rho^2} - t$ *and* $2\mathbb{E}(-W-t)_+ \leq \sqrt{t^2+\rho^2} - t$;

(iii) χ_h^B, χ_h^C *are C^1, convex and nonincreasing in t, with* $\frac{d^2}{dt^2}\chi_h^\bullet(t) = \mathbb{P}(W_\bullet > t-h)/h \in [0, 1/h]$ *a.e.;*

(iv) $\chi_h^B(t)$ *and* $\chi_h^C(t)$ *are nondecreasing in a and in b (the other fixed), and* $\chi_h^B(t)$ *is nondecreasing in θ.*

Proof. (i) $2\mathbb{E}(W-t)_+ \leq 2\mathbb{E}\psi_{t,h}(W)$. Apply Lemma 9.4 to K_R with $T(x) = \theta$ on $(0,\theta)$ and $T(x) = 0$ on $[-A, 0]$: $T_\# K_R = a\delta_\theta + b\delta_0$ and $Z_{T_\# K_R} \overset{d}{=} W_B$. For the second bound, $-W = Z_{\tilde{K}}$ with $\tilde{K}(B) = K_R(-B)$, carried by $(-\theta, A]$; take $T(x) = A$ on $[0, A]$ and $T(x) = 0$ on $(-\theta, 0)$, so $T_\#\tilde{K} = b\delta_A + a\delta_0$ and $Z_{T_\#\tilde{K}} \overset{d}{=} W_C$. (ii) $2(W-t)_+ = |W-t| + (W-t)$, so $2\mathbb{E}(W-t)_+ = \mathbb{E}|W-t| - t \leq (t^2+\rho^2)^{1/2} - t$; the same for $-W$. (iii) For fixed w, $t \mapsto (w-t+h)_+^2$ is C^1, convex, nonincreasing, with second derivative $2 \cdot \mathbf{1}\{w > t-h\}$; differentiate under $\mathbb{E}$ (dominated convergence). (iv) Increasing a to a' replaces W_B by $W_B + \theta(N' - \lambda')$ with an independent centred Poisson term, and increasing b adds

an independent centred Gaussian; for the convex function $w \mapsto (w-t+h)_+^2$ Jensen's inequality (conditionally on W_B) gives monotonicity. The same for W_C. Monotonicity in θ is Lemma 9.4 again (moving the atom $a\delta_\theta$ to $a\delta_{\theta'}$, $\theta' > \theta$). □

9.4 The jump law and the band bound

Lemma 9.7 (one jump)**.** *Let J take values in $[j_0, j_1]$ ($j_0 < j_1$), with mean μ and variance σ^2. (a) For every convex φ on $[j_0, j_1]$: $\mathbb{E}\varphi(J) \le \frac{(j_1-\mu)\varphi(j_0)+(\mu-j_0)\varphi(j_1)}{j_1-j_0}$. (b) If $\varphi \le \Gamma$ on $[j_0, j_1]$, where Γ is C^1 with Γ' absolutely continuous and $\Gamma'' \le \kappa$ a.e. on $[j_0, j_1]$, then $\mathbb{E}\varphi(J) \le \Gamma(\mu) + \kappa\sigma^2/2$. (c) (two-point bound) Let $\varphi \le \psi$ on $[j_0, \infty)$, where ψ is C^1 on $[j_0, \infty)$ with ψ' absolutely continuous and ψ'' nonincreasing a.e. (that is, ψ' is concave). Let $\mu > j_0$, $d = \mu - j_0$, $x = \mu + \sigma^2/d$ and $w = d^2/(d^2+\sigma^2)$. Then $\mathbb{E}\varphi(J) \le T_\psi(\sigma^2) := (1-w)\psi(j_0) + w\,\psi(x)$. If moreover ψ is convex and nonincreasing on $\mathbb{R}$, then for all $s^2 \ge \sigma^2$, $j_0' \le j_0$, $0 \le w' \le d^2/(d^2+s^2)$ and $u' \le d + s^2/d$,*

$$\mathbb{E}\varphi(J) \le (1-w')\,\psi(j_0') + w'\,\psi(j_0' + u').$$

Proof. (a) is convexity, $\varphi(J)$ lying below the chord. (b) $\Gamma(J) = \Gamma(\mu) + \Gamma'(\mu)(J-\mu) + \int_\mu^J (J-u)\Gamma''(u)\,du \le \Gamma(\mu) + \Gamma'(\mu)(J-\mu) + \kappa(J-\mu)^2/2$; take expectations.

(c) The law $P^* = (1-w)\delta_{j_0} + w\delta_x$ has mean $j_0 + w(x-j_0) = j_0 + \frac{d^2}{d^2+\sigma^2}\cdot\frac{d^2+\sigma^2}{d} = \mu$ and variance $(1-w)d^2 + w\sigma^4/d^2 = \sigma^2$. Let q be the quadratic with $q(j_0) = \psi(j_0)$, $q(x) = \psi(x)$, $q'(x) = \psi'(x)$ (if $\sigma^2 = 0$ then $x = \mu$, $w = 1$, $J = \mu$ a.s. and there is nothing to prove), and $k = q - \psi$. Then $k(j_0) = k(x) = k'(x) = 0$ and $k' = q' - \psi'$ is convex. By Rolle $k'(\xi) = 0$ for some $\xi \in (j_0, x)$; a convex function vanishing at the two points $\xi < x$ is ≤ 0 on $[\xi, x]$ and ≥ 0 on $[j_0, \xi] \cup [x, \infty)$. So k is nondecreasing on $[j_0, \xi]$, nonincreasing on $[\xi, x]$ and nondecreasing on $[x, \infty)$; with $k(j_0) = k(x) = 0$ this gives $k \ge 0$, i.e. $\psi \le q$ on $[j_0, \infty)$. As $\mathbb{E}q(J)$ depends only on the mean and variance of J, $\mathbb{E}\varphi(J) \le \mathbb{E}\psi(J) \le \mathbb{E}q(J) = \mathbb{E}_{P^*}q = \mathbb{E}_{P^*}\psi = T_\psi(\sigma^2)$.

For the second statement: if $\sigma^2 < s^2$, the two-point law P^{**} on $\{j_0, x(s^2)\}$ with mean μ arises from P^* by splitting the mass at $x(\sigma^2)$ between j_0 and $x(s^2) > x(\sigma^2)$ with conditional mean $x(\sigma^2)$, so $T_\psi(\sigma^2) \le T_\psi(s^2)$ for convex ψ (Jensen). Write $\tilde w = d^2/(d^2+s^2)$ and $\tilde u = d + s^2/d$, so $T_\psi(s^2) = \psi(j_0) - \tilde w\,(\psi(j_0) - \psi(j_0+\tilde u))$. The bracket is ≥ 0 as ψ is nonincreasing, so $T_\psi(s^2) \le (1-w')\psi(j_0) + w'\psi(j_0+\tilde u)$ for $w' \le \tilde w$, and $\psi(j_0) \le \psi(j_0')$, $\psi(j_0+\tilde u) \le \psi(j_0'+u')$ because $j_0' \le j_0$ and $j_0' + u' \le j_0 + \tilde u$. □

For $K_S \ne 0$ carried by $[\theta, A]$ the jump law ν_S/Λ of Lemma 9.3 has mean $\mu_1 = m/\Lambda$ and second moment $\int x^2\,\nu_S(dx)/\Lambda = V/\Lambda$, hence variance $\sigma_J^2 = (\Lambda V - m^2)/\Lambda^2$.

Lemma 9.8 (feasible parameters)**.** *If $K_S \ne 0$ is carried by $[\theta, A]$ and has mass V, then (F1) $V/A^2 \le \Lambda \le V/\theta^2$; (F2) $V/A \le m \le V/\theta$; (F3) $\theta\Lambda \le m \le A\Lambda$; (F4) $m^2 \le \Lambda V$; (F5) $\Lambda \le (\frac{1}{A} + \frac{1}{\theta})\,m - \frac{V}{A\theta}$.*

Proof. Integrate against K_S the pointwise inequalities, valid for $x \in [\theta, A]$: $A^{-2} \le x^{-2} \le \theta^{-2}$, $A^{-1} \le x^{-1} \le \theta^{-1}$, $\theta x^{-2} \le x^{-1} \le Ax^{-2}$, and $(x^{-1} - A^{-1})(\theta^{-1} - x^{-1}) \ge 0$; (F4) is Cauchy–Schwarz. □

Proposition 9.9 (band bound)**.** *Let $0 < \theta \le A$ and let K be a finitely supported probability Kolmogorov measure on $[-A, A]$ with $K_S = K|_{[\theta,A]} \ne 0$; let V, Λ, m be as in Lemma 9.3, $K_R = K - K_S$ with $a, b, \rho^2 = 1 - V$ as in Lemma 9.6, $W = Z_{K_R}$, $\ell(y) = \mathbb{E}|y + W|$ and $P_2(\Lambda) = 1 - e^{-\Lambda}(1+\Lambda)$.*

Let $c_B \ge 2\mathbb{E}(W-m)_+$, $c_C \ge 2\mathbb{E}(-W-(2\theta-m))_+$ and $O \ge \mathbb{E}\,\ell(J-m)$, $J \sim \nu_S/\Lambda$, independent of W. Then

$$\mathbb{E}|Z_K| \le e^{-\Lambda}(m+c_B) + \Lambda e^{-\Lambda}\,O + m\Lambda e^{-\Lambda} + P_2(\Lambda)\,c_C. \tag{9.1}$$

Moreover O may be taken as $\mu_1 - m + O'$ with $O' \ge 2\mathbb{E}[(-W-(J-m))_+]$, and then the right side of (9.1) equals $2me^{-\Lambda} + e^{-\Lambda}c_B + \Lambda e^{-\Lambda}O' + P_2(\Lambda)c_C$.

Proof. By Lemmas 9.2 and 9.3, $\mathbb{E}|Z_K| = \sum_{n\ge0}\mathbb{P}(N_S=n)\,\mathbb{E}\,\ell(S_n-m)$. For $n=0$, $\ell(-m) = m + 2\mathbb{E}(W-m)_+$ (Lemma 9.2). For $n=1$ the term is $\Lambda e^{-\Lambda}\mathbb{E}\ell(J-m)$. For $n\ge2$, $y = S_n - m \ge 2\theta - m$ and $\ell(y) = y + 2\mathbb{E}(-W-y)_+ \le y + 2\mathbb{E}(-W-(2\theta-m))_+$, because $y \mapsto \mathbb{E}(-W-y)_+$ is nonincreasing. Finally $\sum_{n\ge2}\mathbb{P}(N_S=n)\mathbb{E}(S_n-m) = \mathbb{E}(S_{N_S}-m) + me^{-\Lambda} - \Lambda e^{-\Lambda}(\mu_1-m) = m\Lambda e^{-\Lambda}$, using $\mathbb{E}Y=0$ and $\Lambda\mu_1 = m$. For the second form, $\ell(y) = y + 2\mathbb{E}(-W-y)_+$ holds for every real y (Lemma 9.2), so $\mathbb{E}\ell(J-m) = \mu_1 - m + 2\mathbb{E}(-W-(J-m))_+$, and $e^{-\Lambda}m + \Lambda e^{-\Lambda}(\mu_1-m) + m\Lambda e^{-\Lambda} = 2me^{-\Lambda}$. □

Admissible choices, all from Lemmas 9.2, 9.6 and 9.7: $c_B = \min(\chi_h^B(m), \sqrt{m^2+\rho^2} - m)$, $c_C = \min(\chi_h^C(2\theta-m), \sqrt{(2\theta-m)^2+\rho^2} - (2\theta-m))$, any $h>0$; for O the chord of the convex function ℓ on $[\theta-m, A-m]$ with endpoint values bounded by $\ell(y) \le \min\big(y+\chi_h^C(y),\ -y+\chi_h^B(-y),\ \sqrt{y^2+\rho^2}\big)$, or the variance bound of Lemma 9.7(b) on $[j_0,j_1] = [\theta-m, A-m]$, $\mu = \mu_1 - m$, $\sigma^2 = \sigma_J^2$, with $\Gamma(y) = y + \chi_h^C(y)$ ($\kappa = \mathbb{P}(W_C > \theta - m - h)/h$), $\Gamma(y) = -y + \chi_h^B(-y)$ ($\kappa = \mathbb{P}(W_B > m - A - h)/h \le 1/h$) or $\Gamma(y) = \sqrt{y^2+\rho^2}$ ($\kappa = \rho^2/(y_{\rm lo}^2+\rho^2)^{3/2}$, $y_{\rm lo} = \max(\theta-m, 0)$); these κ bound Γ'' on the range by Lemma 9.6(iii). For O': the chord on $[\theta-m, A-m]$ of the convex functions χ_h^C or $\sqrt{y^2+\rho^2} - y$.

The φ-form of these choices (used in Section 9.6). Put $\varphi(y) = 2\mathbb{E}(-W-y)_+$, so that $O' \ge \mathbb{E}\varphi(J-m)$ is required; φ is convex and nonincreasing, and by Lemmas 9.2 and 9.6

$$\varphi(y) \le \chi_h^C(y), \quad \varphi(y) \le \sqrt{y^2+\rho^2} - y, \quad \varphi(y) = -2y + 2\mathbb{E}(W+y)_+ \le -2y + \chi_h^B(-y)$$

for all $y \in \mathbb{R}$ and $h>0$. Admissible O' (with $J \in [\theta, A]$, mean μ_1, variance σ_J^2, $y = J-m$): (O1) the chord of φ itself (Lemma 9.7(a)), with the endpoint values $\varphi(\theta-m)$, $\varphi(A-m)$ replaced by any of the upper bounds above; (O2) Lemma 9.7(b) with $\Gamma(y) = -2y + \chi_h^B(-y)$, $\kappa = 1/h$ (Lemma 9.6(iii)); (O3) Lemma 9.7(c) with $j_0 = \theta - m$ and $\psi = \chi_h^C$, whose second derivative $\mathbb{P}(W_C > y - h)/h$ is nonincreasing (Lemma 9.6(iii)), ψ being convex and nonincreasing; (O4) if $\theta \ge m$: Lemma 9.7(c) with $j_0 = \theta - m \ge 0$ and $\psi(y) = \sqrt{y^2+r^2} - y$ for any $r^2 \ge \rho^2$, whose second derivative $r^2/(y^2+r^2)^{3/2}$ is nonincreasing on $[0,\infty)$. In (O3) and (O4) the mean of $J-m$ exceeds j_0 unless $J \equiv \theta$, in which case $\mathbb{E}\varphi(J-m) = \varphi(\theta-m)$. Upper bounds for σ_J^2: $(\Lambda V - m^2)/\Lambda^2$ (exact) and $(\mu_1-\theta)(A-\mu_1)$ (Bhatia–Davis).

9.5 The band lemma for C5

Theorem 9.10 (band lemma, $\theta=1$, $A=\sqrt{2}$)**.** *Let K be a probability Kolmogorov measure on $[-\sqrt{2},\sqrt{2}]$ with $K([1,\sqrt{2}]) \ge 9/10$ or $K([-\sqrt{2},-1]) \ge 9/10$. Then $\mathbb{E}|Z_K| \le \sqrt{2/e}$. If K is finitely supported, equality holds only for $K = \delta_{\pm\sqrt{2}}$.*

Proof. Reflection $x \mapsto -x$ maps Z_K to $-Z_K$, so assume $K([1,\sqrt{2}]) \ge 9/10$. Let first K be finitely supported, $K_S = K|_{[1,\sqrt{2}]}$, $V = K_S(\mathbb{R}) \ge 9/10$, $\rho^2 = 1 - V$.

Case $\rho^2 = 0$. $K = K_S$. If $K = \delta_1$ then $\mathbb{E}|Z_K| = \mathbb{E}|N_1 - 1| = 2/e < \sqrt{2/e}$. Otherwise $m = \int x^{-1}dK < 1$, Lemma 9.3 (with $K_R = 0$, $\theta = 1$) gives $\mathbb{E}|Z_K| = 2me^{-\Lambda} \le g(\Lambda) \le \sqrt{2/e}$, with equality iff $K = \delta_{\sqrt{2}}$.

Case $0 < \rho^2 \le 1/10$. Proposition 9.9 in its second form, with $\theta = 1$ and $A = \sqrt{2}$, gives

$$\mathbb{E}|Z_K| \le F := 2me^{-\Lambda} + e^{-\Lambda}c_B(m) + \Lambda e^{-\Lambda}O' + P_2(\Lambda)c_C(2-m),$$

with c_B, c_C, O' as listed after Proposition 9.9. The parameters (a, b, Λ, m) lie in

$$\mathcal{D} = \{a, b \geq 0,\ 0 < a + b \leq \tfrac{1}{10},\ (\Lambda, m) \text{ satisfy (F1)–(F5) with } V = 1 - a - b,\ \theta = 1,\ A = \sqrt{2}\},$$

and F depends only on (a, b, Λ, m) and the free parameters h. Section 9.5.1 describes a certified computation showing $F < \sqrt{2/e}$ on $\mathcal{D}$, which proves the strict inequality.

General K. Choose finitely supported probability measures K_n on $[-\sqrt{2}, \sqrt{2}]$ with $K_n([1, \sqrt{2}]) \geq 9/10$ and $K_n \to K$ weakly (move the mass of each cell of a partition of $[-\sqrt{2}, 1)$ and of $[1, \sqrt{2}]$ of mesh $1/n$ to a point of the same cell). Then $Z_{K_n} \to Z_K$ in law (the integrand in the Lévy–Khintchine exponent is bounded and continuous in x), and $\mathbb{E}Z_{K_n}^2 = 1$ gives uniform integrability, so $\mathbb{E}|Z_{K_n}| \to \mathbb{E}|Z_K|$ (this is the continuity step of RQ-AUD A.8 / A.26(e)). □

Corollary 9.11 (C5 reduces to the far region)**.** *If $\mathbb{E}|Z_K| \leq \sqrt{2/e}$ for every probability Kolmogorov measure K on $[-\sqrt{2}, \sqrt{2}]$ with $K([1, \sqrt{2}]) < 9/10$ and $K([-\sqrt{2}, -1]) < 9/10$, then C5 holds.*

Proof. Suppose $R_{\mathrm{ID}} := \sup_K \mathbb{E}|Z_K|/K(\mathbb{R})^{1/2} > \sqrt{2/e}$. By RQ-B Lemma 8.1 (audited, A.13a) a maximiser K^* with $K^*(\mathbb{R}) = 1$ exists, and by RQ-B Proposition 8.3 (A.13a) every support point $x > 0$ of K^* satisfies $x \leq 2(1 - u)/R_{\mathrm{ID}}$, where $u = \mathbb{P}(Z_{K^*} > 0)$, while $(1 - u)^2 \leq R_{\mathrm{ID}}^2/2$; hence $x \leq \sqrt{2}$. Mirrored, every support point $x < 0$ satisfies $|x| \leq 2u/R_{\mathrm{ID}} \leq \sqrt{2}$. So K^* is carried by $[-\sqrt{2}, \sqrt{2}]$, and by Theorem 9.10 or by the hypothesis, $R_{\mathrm{ID}} = \mathbb{E}|Z_{K^*}| \leq \sqrt{2/e}$, a contradiction. □

9.5.1 The certified computation (`scripts/verify_band.py`)

All inequalities are decided in ball arithmetic (python-flint `arb`, 80 bits); floating point is used only to choose the parameters h and the subdivision. Outputs: `outputs/verify_band_S.txt`, `outputs/verify_band_B.txt`; environment and md5 of the script in `outputs/verify_band_env.txt`.

Evaluation of χ. For $J > 0$, $\lambda \geq 0$, $s \geq 0$, $c \in \mathbb{R}$: $\mathbb{E}(J(N_\lambda - \lambda) - c + sG)_+^2 = \sum_{n \geq 0} p_n(\lambda)\, Q(J(n - \lambda) - c, s)$ with $Q(d, s) = \mathbb{E}(d + sG)_+^2 = (d^2 + s^2)\Phi(d/s) + ds\,\varphi(d/s)$ ($Q(d, 0) = d_+^2$). The sum is taken over $n \leq 14$; the tail is bounded by $\sum_{n>14} \frac{\lambda^n}{n!}((Jn + C)^2 + s^2) \leq t_{15}/(1 - q)$ with $C = J\lambda + |c|$, t_{15} its first term and $q = 16\lambda/15^2 < 1$ (ratio of consecutive terms), using $Q(d, s) \leq d^2 + s^2$ and $e^{-\lambda} \leq 1$.

Part S ($0 < \rho^2 \leq r = 1/50$). For $c = t - h > 0$ and $a, b \geq 0$, $a + b \leq r$: $\chi_h^B(t) \leq a\,\alpha_B + b\,\beta_B$ with $\beta_B = \tau(c/\sqrt{r})/(2h)$, $\tau(x) = \mathbb{E}(G - x)_+^2$, and $\alpha_B = \frac{1}{2h}\sum_{n \geq 1} \frac{r^{n-1}}{n!}((n - c)^2 + r)$ (the term $n = 0$ is $\mathbb{E}(\sqrt{b}G - a - c)_+^2 \leq b\,\tau(c/\sqrt{b}) \leq b\,\tau(c/\sqrt{r})$; for $n \geq 1$, $\mathbb{P}(N_a = n) \leq a\, r^{n-1}/n!$ and $\mathbb{E}(n - a - c + \sqrt{b}G)_+^2 \leq (n - a - c)^2 + b \leq (n - c)^2 + r$ when $0 \leq a \leq 2(n - c)$, which holds as $c < 0.95$); symmetrically $\chi_h^C(y) \leq a\,\alpha_C + b\,\beta_C$ with $\alpha_C = \tau(c/\sqrt{r})/(2h)$, $\beta_C = \frac{1}{2h}\sum_{n \geq 1} \frac{r^{n-1}}{2^n n!}((\sqrt{2}n - c)^2 + r)$. The series are summed to $n = 11$ with a tail bound of twice the next term. With $e^{-\Lambda}$, $\Lambda e^{-\Lambda}$, P_2 bounded on a (Λ, m) box and the chord weights at the box, this gives $F \leq M_0 + a\mathcal{A} + b\mathcal{B} \leq M_0 + \rho^2 \max(\mathcal{A}, \mathcal{B})$, where M_0 bounds $2me^{-\Lambda}$. Since $2me^{-\Lambda} \leq \sqrt{1 - \rho^2}\, g(\Lambda) \leq (1 - \rho^2/2)\sqrt{2/e}$, the box is certified if $\max(\mathcal{A}, \mathcal{B}) < \frac{1}{2}\sqrt{2/e}$ (then $F < \sqrt{2/e}$ for every $\rho^2 > 0$), or if $M_0 + r_B \max(\mathcal{A}, \mathcal{B}) < \sqrt{2/e}$ with $r_B = \min(r, 1 - m_1^2/\Lambda_2)$ (from (F4)), or by the crude bound $c_B \leq \rho^2/(2m)$, $O' \leq \rho$, $c_C \leq \rho^2/(2(2 - m))$. Result: 1098 boxes, 0 failures.

Part B ($1/50 \le \rho^2 \le 1/10$). The triangle $\{a, b \ge 0,\ a + b \le 1/10\}$ is covered by squares of side $1/256$; squares not certified are split into four, down to side $1/1024$. For a square $[a_1, a_2] \times [b_1, b_2]$ all costs are evaluated at the corner (a_2, b_2) and the Cauchy–Schwarz terms with $\rho^2 = a_2 + b_2$ (monotone by Lemma 9.6(iv)), and $V \in [1 - \min(a_2 + b_2, \frac{1}{10}),\ 1 - \max(a_1 + b_1, \frac{1}{50})]$. On a box $[\Lambda_1, \Lambda_2] \times [m_1, m_2]$ (with m on the grid $k/1024$) the box is discarded if (F1)–(F5) fail at every point, and otherwise certified if

$$M + e^{-\Lambda_1} c_B(m_1) + \Lambda_2 e^{-\Lambda_2}\, O'(m_2, \mu_{1,\mathrm{lo}}) + P_2(\Lambda_2)\, c_C(2 - m_2) < \sqrt{2/e},$$

where $M \ge \max 2me^{-\Lambda}$ over the box subject to $m \le \sqrt{\Lambda V_{\mathrm{hi}}}$ (computed exactly from the unimodality of g), $\mu_{1,\mathrm{lo}} = \max(1, m_1/\Lambda_2)$, and $O'(m_2, \mu)$ is the smallest of the chords of χ_h^C (four float-chosen h, common to both endpoints) and of $\sqrt{y^2 + \rho^2} - y$, with endpoint values at $y = 1 - m_2$ and $y = \sqrt{2} - m_2$. Validity: $2\mathbb{E}(W - t)_+$ and $2\mathbb{E}(-W - t)_+$ are nonincreasing in t, and so are the chord endpoint functions φ (Lemma 9.6(iii)); the chord has nonnegative weights, so it is at most the chord through the upper values $\bar g_1 \ge \varphi(1 - m)$, $\bar g_2 \ge \varphi(\sqrt{2} - m)$; the verifier replaces $\bar g_1$ by $\max(\bar g_1, \bar g_2)$ (still an upper bound, as $\varphi(1 - m) \ge \varphi(\sqrt{2} - m)$), which makes this chord nonincreasing in μ_1, so its value at $\mu_{1,\mathrm{lo}}$ bounds it on the box (the same is done for the linear coefficients of Part S); $e^{-\Lambda}$ decreases and $\Lambda e^{-\Lambda}$, P_2 increase on $[0, 1]$. Boxes are bisected (alternately in m and Λ) until certified. Result: 341 squares at side $1/256$ (85 not certified), 333 at $1/512$ (3 not certified), 12 at $1/1024$ (all certified); 598 squares certified in all, 1,339,228 (Λ, m) boxes, 95 s on 8 cores.

Controls. (Run before the $\max(\bar g_1, \bar g_2)$ change, which can only increase the computed bounds.) With $r = 0.06$ in Part S the linear certificate fails on 426,627 boxes; with the target lowered to $\sqrt{2/e} - 0.002$ Part S fails on 5,750 boxes, and Part B with target $\sqrt{2/e} - 0.001$ fails on 110 of 1281 squares at side $1/512$ (so the check is not vacuous; the margin is below 10^{-3} near $\rho^2 = 0.02$). A float test on 400 random K in the band (`scripts/band_soundness.py`) gives $F - \mathbb{E}|Z_K| \ge 1.5 \cdot 10^{-5}$ (the bound is above the exact value, computed by Poisson enumeration) and $\sqrt{2/e} - F \ge 3.2 \cdot 10^{-5}$.

9.6 The band lemma in the form needed at finite q

By the audited reduction (RQ-B C19 = RQ-A U.1, A.26) and the finite-q localisation (RQ-C C15, A.28), Conjecture S for all $q \le q_5 = 1 - 2/\sqrt{5}$ (and hence, with RQ-A MAIN-5, A.25, for all q) follows from the statement

$$\mathrm{ID}^*: \quad \mathbb{E}|Z_K| \le \max\big(g(\lambda_\theta^+(K)),\, g(\lambda_\theta^-(K)),\, C_5\big) \ \text{ for some } \theta = \theta(K),$$
$$\lambda_\theta^{\pm}(K) = \int_{\pm x \ge \theta} x^{-2}\, dK, \qquad C_5 = g(2\ln\tfrac{5}{4}) = 1.28\sqrt{2\ln 1.25} = 0.8551004\ldots,$$

for all finitely supported probability measures K on $[-1.54, 1.54]$ (A' of A.28 increases in q and $A'(q_5) = 1.538\ldots < 1.54$). We prove ID^* with $\theta = 0.85$ on a band.

Near the Dirac laws with $g(\Lambda) > C_5$ the bound F has to be sharp to first order in ρ^2, and one more choice of O' is needed, together with a lemma that absorbs its constant term into the main term.

(O5) If $\mu_1 > \theta$: for every $h > 0$ and $j_0' \le j_0 = \theta - m$, with $\kappa = (h - j_0')_+^2/(2h)$, $d = \mu_1 - \theta$ and $w = d^2/(d^2 + \sigma_J^2)$ (the *exact* σ_J^2),

$$O' = (1 - w)\,\kappa + (1 - w)\frac{\rho^2}{2h} + \chi_h^C(\mu_1 - m).$$

Indeed Lemma 9.7(c) (first statement) with $\psi = \chi_h^C$ gives $\mathbb{E}\varphi(J-m) \le (1-w)\chi_h^C(j_0) + w\chi_h^C(x)$ with $x = \mu_1 - m + \sigma_J^2/d \ge \mu_1 - m$; then $w \le 1$, $\chi_h^C \ge 0$ is nonincreasing, and $\chi_h^C(j_0) \le \chi_h^C(j_0') \le \kappa + \rho^2/(2h)$, because W_C has mean 0 and variance $a+b=\rho^2$, so that $\mathbb{E}(W_C+e)_+^2 \le \mathbb{E}(W_C+e)^2 = e^2+\rho^2$ for $e = h - j_0' \ge 0$ and $\mathbb{E}(W_C - c)_+^2 \le \mathbb{E}W_C^2 = \rho^2$ for $c = j_0' - h \ge 0$. The term $(1-w)\kappa$ does not vanish as $\rho^2 \to 0$; the next lemma absorbs it into the main term, using the slack that Cauchy–Schwarz (F4) leaves when $\sigma_J^2 > 0$.

Lemma 9.12 (absorption)**.** *Let $K_S \ne 0$ be carried by $[\theta, A]$, with mass V, Λ, m, $\mu_1 = m/\Lambda$ and σ_J^2 as above, $d = \mu_1 - \theta > 0$ and $w = d^2/(d^2+\sigma_J^2)$. If $0 < D \le d$ and $0 \le \kappa \le D^2\sqrt{\Lambda/V}$, then*

$$2me^{-\Lambda} + \Lambda e^{-\Lambda}\kappa\,(1-w) \le \sqrt{V}\,g(\Lambda).$$

Proof. $1 - w = \sigma_J^2/(d^2+\sigma_J^2) \le \sigma_J^2/D^2 = (\Lambda V - m^2)/(\Lambda^2 D^2)$, so the left side is at most $e^{-\Lambda}q(m)$ with $q(t) = 2t + \kappa(\Lambda V - t^2)/(\Lambda D^2)$. If $\kappa = 0$, $q(m) = 2m \le 2\sqrt{\Lambda V}$ by (F4). If $\kappa > 0$, q is a concave quadratic with vertex $t^* = \Lambda D^2/\kappa \ge \Lambda D^2/(D^2\sqrt{\Lambda/V}) = \sqrt{\Lambda V}$, so q is nondecreasing on $(-\infty, \sqrt{\Lambda V}]$; as $m \le \sqrt{\Lambda V}$ by (F4), $q(m) \le q(\sqrt{\Lambda V}) = 2\sqrt{\Lambda V}$. Finally $2e^{-\Lambda}\sqrt{\Lambda V} = \sqrt{V}\,g(\Lambda)$. □

Theorem 9.13 (ID* band lemma, $\theta = 0.85$, $A = 1.54$)**.** *Let K be a finitely supported probability Kolmogorov measure on $[-1.54, 1.54]$. If $K([0.85, 1.54]) \ge 4/5$ then $\mathbb{E}|Z_K| \le \max(g(\lambda_{0.85}^+(K)), C_5)$; if $K([-1.54, -0.85]) \ge 4/5$ then $\mathbb{E}|Z_K| \le \max(g(\lambda_{0.85}^-(K)), C_5)$.*

Proof. Reflection $x \mapsto -x$ maps Z_K to $-Z_K$ and exchanges λ_θ^+ and λ_θ^-, so assume $K([\theta, A]) \ge 4/5$ with $\theta = 0.85$, $A = 1.54$. Then $K_S = K|_{[\theta,A]} \ne 0$, $V = K_S(\mathbb{R}) \ge 4/5$, $\Lambda = \lambda_\theta^+(K)$, and $K_R = K - K_S$ is carried by $[-A, \theta)$ with $a = K_R((0,\theta))$, $b = K_R([-A, 0])$, $\rho^2 = a+b = 1-V \le 1/5$. Proposition 9.9 in its second form (no sign condition on $\theta - m$) gives

$$\mathbb{E}|Z_K| \le F := 2me^{-\Lambda} + e^{-\Lambda}c_B + \Lambda e^{-\Lambda}O' + P_2(\Lambda)\,c_C,$$

with $c_B \ge 2\mathbb{E}(W-m)_+$ and $c_C \ge 2\mathbb{E}(-W - (2\theta - m))_+$ from Lemma 9.6 and O' any of (O1)–(O4) after Proposition 9.9 or (O5) above. Every bound used is a function of (a, b, Λ, m), of $\sigma_J^2 = (\Lambda V - m^2)/\Lambda^2$ and of free parameters (h, upper bounds for σ_J^2), and (a, b, Λ, m) lies in

$$\mathcal{D}^* = \{a, b \ge 0,\ a + b \le \tfrac{1}{5},\ (\Lambda, m) \text{ satisfy (F1)–(F5) with } V = 1 - a - b\}.$$

The computation of Section 9.6.1 covers $\mathcal{D}^*$ by boxes in (a, b, Λ, m) and shows on each box that $F \le \max(g(\Lambda), C_5)$: either directly ($F < \max(g(\Lambda), C_5)$ with all costs at a corner of the box), or, for $a + b \le 1/50$ and $m < \theta$, from $F \le \sqrt{1-\rho^2}\,g(\Lambda) + a\mathcal{A} + b\mathcal{B}$ (by (F4), or by Lemma 9.12 when (O5) is used) and one of the tests (T1)–(T3) of Section 9.6.1. □

Corollary 9.14 (ID* reduces to a far region)**.** *Suppose that $\mathbb{E}|Z_K| \le C_5$ for every finitely supported probability measure K on $[-1.54, 1.54]$ with $K([0.85, 1.54]) < 4/5$ and $K([-1.54, -0.85]) < 4/5$. Then ID* holds for every finitely supported probability measure on $[-1.54, 1.54]$.*

Proof. On the band use Theorem 9.13 with $\theta = 0.85$; off the band the hypothesis gives $\mathbb{E}|Z_K| \le C_5 \le \max(g(\lambda_\theta^+), g(\lambda_\theta^-), C_5)$ for every θ. □

Since $\max(g(\Lambda), C_5) \le \max g = \sqrt{2/e}$, Theorem 9.13 also settles C5 on its band, and the far region left for C5 is that of Corollary 9.14. RQ-C pointed this out at 19:00 UTC. RQ-C's numerical lower bounds for $\sup \mathbb{E}|Z_K|$ are about 0.827 on this far region and about 0.850 on that of Corollary 9.11, against $\sqrt{2/e} = 0.8578$.

Corollary 9.15 (C5 reduces to the far region of Theorem 9.13)**.** (a) *The bound of Theorem 9.13 holds for every probability Kolmogorov measure K on $[-1.54, 1.54]$, finitely supported or not.* (b) *If $\mathbb{E}|Z_K| \le \sqrt{2/e}$ for every probability Kolmogorov measure K on $[-\sqrt{2}, \sqrt{2}]$ with $K([0.85, \sqrt{2}]) < 4/5$ and $K([-\sqrt{2}, -0.85]) < 4/5$, then C5 holds. In particular C5 follows from the hypothesis of Corollary 9.14.*

Proof. (a) By reflection, assume $K([\theta, A]) \ge 4/5$ ($\theta = 0.85$, $A = 1.54$). As in the proof of Theorem 9.10, move the mass of each cell of a partition of $[-A, \theta)$ and of $[\theta, A]$ of mesh $1/n$ to a point of the same cell. This gives finitely supported probability measures K_n on $[-A, A]$ with $K_n([\theta, A]) = K([\theta, A]) \ge 4/5$ and $K_n \to K$ weakly, so $\mathbb{E}|Z_{K_n}| \to \mathbb{E}|Z_K|$ by the continuity step there. Moreover $\lambda_\theta^+(K_n) \to \lambda_\theta^+(K)$, because x^{-2} is uniformly continuous on $[\theta, A]$ and the cells inside $[\theta, A]$ carry the same masses under K_n and K. As g is continuous, $\mathbb{E}|Z_K| = \lim \mathbb{E}|Z_{K_n}| \le \lim \max(g(\lambda_\theta^+(K_n)), C_5) = \max(g(\lambda_\theta^+(K)), C_5)$.

(b) As in the proof of Corollary 9.11, if C5 fails there is a maximiser K^* with $K^*(\mathbb{R}) = 1$, carried by $[-\sqrt{2}, \sqrt{2}] \subset [-1.54, 1.54]$, with $\mathbb{E}|Z_{K^*}| = R_{\mathrm{ID}} > \sqrt{2/e}$. If $K^*([0.85, \sqrt{2}]) \ge 4/5$ or $K^*([-\sqrt{2}, -0.85]) \ge 4/5$, part (a) gives $\mathbb{E}|Z_{K^*}| \le \max(g(\lambda_\theta^\pm(K^*)), C_5) \le \sqrt{2/e}$; otherwise the hypothesis does. Both contradict $R_{\mathrm{ID}} > \sqrt{2/e}$.

For the last sentence: the hypothesis of Corollary 9.14 (finitely supported K, bound $C_5 < \sqrt{2/e}$) extends to all probability measures K on $[-1.54, 1.54]$ with $K([0.85, 1.54]) < 4/5$ and $K([-1.54, -0.85]) < 4/5$. To see this, approximate as in (a) with cells inside $[-1.54, -0.85]$, $(-0.85, 0.85)$ and $[0.85, 1.54]$; these keep the two masses, so K_n stays in the far region. Every probability measure on $[-\sqrt{2}, \sqrt{2}]$ in the far region of (b) is such a K. □

9.6.1 The certified computation (`scripts/verify_bandstar.py`)

All inequalities are decided in ball arithmetic (python-flint `arb`, 80 bits), with $\theta = 17/20$, $A = 77/50$ and C_5 as balls containing the exact values; floating point only chooses the parameters h and the subdivision. The values χ_h^B, χ_h^C are enclosed as in Section 9.5.1 (lattice sum over $n \le 14$ plus the geometric tail bound, with jump θ resp. A). Grid points are rounded by exact comparisons with dyadic rationals. Output: `outputs/verify_bandstar.txt` (summary), `outputs/verify_bandstar_squares.jsonl` (one line per (a, b) square), environment and md5 in `outputs/verify_bandstar_env.txt`.[1]

Squares in (a, b). The triangle $\{a, b \ge 0,\ a + b \le \frac{1}{5}\}$ is covered by the squares $[a_1, a_2] \times [b_1, b_2]$ of side $1/128$ with $a_1 + b_1 < \frac{1}{5}$; a square that is not certified is split into four, down to side $1/8192$. On a square, $V \in [V_{\mathrm{lo}}, V_{\mathrm{hi}}] = [1 - \min(a_2 + b_2, \frac{1}{5}),\ 1 - a_1 - b_1]$, and every (a, b) of the square with $a + b \le \frac{1}{5}$ satisfies $a \le \bar{a}$, $b \le \bar{b}$, where $(\bar{a}, \bar{b}) = (a_2, b_2)$ if $a_2 + b_2 \le \frac{1}{5}$ and otherwise $\bar{a} = \min(a_2, \lceil \frac{1}{5} - b_1 \rceil)$, $\bar{b} = \min(b_2, \lceil \frac{1}{5} - a_1 \rceil)$ (rounded up to multiples of 2^{-24}). The costs χ_h^B, χ_h^C are evaluated at $(\bar{a}, \bar{b})$ (Lemma 9.6(iv)), and the Cauchy–Schwarz terms with $r^2 = \min(\bar{a} + \bar{b}, \frac{1}{5}) \ge \rho^2$.

Boxes in (Λ, m). For each square, $\Lambda \in [V_{\mathrm{lo}}/A^2 - 0.01,\ V_{\mathrm{hi}}/\theta^2 + 0.01]$ (in strips of width $1/64$) and $m \in [2125, 4820]/4096 \supset [0.8/A, 1/\theta]$ (in blocks of $64/4096$), which contains every point allowed by

[1] Editorial note. RQ-REF3's second robustness remark: this run stores no box-level certificate, only the per-square summaries listed here, so it cannot be replayed box by box. RQ-REF3 therefore re-did the computation from scratch with its own exact cover (1 212 certified squares, 9 077 343 leaf boxes, every square certified), and RQ-AUD's verdict A.34 also rests on its own cover (1 303 squares, 13 083 096 boxes, none uncertified). After the report, RQ-D re-ran this script unchanged and recorded every leaf box with its method and parameters, in new files on which no proof depends. RQ-AUD replayed that record leaf by leaf with its own verifier (A.34, addendum of 23 October 04:51 UTC): all 7 874 211 leaves are certified, so the record is VALID. See Appendices A and B.

(F1)–(F2). A box $[\Lambda_1,\Lambda_2]\times[m_1,m_2]$ is discarded if one of (F1)–(F5) fails at every point of the box for every $V\in[V_{\rm lo},V_{\rm hi}]$; otherwise it must pass the direct check or (if $a_2+b_2\le\frac{1}{50}$) the slope check below. Boxes that pass neither are bisected, alternately in m and in Λ, down to m-width $1/4096$ and Λ-width $1/16384$; a box that still fails makes the square uncertified.

On a box: $e^{-\Lambda}\le e^{-\Lambda_1}$, $\Lambda e^{-\Lambda}\le\max_{[\Lambda_1,\Lambda_2]}te^{-t}$, $P_2(\Lambda)\le P_2(\Lambda_2)$ ($P_2'(t)=te^{-t}\ge0$); the target is bounded below by $T=\max(\min(g(\Lambda_1),g(\Lambda_2)),C_5)$ (g is unimodal); M bounds $2me^{-\Lambda}=2e^{-\Lambda}\min(m,\sqrt{\Lambda V})$ (by (F4)) over the box with $m\le m_2$, $V\le V_{\rm hi}$, computed from the unimodality of g as in Section 9.5.1; $\mu_1=m/\Lambda\in[\mu_{\rm lo},\mu_{\rm hi}]$ with $\mu_{\rm lo}=\max(\theta,m_1/\Lambda_2)$, $\mu_{\rm hi}=\min(A,m_2/\Lambda_1)$; $d=\mu_1-\theta\ge d_{\rm lo}=\mu_{\rm lo}-\theta$; $\sigma_J^2\le s^2=\min((\Lambda_2V_{\rm hi}-m_1^2)/\Lambda_1^2,\ d_{\rm hi}(A-\theta-d_{\rm lo}))$ (exact formula and Bhatia–Davis); in the box version of Lemma 9.7(c), $j_0'=\theta-m_2$, $w'=d_{\rm lo}^2/(d_{\rm lo}^2+s^2)$ and $u'=\min_{d\in[d_{\rm lo},d_{\rm hi}]}(d+s^2/d)$, the far point $j_0'+u'$ being rounded down to the m-grid. The functions $t\mapsto2\mathbb{E}(W-t)_+$ and φ are nonincreasing, so their bounds are evaluated at the end of the box range where the function is largest: c_B at $t=m_1$, c_C at $2\theta-m_2$, the endpoint values of φ at $\theta-m_2$ and $A-m_2$ (any pointwise bound of φ may then be used at that point).

Direct check. With $c_B=\min(\chi_h^B(t),\sqrt{t^2+r^2}-t)$ at $t=m_1$ and $c_C=\min(\chi_h^C(y),\sqrt{y^2+r^2}-y)$ at $y=2\theta-m_2$, the box is certified if

$$M+e^{-\Lambda_1}c_B+P_2(\Lambda_2)\,c_C+\max_{[\Lambda_1,\Lambda_2]}(te^{-t})\,O'<T$$

for one of the following O', tried in this order: (O1) the chord with endpoint bounds $\bar\varphi_1=\min(\chi_h^C(y),\sqrt{y^2+r^2}-y,-2y+\chi_h^B(-y))$ at $y=\theta-m_2$ and $\bar\varphi_2=\min(\chi_h^C(y),\sqrt{y^2+r^2}-y)$ at $y=A-m_2$, with $\bar\varphi_1$ replaced by $\max(\bar\varphi_1,\bar\varphi_2)$ and μ_1 by $\mu_{\rm lo}$ (the chord through these values is nonincreasing in μ_1, see Section 9.5.1); (O3) in the box version with three float-chosen h; (O4) in the box version if $\theta-m_2\ge0$; (O2) with $\Gamma(\mu)\le-2(\mu_{\rm lo}-m_2)+\chi_h^B(t)$, $t\le-(\mu_{\rm hi}-m_1)$ on the grid, and $\sigma_J^2\le s^2$, two float-chosen h.

Slope check. Used when $a_2+b_2\le\frac{1}{50}$ and $m_2<\theta$. The range of ρ^2 on the box is $[r_0,r_B]$ with $r_0=a_1+b_1$ and $r_B=\min(a_2+b_2,\,1-m_1^2/\Lambda_2)$ (by (F4)); it is bisected up to six times. On a piece $[r_1,r_2]$: $V\le1-r_1$ is used for s^2, and all costs are replaced by linear bounds valid for $a,b\ge0$, $a+b\le r$, with $r=\min(\lceil4096r_2\rceil/4096,\frac{1}{50})\ge r_2$. For $c=t-h>0$ with $r/\theta\le2(\theta-c)$,

$$\chi_h^B(t)\le a\,\frac{1}{2h\theta^2}\sum_{n\ge1}\frac{(r/\theta^2)^{n-1}}{n!}\big((\theta n-c)^2+r\big)+b\,\frac{\tau(c/\sqrt{r})}{2h},\qquad\tau(x)=\mathbb{E}(G-x)_+^2,$$

because the term $n=0$ of the lattice sum is $\mathbb{E}(\sqrt{b}G-a/\theta-c)_+^2\le b\,\tau(c/\sqrt{b})\le b\,\tau(c/\sqrt{r})$, and for $n\ge1$, $\mathbb{P}(N_{a/\theta^2}=n)\le\frac{a}{\theta^2}\frac{(r/\theta^2)^{n-1}}{n!}$ and $\mathbb{E}(\theta n-a/\theta-c+\sqrt{b}G)_+^2\le(\theta n-a/\theta-c)^2+b\le(\theta n-c)^2+r$ (as $0\le a/\theta\le2(\theta n-c)$); symmetrically, for $c=y-h>0$ with $r/A\le2(A-c)$, $\chi_h^C(y)\le a\,\frac{\tau(c/\sqrt{r})}{2h}+b\,\frac{1}{2hA^2}\sum_{n\ge1}\frac{(r/A^2)^{n-1}}{n!}((An-c)^2+r)$. The series are summed to $n=11$, and the rest is bounded by twice the term $n=12$ with c replaced by 0 (consecutive terms decrease by a factor below $1/100$, as $r/\theta^2<0.03$). Further $\sqrt{t^2+\rho^2}-t\le\rho^2/(2t)$ for $t>0$. This gives linear bounds (α,β) for c_B (at m_1), c_C (at $2\theta-m_2$), and for O' through (O1) (the chord, with the max replacement done coefficientwise), (O3), (O4) and (O5). In (O5), $j_0'=\theta-m_2$, $\kappa=(h-j_0')_+^2/(2h)$ must satisfy $\kappa\le d_{\rm lo}^2\sqrt{\Lambda_1/(1-r_1)}$, $(1-w)\rho^2/(2h)\le(1-w')\rho^2/(2h)$, and $\chi_h^C(\mu_1-m)\le\chi_h^C(\theta-m_2+d_{\rm lo})$ (far point rounded down to the grid). Put $\mathcal{A}=e^{-\Lambda_1}\alpha_B+\max(te^{-t})\alpha_O+P_2(\Lambda_2)\alpha_C$, $\mathcal{B}$ likewise and $M_x=\max(\mathcal{A},\mathcal{B})$, for the combination of options that minimises M_x (chosen in floats). Then on the piece

$$F\le\sqrt{1-\rho^2}\,g(\Lambda)+\rho^2M_x\le\big(1-\tfrac{\rho^2}{2}\big)g(\Lambda)+\rho^2M_x,$$

by (F4) for (O1), (O3), (O4), and by Lemma 9.12 (with $D = d_{\mathrm{lo}}$, as $\Lambda \geq \Lambda_1$, $V \leq 1 - r_1$) for (O5). The piece is certified by one of: (T1) $M_x \leq \frac{1}{2}\min(g(\Lambda_1), g(\Lambda_2))$; then $F \leq g(\Lambda) \leq \max(g(\Lambda), C_5)$; (T2) $\hat{g} + \max(r_1(M_x - \hat{g}/2), r_2(M_x - \hat{g}/2)) < T$ with $\hat{g} = \max_{[\Lambda_1, \Lambda_2]} g$; then $F \leq \hat{g} + \rho^2(M_x - \hat{g}/2) < T$; (T3) $M_0 + r_2 M_x < T$, where M_0 bounds $2me^{-\Lambda}$ (with $V \leq 1 - r_1$), and for (O5) $M_0 = \max\big(M,\, e^{-\Lambda_1}(2m_2 + \kappa \max(0, \Lambda_2(1 - r_1) - m_2^2)/(\Lambda_1 d_{\mathrm{lo}}^2))\big)$, which bounds $2me^{-\Lambda} + \Lambda e^{-\Lambda}\kappa(1 - w)$ by the proof of Lemma 9.12 ($e^{-\Lambda}q(m) \leq e^{-\Lambda}q(m_2)$ if $m_2 < \sqrt{\Lambda V}$, and $\leq \sqrt{V}\, g(\Lambda) \leq M$ otherwise). Pieces with $m_1^2 > \Lambda_2(1 - r_1)$ are empty by (F4).

The slope check is what makes the theorem hold up to $\rho^2 = 0$ in the range $0.4463 < \Lambda < 0.5579$[2] where $g(\Lambda) > C_5$: there F equals $g(\Lambda)$ at the Dirac law and the margin is of order ρ^2. In this range (O3) with $h < \theta - m$ loses a factor about 3 in the b-coefficient and (O4) is lossy in the a-coefficient; (O5) with $h \approx 0.3$–$0.55 > \theta - m \approx 0.1$ is what makes $M_x < g/2$ near the Dirac curve.

Result. The recorded run of `scripts/verify_bandstar.py` (md5 `b5b55ceec828f01d ebc6c1a422e7270f`; 2026-10-22, 18:39:45–18:52:59 UTC, 8 processes, 793 s) certifies every square:

side of the squares	squares	not certified	(Λ, m) boxes
1/128	351	215	2,094,045
1/256	837	102	5,839,031
1/512	408	20	5,825,480
1/1024	80	0	1,135,478

The squares of a level are the children of the squares not certified at the level before, restricted to those that meet the triangle. So the 1339 certified squares cover the triangle, and the proof of Theorem 9.13 is complete. The leaf boxes of the certified squares are disposed of as follows: 3,114,781 are infeasible, 551,105 are certified by (O1), 2,876,016 by (O3), 128,597 by (O4), 1,203,286 by (O2) and 426 by the slope check. An earlier run (18:25–18:38 UTC) of a copy of the script that differs only in its docstring, an unused constant and argument, a log flush and the control shift below (which is 0 by default) gave the same counts (`outputs/verify_bandstar_run2.txt`).

Controls (not part of the proof). `scripts/verify_bandstar_controls.py` (output `outputs/verify_bandstar_controls.txt`, 60 s) reruns single squares, without refinement, with the target lowered by a shift (environment variable `BANDSTAR_TGT_SHIFT`; test (T1) is then disabled, since it only gives $F \leq g(\Lambda)$). The origin squares $[0, \frac{1}{256}]^2$ and $[0, \frac{1}{128}]^2$ are certified at shift 0 and are not certified at shift 0.0005. The first failing box, $\Lambda \in [0.56323, 0.56329]$, $m \in [3074, 3075]/4096$, lies on the Dirac curve $m^2 = \Lambda$, where $C_5 - g(\Lambda) \in [0.000496, 0.000502]$, so that the lowered target is at most $g(\Lambda) + 2 \cdot 10^{-6}$, while $F = g(\Lambda)$ at $\rho^2 = 0$. (The two neighbouring squares of side 1/128 are not certified without refinement even at shift 0; the certificate run splits them.) The 80 squares of side 1/1024 of the last level lie along the hypotenuse ($a + b \in [0.1972, 0.2]$, $a \in [0.0566, 0.0958]$).[3] All are certified at shift 0, and at shift 0.001, 63 of them are not. So the certified margin is below 10^{-3} along the hypotenuse and is 0 on the Dirac curve; the check is not vacuous.

[2] Editorial note. The refereed text (md5 `212c6f23...`) read 0.5599 here. RQ-AUD raised this as finding f1 of A.34 (addendum of 23 October, 03:02 UTC, text only): $g(\Lambda) > C_5$ exactly for $0.4462871\ldots < \Lambda < 0.5578588\ldots$. RQ-D corrected the figure at 05:35 UTC, and RQ-AUD checked the correction at 06:58 UTC (A.34 addendum, check a34i). The number plays no part in the proof.

[3] Editorial note. The refereed text read $a + b \in [0.1973, 0.2]$. In its replay of RQ-D's box-level record (A.34, addendum of 23 October, 04:51 UTC) RQ-AUD remarked that these 80 squares have $a + b \in [\frac{101}{512}, \frac{1}{5}]$ and $a \in [\frac{29}{512}, \frac{49}{512}]$, and $\frac{101}{512} = 0.197265625 < 0.1973$. RQ-D corrected the figure at 05:36 UTC, and RQ-AUD checked the correction at 06:58 UTC (check a34i). These controls are not part of the proof.

Float soundness test (evidence only). `scripts/bandstar_soundness2.py` draws random finitely supported K in the band and compares every ingredient bound with its exact value, computed from the exact laws of W (Poisson enumeration) and of J: c_B, c_C, each option (O1)–(O5) for $\mathbb{E}\varphi(J-m)$ (the two-point options also with the larger Bhatia–Davis variance, as in the box version), the bound $\chi_h^C(\theta-m) \le \kappa + \rho^2/(2h)$, the inequality of Lemma 9.12, and $F \ge \mathbb{E}|Z_K|$. Two samples were run: 400 random K with $\rho^2 \le \frac{1}{5}$ (`outputs/bandstar_soundness2.txt`) and 400 near-Dirac K with $\rho^2 \le \frac{1}{50}$ (`outputs/bandstar_soundness2_dirac.txt`). In both, no bound is below its exact value by more than 10^{-15}. The two bounds that are equalities in limit cases, $\chi_h^C(\theta-m) \le \kappa+\rho^2/(2h)$ and Lemma 9.12, have smallest gaps $-8.9\cdot10^{-16}$ and $-2.2\cdot10^{-16}$ (rounding). On the first sample $\min(F-\mathbb{E}|Z_K|) = 2.1\cdot10^{-4}$ and $\min(\max(g(\Lambda),C_5)-F) = 5.8\cdot10^{-4}$; on the second these are $1.5\cdot10^{-7}$ and $7.3\cdot10^{-7}$, as expected near the Dirac curve.

9.7 The heavy part of the far region

Throughout this section $\tau = 17/20$ and $A = 77/50$. For a probability Kolmogorov measure K on $[-A,A]$ put $V_+ = K([\tau,A])$ and $V_- = K([-A,-\tau])$. The far region of Corollary 9.14 is $\{V_+ < \frac{4}{5},\ V_- < \frac{4}{5}\}$; we split it into the *light* part $\{V_+ < \frac{1}{2},\ V_- < \frac{1}{2}\}$ and the *heavy* part, where $V_+ \ge \frac{1}{2}$ or $V_- \ge \frac{1}{2}$.

Theorem 9.16 (heavy far region)**.** *Let K be a probability Kolmogorov measure on $[-1.54,1.54]$ with $\frac{1}{2} \le K([0.85,1.54]) < \frac{4}{5}$ or $\frac{1}{2} \le K([-1.54,-0.85]) < \frac{4}{5}$. Then $\mathbb{E}|Z_K| < C_5$.*

Corollary 9.17 (ID* and C5 reduce to the light far region)**.** *Suppose that $\mathbb{E}|Z_K| \le C_5$ for every finitely supported probability measure K on $[-1.54,1.54]$ with $K([0.85,1.54]) < \frac{1}{2}$ and $K([-1.54,-0.85]) < \frac{1}{2}$. Then the hypothesis of Corollary 9.14 holds. Hence ID* holds for every finitely supported probability measure on $[-1.54,1.54]$, and C5 holds (Corollary 9.15).*

Proof. Let K be finitely supported on $[-1.54,1.54]$ with $V_+ < \frac{4}{5}$ and $V_- < \frac{4}{5}$. If $V_+ < \frac{1}{2}$ and $V_- < \frac{1}{2}$, the hypothesis gives $\mathbb{E}|Z_K| \le C_5$; otherwise Theorem 9.16 does. This is the hypothesis of Corollary 9.14, and Corollary 9.15 (last sentence) gives C5. □

The proof of Theorem 9.16 is a moment argument for everything except the positive edge $[\tau,A]$, which is handled exactly. Lemma 9.18 replaces the jumps in $[\tau,A]$ by jumps at τ and A (a convex-order increase). Their Poisson counts are then fixed on a box of the two chord rates. Everything else (the negative edge, the residual, and the part of the chord rates above the lower corner of the box) is a rest measure W on $[-A,\tau]\cup\{A\}$. It enters only through its cumulants, which are bounded by a degree-16 polynomial majorant and a Lagrangian relaxation, both checked in ball arithmetic.

9.7.1 Chord reduction of the positive edge

For $a,b \ge 0$ put $M(a,b) = a\tau^2 + bA^2$ and $Q(a,b) = (a\tau+bA)^2/(a+b)$, with $Q(0,0) = 0$.

Lemma 9.18 (chord reduction)**.** *Let K_+ be a finite measure on $[\tau,A]$, $\nu(dx) = x^{-2}K_+(dx)$, and*

$$a_+ = \int \frac{A-x}{A-\tau}\,\nu(dx), \qquad b_+ = \int \frac{x-\tau}{A-\tau}\,\nu(dx), \qquad K_+^{\#} = a_+\tau^2\delta_\tau + b_+A^2\delta_A.$$

(i) $Q(a_+,b_+) \le K_+(\mathbb{R}) \le M(a_+,b_+)$. (ii) *For every finite measure W with bounded support and every convex $\psi:\mathbb{R}\to\mathbb{R}$ with $|\psi(z)| \le c(1+|z|)$, $\mathbb{E}\psi(Z_{K_+ + W}) \le \mathbb{E}\psi(Z_{K_+^{\#}+W})$. In particular $\mathbb{E}|Z_{K_+ + W}| \le \mathbb{E}|Z_{K_+^{\#}+W}|$.*

Proof. Put $\Lambda = \nu(\mathbb{R}) \le \tau^{-2} K_+(\mathbb{R})$ and $m = \int x\,\nu(dx)$. Since $\tau(A-x) + A(x-\tau) = (A-\tau)x$, we have $a_+ + b_+ = \Lambda$ and $a_+\tau + b_+ A = m$. If $\Lambda = 0$ then $K_+ = K_+^{\#} = 0$ and there is nothing to prove; let $\Lambda > 0$.

(i) Cauchy–Schwarz gives $m^2 \le \Lambda \int x^2\,\nu(dx) = \Lambda K_+(\mathbb{R})$, i.e. $Q(a_+, b_+) \le K_+(\mathbb{R})$. By convexity, $x^2 \le \frac{A-x}{A-\tau}\tau^2 + \frac{x-\tau}{A-\tau}A^2$ on $[\tau, A]$; integrating against ν gives $K_+(\mathbb{R}) \le M(a_+, b_+)$.

(ii) As in the proof of Lemma 9.3, $Z_{K_+} \overset{d}{=} S_N - m$, where $N \sim \text{Poisson}(\Lambda)$ and, independently, $S_n = J_1 + \cdots + J_n$ with J_i i.i.d. of law ν/Λ. Let $J_i^{\#}$ be i.i.d. of law $\pi = (a_+\delta_\tau + b_+\delta_A)/\Lambda$, with partial sums $S_n^{\#}$, independent of N. For convex φ and $x \in [\tau, A]$, $\varphi(x) \le \frac{A-x}{A-\tau}\varphi(\tau) + \frac{x-\tau}{A-\tau}\varphi(A)$, and integrating against ν/Λ gives $\mathbb{E}\varphi(J_1) \le \mathbb{E}\varphi(J_1^{\#})$. Applying this to the convex functions $\varphi(\cdot + s)$ and integrating over the other (independent) summands, we may replace $J_1, \dots, J_n$ by $J_1^{\#}, \dots, J_n^{\#}$ one at a time: $\mathbb{E}\varphi(S_n + y) \le \mathbb{E}\varphi(S_n^{\#} + y)$ for all n and y. Summing against $\mathbb{P}(N = n)$ gives $\mathbb{E}\varphi(S_N - m + y) \le \mathbb{E}\varphi(S_N^{\#} - m + y)$. By the colouring theorem for Poisson processes, $S_N^{\#} \overset{d}{=} \tau N_{a_+} + A N_{b_+}$ with independent counts, so $S_N^{\#} - m \overset{d}{=} Z_{K_+^{\#}}$. Finally, $Z_{K_+ + W} = Z_{K_+} + Z_W$ and $Z_{K_+^{\#} + W} = Z_{K_+^{\#}} + Z_W$ with independent summands; take $\varphi = \psi$, condition on $Z_W = y$ and integrate. All expectations are finite, since $|\psi(z)| \le c(1 + |z|)$ and all the variables are square integrable. □

Lemma 9.19 (the rate functions)**.** *On $[0,\infty)^2$ the functions M, Q and $M - Q$ are continuous and nondecreasing in each variable, $M(a,b) - Q(a,b) = ab(A-\tau)^2/(a+b)$ for $a + b > 0$, and $Q(a,b) \ge \max(a\tau^2, bA^2)$.*

Proof. For $a + b > 0$, $(a\tau^2 + bA^2)(a+b) - (a\tau + bA)^2 = ab(A-\tau)^2$, which gives the formula. The function $ab/(a+b)$ is nondecreasing in each variable: it equals $(1/a + 1/b)^{-1}$ if $a, b > 0$ and 0 otherwise. Continuity at 0 follows from $0 \le Q \le M \le A^2(a+b)$. With $s = a\tau + bA$, $\partial_a Q = s\,(a\tau + b(2\tau - A))/(a+b)^2 \ge 0$ because $2\tau = 1.7 > A$, and $\partial_b Q = s\,(a(2A - \tau) + bA)/(a+b)^2 \ge 0$. Hence $Q(a,b) \ge Q(a,0) = a\tau^2$ and $Q(a,b) \ge Q(0,b) = bA^2$. □

9.7.2 Reduction to a box of chord rates

For a box $B = [a_1, a_2] \times [b_1, b_2] \subset [0,\infty)^2$ put

$$\mu_B = 1 - \max\bigl(Q(a_2, b_2), \tfrac{1}{2}\bigr) + M(a_2, b_2) - M(a_1, b_1), \qquad \text{cap}_B = (b_2 - b_1)A^2,$$

$C_B = \tau(N_{a_1} - a_1) + A(N_{b_1} - b_1)$ (independent Poisson counts) and $h_B(r) = \mathbb{E}|C_B + r|$. Let $\mathcal{W}_B$ be the set of measures W on $[-A, \tau] \cup \{A\}$ with $W(\mathbb{R}) = \mu_B$ and $W(\{A\}) \le \text{cap}_B$. Call B *empty* if $Q(a_1, b_1) \ge \frac{4}{5}$ or $M(a_2, b_2) < \frac{1}{2}$.

Lemma 9.20 (box reduction)**.** *Let K be a probability Kolmogorov measure on $[-A, A]$ with $\frac{1}{2} \le V_+ < \frac{4}{5}$, and let (a_+, b_+) be the chord rates of $K_+ = K|_{[\tau, A]}$ (Lemma 9.18).* (i) $(a_+, b_+) \in [0, \frac{28}{25}] \times [0, \frac{17}{50}]$. (ii) *If $(a_+, b_+) \in B$, then B is not empty, and there is $W \in \mathcal{W}_B$ with $\mathbb{E}|Z_K| \le \mathbb{E}h_B(Z_W)$.*

Proof. (i) By Lemmas 9.18(i) and 9.19, $\max(a_+\tau^2, b_+A^2) \le Q(a_+, b_+) \le V_+ < \frac{4}{5}$. So $a_+ < 0.8/\tau^2 = 1.107\ldots < \frac{28}{25}$ and $b_+ < 0.8/A^2 = 0.337\ldots < \frac{17}{50}$.

(ii) Write $Q_+ = Q(a_+, b_+)$, $M_+ = M(a_+, b_+)$, $Q_i = Q(a_i, b_i)$ and $M_i = M(a_i, b_i)$. By Lemma 9.19, $Q_1 \le Q_+ \le Q_2$ and $M_1 \le M_+ \le M_2$. If $Q_1 \ge \frac{4}{5}$ then $Q_+ > V_+$, and if $M_2 < \frac{1}{2}$ then $M_+ < V_+$; both contradict Lemma 9.18(i). So B is not empty.

Let $W_0 = K|_{[-A,\tau)}$, of mass $1 - V_+$, and $W_1 = W_0 + (a_+ - a_1)\tau^2\delta_\tau + (b_+ - b_1)A^2\delta_A$. Then $K_+^{\#} + W_0 = K_c + W_1$ with $K_c = a_1\tau^2\delta_\tau + b_1A^2\delta_A$, and $Z_{K_c} \overset{d}{=} C_B$. The measure W_1 is carried by $[-A, \tau] \cup \{A\}$, $W_1(\{A\}) = (b_+ - b_1)A^2 \le \text{cap}_B$, and $W_1(\mathbb{R}) = 1 - V_+ + M_+ - M_1$. We claim

that $W_1(\mathbb{R}) \le \mu_B$. Since $V_+ \ge \max(Q_+, \frac{1}{2})$ by Lemma 9.18(i), it suffices that $\max(Q_+, \frac{1}{2}) - M_+ \ge \max(Q_2, \frac{1}{2}) - M_2$:

- if $Q_2 \le \frac{1}{2}$, the left side is at least $\frac{1}{2} - M_+ \ge \frac{1}{2} - M_2$, which is the right side;
- if $Q_2 > \frac{1}{2}$, the left side is at least $Q_+ - M_+ \ge Q_2 - M_2$, because $M - Q$ is nondecreasing.

Put $W = W_1 + (\mu_B - W_1(\mathbb{R}))\,\delta_0 \in \mathcal{W}_B$; then $Z_W \overset{d}{=} Z_{W_1} + \sigma G$ with $\sigma^2 = \mu_B - W_1(\mathbb{R})$. Now $\mathbb{E}|Z_K| \le \mathbb{E}|Z_{K_+^{\#}+W_0}|$ by Lemma 9.18(ii), and $\mathbb{E}|Z_{K_+^{\#}+W_0}| = \mathbb{E}|C_B + Z_{W_1}|$. Next, $\mathbb{E}|C_B + Z_{W_1}| \le \mathbb{E}|C_B + Z_{W_1} + \sigma G|$ by Jensen ($\mathbb{E}|x + \sigma G| \ge |x|$, conditionally on $C_B + Z_{W_1}$), and $\mathbb{E}|C_B + Z_{W_1} + \sigma G| = \mathbb{E}|C_B + Z_W| = \mathbb{E}h_B(Z_W)$ by independence. □

9.7.3 The rest: moments, linear functionals, and the certificate inequalities

For $W \in \mathcal{W}_B$ put $\kappa_j(W) = \int x^{j-2}\,W(dx)$ for $j \ge 2$; so $\kappa_2(W) = \mu_B$ (with $0^0 = 1$), and κ_3, κ_4 are the first and second moments of W. Put $R_B = [-A\mu_B,\ \tau\mu_B + (A-\tau)\mathrm{cap}_B] \times [0,\ A^2\mu_B]$.

Lemma 9.21 (moments of the rest)**.** *Let $W \in \mathcal{W}_B$ and $Y = Z_W$. Then $\mathbb{E}e^{s|Y|} < \infty$ for every s. The cumulants of Y are 0 (first) and $\kappa_j(W)$ ($j \ge 2$), and $\mathbb{E}Y^n = P_n$, where $P_0 = 1$, $P_1 = 0$ and $P_n = \sum_{i=2}^{n} \binom{n-1}{i-1}\kappa_i(W)P_{n-i}$. Moreover $(\kappa_3(W), \kappa_4(W)) \in R_B$.*

Proof. W has compact support, so $\mathcal{K}(s) = \log \mathbb{E}e^{sY} = \int (e^{sx} - 1 - sx)\,x^{-2}\,W(dx) = \sum_{j\ge 2} \frac{s^j}{j!}\kappa_j(W)$ is an entire function. Comparing the coefficients of $s^{n-1}/(n-1)!$ in $\mathcal{M}' = \mathcal{K}'\mathcal{M}$, where $\mathcal{M} = e^{\mathcal{K}}$, gives the recursion. For the last claim, with $w = W(\{A\}) \le \mathrm{cap}_B$: $\kappa_3 \le \tau(\mu_B - w) + Aw \le \tau\mu_B + (A-\tau)\mathrm{cap}_B$, $\kappa_3 \ge -A\mu_B$, and $0 \le \kappa_4 \le A^2\mu_B$. □

Lemma 9.22 (linear functionals)**.** *Let R be a Borel function on $[-A, \tau] \cup \{A\}$, bounded above on $[-A, \tau]$ by S. Then $\int R\,dW \le \mu_B S + \mathrm{cap}_B\,(R(A) - S)_+$ for every $W \in \mathcal{W}_B$.*

Proof. With $w = W(\{A\}) \in [0, \mathrm{cap}_B]$ we have $W([-A, \tau]) = \mu_B - w \ge 0$. So $\int R\,dW \le (\mu_B - w)S + wR(A) = \mu_B S + w(R(A) - S) \le \mu_B S + \mathrm{cap}_B(R(A) - S)_+$. □

A *cell* is a rectangle $\mathcal{C} = [k_3^-, k_3^+] \times [k_4^-, k_4^+]$. We write $\mathcal{W}_B(\mathcal{C}) = \{W \in \mathcal{W}_B : (\kappa_3(W), \kappa_4(W)) \in \mathcal{C}\}$. All statements below are about $W \in \mathcal{W}_B(\mathcal{C})$, and every real parameter in them (s_3, s_4, the multipliers, the coefficients of φ) is arbitrary. The certificate supplies them, and they need not be optimal.

(a) Cumulant ranges. Let $j \in \{3, \dots, 16\}$, $s_3, s_4 \in \mathbb{R}$, $g(x) = x^{j-2} - s_3 x - s_4 x^2$ and $S \ge \sup_{[-A,\tau]} g$. Then $\kappa_j = \int g\,dW + s_3\kappa_3 + s_4\kappa_4$, so Lemma 9.22 gives

$$\kappa_j \le U_j := \mu_B S + \mathrm{cap}_B(g(A) - S)_+ + \max(s_3 k_3^-, s_3 k_3^+) + \max(s_4 k_4^-, s_4 k_4^+).$$

The lower bound L_j comes in the same way from $-g$ (with its own s_3, s_4). For $j = 3, 4$ the ranges are intersected with $\mathcal{C}$. If $L_j > U_j$ for some j, then $\mathcal{W}_B(\mathcal{C}) = \emptyset$.

(b) Empty cells (Farkas). Let $g(x) = -s_3 x - s_4 x^2$ and $S \ge \sup_{[-A,\tau]} g$. For every $W \in \mathcal{W}_B(\mathcal{C})$ we have $0 = \int g\,dW + s_3\kappa_3 + s_4\kappa_4 \le \Phi := \mu_B S + \mathrm{cap}_B(g(A) - S)_+ + \max(s_3 k_3^-, s_3 k_3^+) + \max(s_4 k_4^-, s_4 k_4^+)$. So $\Phi < 0$ implies $\mathcal{W}_B(\mathcal{C}) = \emptyset$.

(c) The Lagrangian bound. Let $\varphi(r) = \sum_{k=0}^{16} c_k r^k$. By Lemma 9.21, $\mathbb{E}\varphi(Z_W) = \sum_k c_k P_k$. Expanding the P_k with $\kappa_2 = \mu_B$ gives

$$\mathbb{E}\varphi(Z_W) = c' + \sum_{j=3}^{16} p_j \kappa_j + \sum_{\alpha \in \mathcal{P}} e_\alpha \kappa^\alpha,$$

where $\mathcal{P}$ is the set of sorted tuples $\alpha = (\alpha_1 \le \cdots \le \alpha_t)$, $t \ge 2$, $\alpha_i \ge 3$, that occur in some P_k, $k \le 16$, together with their prefixes of length ≥ 2 (81 tuples, $t \le 5$), and $\kappa^\alpha = \prod_i \kappa_{\alpha_i}$. The coefficients c', p_j, e_α are exact polynomials in μ_B and the c_k. For $\alpha = (\alpha', j) \in \mathcal{P}$ (α' the prefix of length $t-1$) let $X = \kappa^{\alpha'}$ (or $X = \kappa_{\alpha_1}$ if $t = 2$) and $Y = \kappa_j$. Let $[Y^-, Y^+] = [L_j, U_j]$ from (a), and let $[X^-, X^+]$ be the interval product of the ranges from (a) of the factors of X. Likewise $[\kappa^{\alpha,-}, \kappa^{\alpha,+}]$ is the interval product of the ranges of the κ_{α_i}. With $w_\alpha = \kappa^\alpha$ the following are ≥ 0 on $\mathcal{W}_B(\mathcal{C})$:

$$\begin{gathered}
w_\alpha - X^-Y - Y^-X + X^-Y^-, \qquad w_\alpha - X^+Y - Y^+X + X^+Y^+, \\
-w_\alpha + X^+Y + Y^-X - X^+Y^-, \qquad -w_\alpha + X^-Y + Y^+X - X^-Y^+, \\
\mu_B^{t-1} \int |x|^{s_\alpha}\, dW - w_\alpha, \qquad \mu_B^{t-1} \int |x|^{s_\alpha}\, dW + w_\alpha \qquad (s_\alpha = \textstyle\sum_i (\alpha_i - 2)), \\
k_3^+ - \kappa_3, \quad \kappa_3 - k_3^-, \quad k_4^+ - \kappa_4, \quad \kappa_4 - k_4^-.
\end{gathered}$$

The first four are the McCormick inequalities $(X - X^-)(Y - Y^-) \ge 0$, $(X^+ - X)(Y^+ - Y) \ge 0$, $(X^+ - X)(Y - Y^-) \ge 0$, $(X - X^-)(Y^+ - Y) \ge 0$. The next two are Hölder's inequality: for $\mu_B > 0$ and the probability measure W/μ_B, $\prod_i \mathbb{E}|x|^{p_i} \le \prod_i (\mathbb{E}|x|^s)^{p_i/s} = \mathbb{E}|x|^s$ with $p_i = \alpha_i - 2 \ge 1$ and $s = \sum p_i$ (Lyapunov), so $|\kappa^\alpha| \le \prod_i \int |x|^{\alpha_i - 2} dW \le \mu_B^{t-1} \int |x|^{s_\alpha} dW$; if $\mu_B = 0$ then $W = 0$. The last four are the definition of $\mathcal{W}_B(\mathcal{C})$. Add nonnegative multiples of these expressions to $\mathbb{E}\varphi(Z_W)$. Since $\kappa_j = \int x^{j-2} dW$, the result has the form $c'' + \int R\, dW + \sum_\alpha e'_\alpha w_\alpha$ with $R(x) = \sum_j p'_j x^{j-2} + \sum_s \gamma_s |x|^s$. By Lemma 9.22 and $w_\alpha \in [\kappa^{\alpha,-}, \kappa^{\alpha,+}]$,

$$\mathbb{E}\varphi(Z_W) \le \beta := c'' + \mu_B S_R + \mathrm{cap}_B(R(A) - S_R)_+ + \sum_\alpha \max(e'_\alpha \kappa^{\alpha,-}, e'_\alpha \kappa^{\alpha,+}),$$

for any $S_R \ge \sup_{[-A,\tau]} R$. On $[-A, 0]$ and on $[0, \tau]$, R is a polynomial.

Lemma 9.23 (majorant test)**.** *Let $L \ge \tau a_1 + A b_1$ and $n_a, n_b \ge 0$. For $n \le n_a$, $m \le n_b$ put $\pi_{nm} = \mathbb{P}(N_{a_1} = n)\mathbb{P}(N_{b_1} = m)$ and $c_{nm} = \tau(n - a_1) + A(m - b_1)$. Let $T \ge \mathbb{P}(N_{a_1} > n_a) + \mathbb{P}(N_{b_1} > n_b)$ and $e = (T(\tau^2 a_1 + A^2 b_1))^{1/2}$.* (i) *$h_B(r) \le H(r) := \sum_{n \le n_a, m \le n_b} \pi_{nm} |c_{nm} + r| + T|r| + e$ for all r.* (ii) *$h_B(r) = r$ for $r \ge L$, and $h_B(r) \le -r + \delta$ for $r \le -L$, where $\delta = 2 \sum_{n \le n_a, m \le n_b} \pi_{nm} (c_{nm} - L)_+ + 2e$.* (iii) *Let φ be a polynomial and $\varepsilon \ge 0$. Suppose the Taylor coefficients of $t \mapsto \varphi(L + t) - L - t$ and of $t \mapsto \varphi(-L - t) - L - t - \delta$ are nonnegative, and $\varphi + \varepsilon \ge H$ on $[-L, L]$. Then $\varphi + \varepsilon \ge h_B$ on $\mathbb{R}$.*

Proof. Let $E = \{N_{a_1} \le n_a,\ N_{b_1} \le n_b\}$, so $\mathbb{P}(E^c) \le T$, and recall $\mathbb{E}C_B = 0$, $\mathbb{E}C_B^2 = \tau^2 a_1 + A^2 b_1$. (i) $\mathbb{E}[|C_B + r|; E]$ is the sum, and $\mathbb{E}[|C_B + r|; E^c] \le |r|\mathbb{P}(E^c) + \mathbb{E}[|C_B|; E^c] \le T|r| + (\mathbb{P}(E^c)\mathbb{E}C_B^2)^{1/2}$ (Cauchy–Schwarz). (ii) $C_B \ge -\tau a_1 - A b_1 \ge -L$, so $C_B + r \ge 0$ and $h_B(r) = r$ for $r \ge L$. For $r \le -L$, $|C_B + r| = |r| - C_B + 2(C_B - |r|)_+$, so $h_B(r) = -r + 2\mathbb{E}(C_B - |r|)_+ \le -r + 2\mathbb{E}(C_B - L)_+$. On E this is the sum, and on E^c use $(C_B - L)_+ \le |C_B|$ and Cauchy–Schwarz as in (i). (iii) For $t \ge 0$, $\varphi(L + t) \ge L + t = h_B(L + t)$ and $\varphi(-L - t) \ge L + t + \delta \ge h_B(-L - t)$ by (ii); on $[-L, L]$ use (i). □

On $[-L, L]$, H is piecewise linear, with kinks at 0 and at the points $-c_{nm}$. The test $\varphi + \varepsilon \ge H$ is therefore one polynomial upper bound per piece, $\sup(H - \varphi) \le \varepsilon$.

Lemma 9.24 (cell certificate)**.** *If $\varphi + \varepsilon \geq h_B$ on $\mathbb{R}$ and $\mathbb{E}\varphi(Z_W) \leq \beta$ for all $W \in \mathcal{W}_B(\mathcal{C})$, then $\mathbb{E}h_B(Z_W) \leq \beta + \varepsilon$ for all $W \in \mathcal{W}_B(\mathcal{C})$.*

Proof. $h_B \leq \varphi + \varepsilon$ pointwise, and $\mathbb{E}|\varphi(Z_W)| < \infty$ by Lemma 9.21. □

Proof of Theorem 9.16. Reflection $x \mapsto -x$ maps Z_K to $-Z_K$ and exchanges V_+ and V_-, so assume $\frac{1}{2} \leq V_+ < \frac{4}{5}$. By Lemma 9.20(i), the chord rates (a_+, b_+) lie in some leaf box B of the cover of $[0, \frac{28}{25}] \times [0, \frac{17}{50}]$ described in Section 9.7.4. By Lemma 9.20(ii), B is not empty, so the computation has a tiling of R_B by cells with certificates for B. Also by Lemma 9.20(ii), there is $W \in \mathcal{W}_B$ with $\mathbb{E}|Z_K| \leq \mathbb{E}h_B(Z_W)$. By Lemma 9.21, $(\kappa_3(W), \kappa_4(W)) \in R_B$, so it lies in some cell $\mathcal{C}$ of the tiling. Then $\mathcal{W}_B(\mathcal{C}) \neq \emptyset$, so the certificate of $\mathcal{C}$ is not an emptiness certificate ((a) or (b)). It is therefore a polynomial φ with $\varphi + \varepsilon \geq h_B$ (Lemma 9.23) and $\mathbb{E}\varphi(Z_W) \leq \beta$ (by (c)), where $\beta + \varepsilon < C_5$. Lemma 9.24 gives $\mathbb{E}|Z_K| \leq \beta + \varepsilon < C_5$. □

9.7.4 The certified computation (`scripts/verify_plus.py`)

The verifier `scripts/verify_plus.py` and its library `scripts/plus_verify_lib.py` use only python-flint: `fmpq` for exact rationals and `arb` balls at 128 bits. Every inequality is decided by a comparison of balls that is certain. The certificate data are IEEE doubles, which are exact dyadic rationals and are converted exactly. τ, A, the box and cell endpoints, μ_B, cap_B and R_B are exact rationals, and C_5 is a ball containing $1.28\sqrt{2 \ln 1.25}$.

Polynomial upper bounds. For a polynomial p given by ball coefficients and an interval $[u, u']$, an upper bound for $\sup_{[u,u']} p$ is computed by branch and bound. On a piece $[m-d, m+d]$ with exact centre m, the Taylor coefficients q_k of $p(m+t)$ are computed by Horner shifts in ball arithmetic. Then $p \leq q_0 + \sum_{k \text{ odd}} |q_k| d^k + \sum_{k \geq 2 \text{ even}} \max(q_k, 0) d^k$ on the piece. Pieces are bisected while this bound exceeds the best value found by more than a tolerance. The result is the maximum of the bounds of the final pieces; the tolerance affects only the tightness. A piece bound that is not a finite ball stops the verification. This is used for S in (a) and (b), for S_R in (c) (separately on $[-A, 0]$ and $[0, \tau]$), and for each piece of $H - \varphi$ in Lemma 9.23.

Majorant data. In Lemma 9.23, n_a is chosen in floating point (about $a_1 + 12\sqrt{a_1} + 20$, likewise n_b). The probabilities π_{nm} are balls, and T is the upper end of the ball $(1 - \sum_{n \leq n_a} \mathbb{P}(N_{a_1} = n)) + (1 - \sum_{m \leq n_b} \mathbb{P}(N_{b_1} = m))$, clipped at 0. L is the double stored in the certificate (between 7.20 and 14.63), checked to be $\geq \tau a_1 + A b_1$. The kinks $-c_{nm}$ are exact rationals. The returned ε is the upper end of the largest piece bound, and $\varepsilon = 0$ if all are ≤ 0.

Boxes. The rate rectangle $[0, \frac{28}{25}] \times [0, \frac{17}{50}]$ is divided into 16×16 boxes. A box that the generator could not certify was split into four, up to four times. The box with indices (i_a, i_b) at level d is $[i_a, i_a + 1] \cdot \frac{28}{25} 2^{-4-d} \times [i_b, i_b + 1] \cdot \frac{17}{50} 2^{-4-d}$. The verifier checks that the recorded leaves tile the rectangle. Every index must lie in its grid ($0 \leq i_a, i_b < 2^{4+d}$), so every leaf lies in exactly one initial box, and each of the 256 initial boxes must contain at least one leaf. For each initial box, its leaves must be pairwise non-nested dyadic sub-squares whose areas add up to its area. Distinct non-nested dyadic squares have disjoint interiors, so their union then has full measure, and being closed it is the whole box. A leaf recorded as empty must satisfy $Q(a_1, b_1) \geq \frac{4}{5}$ or $M(a_2, b_2) < \frac{1}{2}$ in exact arithmetic.

Cells. For every other leaf, the verifier checks that the recorded cells tile R_B (quadtree leaves with indices in their grid, the same test; in this run of depth ≤ 2), and checks each cell certificate. A certificate of type 'ok' passes if φ has 17 finite coefficients (degree ≤ 16), the tail test of Lemma 9.23(iii) holds at L, and $\beta + \varepsilon < C_5$. Here ε is computed as above, the ranges $[L_j, U_j]$ ($3 \le j \le 16$) come from (a) with the certificate's (s_3, s_4), and β from (c) with the certificate's multipliers (negative entries are replaced by 0). A cell certified empty by (a), i.e. with $L_j > U_j$ for some j, passes whatever its type. A certificate of type 'empty_farkas' passes if $\Phi < 0$ in (b).

Result. The recorded run (`outputs/plus_cert/verify_v1.txt`; 2026-10-22, 22:34:20–22:34:45 UTC, 8 processes; python 3.12.3, python-flint 0.9.0) of `scripts/verify_plus.py` (md5 `c754a7305654c6635025f7e405dd98bb`) with `scripts/plus_verify_lib.py` (md5 `a7db98d4dac237f52493f6d085b97d15`) on the five files `outputs/plus_cert/certs_v1_r0.jsonl`, ..., `certs_v1_r4.jsonl` (their md5s are printed in the run) reports:

box level d	certified leaves	empty leaves
0	96	134
1	71	12
2	66	6
3	44	3
4	3	1

That is 436 leaves tiling the rectangle, 0 failures, and 1237 cell certificates: 1236 of type 'ok' and 1 of type 'empty_farkas'. The cells have depth 0 (109), 1 (536) and 2 (592). The largest certified bound $\beta + \varepsilon$ is $0.854883 < C_5 = 0.8551004\ldots$, in the box $[0.0525, 0.0700] \times [0.2072, 0.2125]$ (where V_+ is close to $\frac{1}{2}$). Boxes were split until their bound was below the generator's target $C_5 - 2 \cdot 10^{-4}$, so many bounds sit just below that target. The eight largest are all at $a_+ \le 0.175$, near $V_+ = \frac{1}{2}$ as well as further inside the region (`outputs/plus_cert/stats_v1.txt`). This proves Theorem 9.16.

An earlier run (21:47 UTC, `outputs/plus_cert/verify_v1_first.txt`) of a first version of the verifier (`verify_plus.py` md5 `0e412f55eda9b9a4c7a92e8e8def58f6`, `plus_verify_lib.py` md5 `8111a51880ffc9e29485682579cadb54`) gave the same counts. That version did not check that the box indices lie in their grid, so a missing initial box could have been replaced by an out-of-range copy of a box. Its polynomial bound also skipped a non-finite piece bound instead of stopping. The recorded version makes both checks, and its run shows that the data pass them.

Certificate files. Each line of `certs_v1_r*.jsonl` is a JSON object for one leaf box. `box` $= [l_a, i_a, l_b, i_b]$ is the box $[i_a, i_a + 1] \cdot \frac{28}{25} 2^{-l_a} \times [i_b, i_b + 1] \cdot \frac{17}{50} 2^{-l_b}$ (here $l_a = l_b = 4 + d$ at box level d), and `status` is `empty` or `ok`. An `ok` box has a list `certs` with one entry per cell. In an entry, `cell` $= [\ell, i, j]$ is the cell (i, j) of the $2^\ell \times 2^\ell$ grid on R_B, and `status` is `ok` or `empty_farkas`. An `ok` entry holds `coef` (the 17 coefficients of φ, ascending), `Lt` (L), `rmult` (for each $j = 3, \ldots, 16$ the pair (s_3, s_4) of (a) for L_j, then the pair for U_j) and `mult`, the multipliers of (c) in the order of the display there: `cell` for the four cell rows, `mcc` for the four McCormick rows and `cheb` for the two Hölder rows of a tuple α, keyed by α. An `empty_farkas` entry holds `farkas` $= (s_3, s_4)$ of (b). Every number is a double, read as an exact dyadic rational. The other keys (`t`, `worst`, `ncell`, `bound`, `lp`) are the generator's bookkeeping, and the verifier does not read them.

How the certificates were found (not part of the proof). `scripts/plus_cert.py` solves, for each box and cell, a linear program in floating point (HiGHS), on a grid of r and of the support of W. The primal is a discretised moment problem. The moment rows are written in the Chebyshev

basis $T_k(r/L)$, and columns for the Taylor coefficients of the tails at $\pm L$ are included. The duals give φ and the multipliers, and an exchange step adds violated grid points. `scripts/plus_driver.py` runs the adaptive box and cell refinement (run `plus_driver.py v1 4 4 2 4`, 21:27–21:38 UTC, log `outputs/plus_cert/log_v1.txt`; generator target $C_5 - 2 \cdot 10^{-4}$). The certificates of run v1 were produced before a repair step for narrow wells of $\varphi - H$ near $\pm L$ (`fix_wells`) was added to `plus_cert.py`. The repair lowers ε but plays no role in the verification.

Controls (not part of the proof). `scripts/verify_plus_controls.py` (`outputs/plus_cert/controls_v1.txt`) reruns all box checks with C_5 replaced by $C_5 - s$. For $s = 0, 10^{-4}, 3 \cdot 10^{-4}, 10^{-3}, 3 \cdot 10^{-3}$, respectively $0, 0, 9, 50, 187$ of the 280 non-empty boxes fail. So the certified margin of the worst boxes lies between 10^{-4} and $3 \cdot 10^{-4}$. Removing any one box record, or one cell of a box, makes the corresponding tiling test fail, and so does moving one box or cell index out of its grid.

Float self-tests (evidence only). `scripts/test_plus_verify.py` (`outputs/plus_cert/selftest_v1_r*.txt`, all pass on all five files) runs five tests.

- It compares the moment polynomials P_n ($n \le 16$) with a direct expansion for two Poisson atoms and a Gaussian (relative difference at most $3.4 \cdot 10^{-14}$).
- It compares the polynomial upper bound with dense evaluation, the exact value at the dense maximiser being below the bound.
- It compares $h_B - \varphi$ on a dense grid of $[-3L, 3L]$ with ε (never above ε).
- It draws 3000 random $W \in \mathcal{W}_B$ per file. Every κ_j lies in its certified range, and $\mathbb{E}\varphi(Z_W) \le \beta$, with smallest gap $4.57 \cdot 10^{-4}$.
- End to end, on 747 random K in the heavy region (edge laws with any $V_+ \in [\max(Q, \frac{1}{2}), \min(M, \frac{4}{5}))$), $\mathbb{E}|Z_K|$, computed in floating point by Poisson enumeration, stays below the certified bound of its cell by at least 0.0327.

The design's value (not part of the proof). For K in the heavy region, with chord rates (a_+, b_+), let $J(K)$ be the supremum of $\mathbb{E}h(Y)$ over all random variables Y whose moments up to degree 16 are those of Z_{W_0}, where $W_0 = K|_{[-A,\tau)}$ and $h(r) = \mathbb{E}|\tau(N_{a_+} - a_+) + A(N_{b_+} - b_+) + r|$. This is the value of the design itself, without boxes, cells or relaxations. One Y serves all values of the counts, as one φ does in Lemma 9.24. For the box B and the rest W of K in the proof of Lemma 9.20(ii), the bound $\beta + \varepsilon$ of the cell that contains $(\kappa_3(W), \kappa_4(W))$ is at least $J(K)$. Indeed, let Y' be the sum of Y, an independent copy of $Z_{W_1 - W_0}$ and an independent σG. Then Y' has the moments of Z_W up to degree 16, so $\mathbb{E}h_B(Y') \le \mathbb{E}\varphi(Y') + \varepsilon \le \beta + \varepsilon$ by Lemma 9.23 and (c). Also $C_B + Z_{W_1 - W_0} \stackrel{d}{=} \tau(N_{a_+} - a_+) + A(N_{b_+} - b_+)$, so $\mathbb{E}h_B(Y') = \mathbb{E}h(Y + \sigma G) \ge \mathbb{E}h(Y)$ by Jensen. The same holds if $\mathbb{E}Y^{16}$ is only bounded above by that of Z_{W_0}, as in the LPs below, because the tail test of Lemma 9.23(iii) gives $c_{16} \ge 0$.

Float searches over the heavy region (`scripts/plus_scan.py`, `outputs/far_extra/plus_scan/`, 15 runs, 8 of them stopped early; J by a discretised moment LP) found values of J up to 0.8390, at V_+ close to $\frac{4}{5}$, while the certified bounds go up to 0.8549. RQ-C's list of adversarial laws (RQ-C notes, 22:12 UTC) has five laws in the heavy region. At them J is between 0.814 and 0.836, and $\mathbb{E}|Z_K| \le \mathbb{E}h_B(Z_W) \le \beta + \varepsilon$ holds for the cell of K, with $\beta + \varepsilon - J$ between 0.018 and 0.027 (`scripts/plus_check_laws.py`,

outputs/plus_cert/check_rqc_laws.txt). The LP measures behind these values of J violate the scaled moment rows by at most $2.2 \cdot 10^{-10}$ beyond the LP tolerance, and the values change by at most 10^{-5} between the tolerances 10^{-11} and 10^{-7} (scripts/plus_lp_tol.py, outputs/plus_cert/plus_lp_tol.txt). The best law of the searches, recomputed from its printed parameters with the same check, gives 0.83893 (scripts/plus_scan_recheck.py, outputs/far_extra/plus_scan/recheck_best.txt).

Part V

The light far region

Chapter 10

The light part of the far region (computer-assisted, exact) (RQ-B, Section 13 of MAIN_RESULT.md, Section 12 of MAIN_RESULT.tex)

Source: RQ-B, `rq/MAIN_RESULT.tex` (md5 `e41938426653fabb413484e593485ccf`; title and author as in Chapter 7), Section 12, "The light part of the far region (computer-assisted, exact)", from its first paragraph to its end. The team calls it RQ-B's Section 13, the number of the same section in `rq/MAIN_RESULT.md` (md5 `b47f294573d030edf79f8022a14d0346`). The `.md` gives three passages in more detail than the `.tex`: what the exact verifier checks (its Section 13.4), the windows with Lemma D and its proof, and Lemma E with its justifications (its Section 13.5). They are transcribed into LaTeX and set in framed blocks headed "Supplement transcribed from ...".

Audit: A.39, VALID and NEW, no fix (23 October, 01:05 UTC). RQ-AUD's own exact verifier on the filed data: $7\,956 + 60 + 537$ roots covered, $8\,481 + 1\,212 + 1\,273 = 10\,966$ certificates, 0 failures, worst bound $0.8549969806 < \frac{171}{200}$. Text remarks r1, r2 and r4; r3 informational. Addendum of 02:29 UTC: RQ-REF3's counts equal RQ-AUD's; length controls 35/35 PASS.

Referee: RQ-REF3, link 4, VALID: the proof checked by hand, and all 10 966 certificates re-verified with RQ-REF3's own code. One robustness remark that does not affect validity: RQ-B's verifier does not enforce the lengths of the atom and rectangle multiplier lists; the data do not trigger this, and RQ-REF3's verifier enforces the lengths. Report `REFEREE.md`, md5 `6ac713c05dd3a1b74e71d5c959ac0ceb`, FINAL, 03:09 UTC on 23 October.

Use in the Main Theorem: Step 4, for $V_+ < \frac{1}{2}$ and $V_- < \frac{1}{2}$: Theorem 10.1 gives $\mathbb{E}|Z_K| \le \frac{171}{200} < C_5$.

Transcription: the heading of RQ-B's Section 12 becomes the chapter title, and its four subsections become Sections 10.1–10.4. Item $12.n$ of the `.tex` is item $10.n$; the tags give the names in the `.md` (Theorem 13.1, Lemmas S1–S5, C, D, E). Labels are prefixed by `ch10:`. Seven editorial footnotes: two in the text of the `.tex` (the status line of Theorem 10.1 and the items of Lemma S2 cited in the `.md` numbering) and five in the supplements (A.39's remarks r1 and r2, RQ-REF3's first robustness remark, the symbol q in (V1), and, at the end of the Lemma E supplement, the `.md` names of the lemmas with the items of Lemma S2).

Constants: $A = \frac{77}{50}$, $\theta = \frac{17}{20}$, target $\frac{171}{200} < C_5 = 0.85510045547$. For a probability measure K on $[-A, A]$ put $V_+ = K([\theta, A])$ and $V_- = K([-A, -\theta])$.

Theorem 10.1 (status: proved, computer-assisted and exact; all three cases independently re-verified; audit requested)**.** [RQ-B tex Theorem 12.1; md Theorem 13.1] *Every finitely supported probability measure K on $[-A, A]$ with $V_+ < \frac{1}{2}$ and $V_- < \frac{1}{2}$ satisfies $\mathbb{E}|Z_K| \le \frac{171}{200}$.*

Use. RQ-D's Corollary 14 (audited, A.34) reduces Conjecture S for all q to $\mathbb{E}|Z_K| \le C_5$ on the far region $F = \{V_+ < \frac{4}{5},\ V_- < \frac{4}{5}\}$. RQ-B proves the bound on $F_{\text{light}} = \{V_+ < \frac{1}{2},\ V_- < \frac{1}{2}\}$ and RQ-D on $F \cap \{V_+ \ge \frac{1}{2} \text{ or } V_- \ge \frac{1}{2}\}$.[1]

10.1 Notation

For a finitely supported finite measure K, Z_K is the mean-zero infinitely divisible law with $\mathbb{E}e^{itZ_K} = \exp\int(e^{itx} - 1 - itx)x^{-2}K(dx)$; concretely $Z_K = \sigma G + \sum_{x\neq 0} x(N_x - \lambda_x)$ with $\sigma^2 = K(\{0\})$, $\lambda_x = K(\{x\})/x^2$ and independent $G \sim N(0,1)$, $N_x \sim \text{Poisson}(\lambda_x)$. Its cumulants are $\kappa_1 = 0$ and $\kappa_j = \int x^{j-2}\,dK$ $(j \ge 2)$, and $Z_{K_1+K_2} = Z_{K_1} + Z_{K_2}$ with independent summands. $X \le_{cx} Y$ means $\mathbb{E}f(X) \le \mathbb{E}f(Y)$ for all convex f. (CO1) If $\mathbb{E}[M \mid X] = 0$ then $X \le_{cx} X + M$. (CO2) If $X \le_{cx} Y$ and Z is independent of X and of Y, then $X+Z \le_{cx} Y+Z$. $\mathbb{E}|Z_K|$ is invariant under $K \mapsto K(-dx)$.

10.2 The split chain

Lemma 10.2 (two-point spread)**.** [RQ-B tex Lemma 12.2; md Lemma S1] *Let $0 < a < b$, $W = [a,b]$, $K = K_W + K_R$ with $K_W = K(\cdot \cap W)$, $\nu = x^{-2}K_W(dx)$, $p_a = \int \frac{b-x}{b-a}\,d\nu$, $p_b = \int \frac{x-a}{b-a}\,d\nu$, and $X''(p) = a(N_a - p_a) + b(N_b - p_b)$ with independent $N_a \sim \text{Poisson}(p_a)$, $N_b \sim \text{Poisson}(p_b)$, independent of Z_{K_R}. Then $Z_K \le_{cx} X''(p) + Z_{K_R}$.*

Proof. Thin each N_x $(x \in W)$ into independent N_x^a, N_x^b with means $\lambda_x\frac{b-x}{b-a}$, $\lambda_x\frac{x-a}{b-a}$, and put $\tilde X = \sum_x(aN_x^a + bN_x^b) - \sum_x \lambda_x x$. Given (N_x), N_x^a is binomial$(N_x, \frac{b-x}{b-a})$, so $\mathbb{E}[\tilde X - Z_{K_W} \mid (N_x)] = \sum_x N_x \frac{(a-x)(b-x)+(b-x)(x-a)}{b-a} = 0$ and $Z_{K_W} \le_{cx} \tilde X$ by (CO1). Also $\sum_x N_x^a \sim \text{Poisson}(p_a)$, $\sum_x N_x^b \sim \text{Poisson}(p_b)$ are independent and $ap_a + bp_b = \sum_x \lambda_x x$, so $\tilde X \overset{d}{=} X''(p)$. Add Z_{K_R} by (CO2). □

Lemma 10.3 (window mass from the rates)**.** [RQ-B tex Lemma 12.3; md Lemma S2] *In Lemma 10.2, $K(W) = a^2p_a + b^2p_b - E_W$ with $E_W = \int(x-a)(b-x)\,d\nu$ and*

$$0 \le E_W \le \frac{(b-a)^2 p_a p_b}{p_a + p_b} \le \Big(\frac{b-a}{b+a}\Big)^2 (a^2p_a + b^2p_b).$$

Hence $K(W) \le a^2p_a + b^2p_b \le K(W)\frac{(a+b)^2}{4ab}$, and if $(p_a, p_b) \in B = [P_a, q_a] \times [P_b, q_b]$ then $V_{\text{lo}} \le K(W) \le V_{\text{hi}}$, where $\text{exc} = \frac{(b-a)^2 q_a q_b}{q_a+q_b}$, $V_{\text{lo}} = a^2P_a + b^2P_b - \text{exc}$, $V_{\text{hi}} = a^2q_a + b^2q_b$.

Proof. $a^2(b-x) + b^2(x-a) = (b-a)(x(a+b) - ab)$ and $x^2 - (x(a+b) - ab) = -(x-a)(b-x)$ give the identity. With $u = \frac{x-a}{b-a}$: $E_W = (b-a)^2\int u(1-u)\,d\nu$, $p_b = \int u\,d\nu$, $p_a = \int(1-u)\,d\nu$, and Jensen for the concave $u(1-u)$ gives the first bound. Cauchy–Schwarz, $(\frac{a^2}{x} + \frac{b^2}{y})(x+y) \ge (a+b)^2$ with $x = a^2p_a$, $y = b^2p_b$, gives the second. $\frac{p_a p_b}{p_a+p_b}$ is nondecreasing in each rate. □

Lemma 10.4 (lower corner and top-up)**.** [RQ-B tex Lemma 12.4; md Lemma S3] *In Lemma 10.2 let $K(\mathbb{R}) = 1$, $(p_a, p_b) \in B$, $P = (P_a, P_b)$ and $\mu = 1 - a^2P_a - b^2P_b + \text{exc}$. Then $X''(p) + Z_{K_R} \le_{cx} X''(P) + Z_{K'}$ with $K' = K_R + t_a\delta_a + t_b\delta_b + g\delta_0$, $t_a = a^2(p_a - P_a) \in [0, a^2(q_a - P_a)]$, $t_b = b^2(p_b - P_b) \in [0, b^2(q_b - P_b)]$, $g \ge 0$, $K'(\mathbb{R}) = \mu$.*

[1] Editorial note. RQ-D's Corollary 14 is Corollary 9.14, and RQ-D's bound on $F \cap \{V_+ \ge \frac{1}{2} \text{ or } V_- \ge \frac{1}{2}\}$ is Theorem 9.16. The status in the theorem header is that of RQ-B's text when it was written. Theorem 10.1 is audited VALID (A.39, 23 October 01:05 UTC) and refereed VALID (RQ-REF3, link 4); see Appendix B.

Proof. Poisson splitting gives $X''(p) \stackrel{d}{=} X''(P) + Z_{t_a\delta_a + t_b\delta_b}$. By Lemma 10.3, $K_R(\mathbb{R}) + t_a + t_b = 1 + E_W - a^2P_a - b^2P_b \le \mu$; the independent $Z_{g\delta_0} = \sqrt{g}\,G$ is added by (CO1). □

Corollary 10.5. [RQ-B tex Corollary 12.5; md Corollary S4] $\mathbb{E}|Z_K| \le \mathbb{E}h_P(Z_{K'})$, $h_P(r) = \sum_{i,j\ge 0} \pi_i(P_a)\pi_j(P_b)\,|r + ai + bj - aP_a - bP_b|$, $\pi_i(\lambda) = e^{-\lambda}\lambda^i/i!$.

Lemma 10.6 (a window straddling θ)**.** [RQ-B tex Lemma 12.6; md Lemma S5] *In Lemma 10.2 let $a < \theta < b < 2a$, $s = K_W([\theta, b])$, $\beta = \frac{b^2(\theta-a)}{(b-a)\theta^2}$ and $\rho = \frac{q_a(b-a)\theta^2}{b-\theta}$. If (p_a, p_b) lies in the box B of Lemma 10.3(iii),*[2] *then $\beta < 1$ and*

$$s \;\ge\; s_{\rm lo} := \max\Big(0,\; \frac{b^2P_b - \beta V_{\rm hi}}{1-\beta},\; b^2P_b - \beta\rho\Big); \qquad \textit{hence} \quad K_R([\theta, A]) = K([\theta, A]) - s \le V_+ - s_{\rm lo}.$$

Proof. $(x-a)/x^2$ has derivative $(2a-x)/x^3 > 0$ on W, so $b^2(x-a)/((b-a)x^2)$ is at most β on $[a, \theta)$ and at most 1 on $[\theta, b]$; integrating against K_W gives $b^2p_b \le \beta r + s$ with $r = K_W([a, \theta))$. On $[a, \theta)$ both factors of $(b-x)/((b-a)x^2)$ decrease, so $p_a \ge (b-\theta)r/((b-a)\theta^2)$, i.e. $r \le \rho$; also $r = K(W) - s \le V_{\rm hi} - s$. With $p_b \ge P_b$: $s \ge b^2P_b - \beta\rho$ and $s(1-\beta) \ge b^2P_b - \beta V_{\rm hi}$. Finally $(b-a)\theta^2 - b^2(\theta - a) = (b-\theta)(a(b+\theta) - b\theta) > 0$ since $a > \frac{b}{2} > \frac{b\theta}{b+\theta}$. □

10.3 Cells and certificates

A cell consists of an outer function ($h = h_P$, or $h = |\cdot|$ for light cells), a mass μ, closed cap intervals I with bounds c_I, possibly an excluded window W and atoms p with caps cap_p, and possibly a rectangle $Q = [L_3, U_3] \times [L_4, U_4]$. Its rest class $\mathcal{C}$ consists of the $K' = K_R + \sum_p t_p\delta_p + g\delta_0$ with K_R finitely supported on $[-A, A] \setminus W$, $K_R(I) \le c_I$, $0 \le t_p \le \mathrm{cap}_p$, $g \ge 0$, $K'(\mathbb{R}) = \mu$ and, if Q is given, $(\int x\,dK', \int x^2 dK') \in Q$.

Lemma 10.7 (certificate)**.** [RQ-B tex Lemma 12.7; md Lemma C] *Let D be even. Suppose (C1) $\varphi = \sum_{k\le D}\varphi_k r^k \ge \hat{h} \ge h$ on $\mathbb{R}$; (C2) $L_j \le \kappa_j(K') \le U_j$ on $\mathcal{C}$ for $3 \le j \le D$; (C3) $z \ge 0$ are multipliers of inequalities valid on $\prod_j [L_j, U_j]$ for the products $w_\alpha = \prod_{i\in\alpha}\kappa_i$ (McCormick for $w_\alpha = w_{\alpha'}\kappa_j$ with exact interval ranges, tangents $w_{(j,j)} \ge 2t\kappa_j - t^2$, and $w_{(j,j)} \le \mu\kappa_{2j-2}$); (C4) $y_0 \in \mathbb{R}$, $y_I, y_p \ge 0$, $y_3^\pm, y_4^\pm \ge 0$ with $f(x) \le y_0 + \sum_I y_I 1_I(x) + y_3x + y_4x^2$ on every closed piece between consecutive breakpoints outside W, $f(p) \le y_0 + y_p + y_3p + y_4p^2$ at the atoms and $f(0) \le y_0$ ($y_k = y_k^+ - y_k^-$). Write $\mathbb{E}\varphi(Y) = \varphi_0 + \sum_k \varphi_k m_k(\kappa)$ ($m_n = \sum_{i=2}^n \binom{n-1}{i-1}\kappa_i m_{n-i}$, $\kappa_1 = 0$, $\kappa_2 = \mu$) as $c_0 + \sum_j g_j\kappa_j + \sum_{|\alpha|\ge 2}\gamma_\alpha w_\alpha$; for the inequalities $\sum_\alpha A_{r\alpha}w_\alpha + \sum_j B_{rj}\kappa_j \le b_r$ put $\varepsilon_\alpha = \gamma_\alpha - \sum_r z_r A_{r\alpha}$, $E_w = \sum_\alpha |\varepsilon_\alpha| \max(|\mathrm{lo}_\alpha|, |\mathrm{hi}_\alpha|)$, $d_j = -\sum_r z_r B_{rj}$, $e_0 = c_0 + \sum_r z_r b_r$, $f(x) = \sum_{j=3}^D (g_j + d_j)x^{j-2}$. Then for every $K' \in \mathcal{C}$,*

$$\mathbb{E}h(Z_{K'}) \le e_0 + E_w + y_0\mu + \sum_I y_I c_I + \sum_p y_p \mathrm{cap}_p + y_3^+U_3 - y_3^-L_3 + y_4^+U_4 - y_4^-L_4.$$

Proof. $\mathbb{E}h(Y) \le \mathbb{E}\varphi(Y) \le c_0 + \sum_j g_j\kappa_j + E_w + \sum_r z_r(b_r - \sum_j B_{rj}\kappa_j) = e_0 + E_w + \int f\,dK'$; integrate (C4) against K'. □

The ranges (C2) are certified by the same x-duals with $f = \pm x^{j-2}$; a certified $L_j > U_j$ shows that the cell is empty. The exact verifier (`numerics/far_verify.py`) recomputes everything from the cell definition and the certificate (doubles, converted exactly): $\hat{h}$ from arb upper bounds of

[2] Editorial note. The items (i)–(iii) are those of RQ-B's `.md` version of Lemma S2: (i) and (ii) are the two inequalities of the chain in the last sentence of Lemma 10.3, and (iii) is the statement about the box B in the same sentence.

the Poisson probabilities with explicit tail terms; $\varphi - \hat{h} \geq 0$ on each piece and on both half-lines; the range certificates; the inequality list, E_w, f; the x-dual; and the final comparison with $\frac{171}{200}$. Polynomial nonnegativity on an interval is checked by midpoint Taylor bounds with bisection and finally an exact Sturm count.

Supplement transcribed from RQ-B's `MAIN_RESULT.md`, Section 13.4, "What the exact verifier checks (`numerics/far_verify.py`)".

Everything is recomputed from the cell definition (`cover_common.py`) and the certificate (all entries are doubles, stored in hex and converted exactly; arithmetic in Python fractions and python-flint fmpq).[3]

- (V1) $\hat{h}$: upper bounds for $\pi_i(P_a)$, $\pi_j(P_b)$, $i \leq I = P+14\sqrt{P}+25$, from arb balls (160 bits), and the tail $\sum_{(i,j) \text{ outside}} \pi_i \pi_j |r + c_{ij}| \leq \pi_T |r| + E_T$ with $P(N > I) \leq \pi_I q/(1-q)$, $q = P/(I+1)$,[4] $\mathbb{E}[N1\{N > I\}] = P(\pi_I + P(N > I))$ and $|c_{ij}| \leq ai + bj + aP_a + bP_b$. Then $\varphi - \hat{h} \geq 0$ is checked exactly on every piece between kinks and on the two half-lines.
- (V2) the range certificates: (C4) for $f = \pm x^n$, exact.
- (V3) the inequality list of (C3) is rebuilt from the certified ranges; $z \geq 0$; γ, ε, E_w, d, e_0 and f exact.
- (V4) the x-dual (C4), exact; (V5) $U \leq 171/200$.[5]
- Polynomial checks $P \geq 0$ on $[\text{lo}, \text{hi}]$: Taylor expansion at the midpoint, accepted if $c_0 - \sum_k |c_k| h^k \geq 0$ (h = half-width), rejected if $c_0 < 0$, else bisection (depth ≤ 18) and finally an exact Sturm count of the squarefree part (any root in the interval: rejected).[6] Half-lines: all coefficients ≥ 0 after the shift, else Sturm.

10.4 Decomposition and cells

Windows: $a_k = 0.3 \cdot 1.03^k$ rounded to 4 decimals, $b_k = \frac{6}{5} a_k$, while $b_k < A$, plus $[\frac{5}{6}A, A]$, and their mirror images. A window is *near* if its end nearer to 0 is below θ in absolute value; the others lie in $[\theta, A]$ or $[-A, -\theta]$.

[3] Editorial note. RQ-AUD, A.39, remark r1 (text): RQ-B's Section 13 does not state four conventions that a reader needs in order to check a certificate, namely the cap order of each case, the row order of (C3), the tangent points $t_q = L + (q+1)(U-L)/7$ (here q is an index), and a safety term ηr^D in φ, whose residuals are paid in E_w. RQ-AUD identified them from the data. Soundness does not depend on them: any $z \geq 0$ gives a valid bound, the residuals are paid in E_w, and a stored range bound that fails the exact test is replaced by a proved supremum. The text is kept as written.

[4] Editorial note. In (V1), q is a local ratio, not the bias parameter of the Introduction, and P stands for P_a or P_b.

[5] Editorial note. RQ-REF3's first robustness remark concerns this checker: `far_verify.check_linear_dual` does not enforce the lengths of the atom and rectangle multiplier lists. The hazard is not triggered by the data, since the verifiers of RQ-REF3 and of RQ-AUD enforce the lengths and accept every certificate. See Appendix B.

[6] Editorial note. RQ-AUD, A.39, remark r2 (text): the data contain exact touchings, that is, stored range inequalities that hold with equality at some point (47 910 in case 1 and 156 in case 2), and RQ-B's checker accepts every record. So either its tests are not strict there, or this sentence is inaccurate. Lemma 10.7 needs only the non-strict inequality, so this is a matter of wording. RQ-AUD's verifier replaces each such bound by its Sturm-proved supremum, and every certificate still passes.

Lemma 10.8 (three cases)**.** [RQ-B tex Lemma 12.8; md Lemma D] *For $K \in F_{\text{light}}$, after a reflection: (1) a heaviest near window $W = [a, b]$ is positive and $K(W) > \frac{1}{4}$; or (2) every near window carries $\leq \frac{1}{4}$, $V_+ \in [\frac{1}{4}, \frac{1}{2})$ and $V_- \leq V_+$; or (3) every window carries $\leq \frac{1}{4}$, $V_\pm < \frac{1}{4}$ and $\int x\, dK \geq 0$.*

Supplement transcribed from RQ-B's `MAIN_RESULT.md`, Section 13.5: the windows, Lemma D and its proof (the `.tex` version states Lemma 10.8 without proof).

Windows (`cover_common.window_family_pos`): $a_k = 0.3{\cdot}1.03^k$ rounded to 4 decimals, $b_k = \frac{6}{5}a_k$, for $k \geq 0$ while $b_k < A$, plus $[A/(6/5), A]$; the family WF consists of these and their mirror images. A window is *near* if its end nearer to 0 is below θ in absolute value ($k \leq 35$), otherwise it lies in $[\theta, A]$ or $[-A, -\theta]$.

Lemma D. Let K be in F_{light}. After a reflection, at least one of the following holds:

- case 1: some near window carries more than $1/4$; $W = [a, b]$ in WF_+ is a heaviest near window ($K(W) \geq K(W')$ for every near W' in WF) and $K(W) > 1/4$;
- case 2: every near window carries $\leq 1/4$, $V_+ \in [1/4, 1/2)$ and $V_- \leq V_+$;
- case 3: every window carries $\leq 1/4$, $V_+ < 1/4$, $V_- < 1/4$ and $\int x\, dK \geq 0$.

Proof. If some near window carries more than $1/4$, reflect so that a heaviest one is positive. Otherwise, if $\max(V_+, V_-) \geq 1/4$, reflect so that $V_+ \geq V_-$. Otherwise reflect so that $\int x\, dK \geq 0$; a window that is not near lies in $[\theta, A]$ or $[-A, -\theta]$, so it carries $\leq \max(V_+, V_-) < 1/4$. QED

Lemma 10.9 (cells, $\delta = \frac{1}{20}$)**.** [RQ-B tex Lemma 12.9; md Lemma E] *In case (1) [resp. (2)], with W [resp. $W = [\theta, A]$] and $B_{ij} = [\frac{i\delta}{a^2}, \frac{(i+1)\delta}{a^2}] \times [\frac{j\delta}{b^2}, \frac{(j+1)\delta}{b^2}] \ni (p_a, p_b)$, Lemma 10.3 gives $i + j \leq 20$ [resp. $i + j \leq 10$]; boxes with $V_{\text{hi}} \leq \frac{1}{4}$ or $V_{\text{lo}} > 1$ [resp. $V_{\text{hi}} < \frac{1}{4}$ or $V_{\text{lo}} \geq \frac{1}{2}$] contain no admissible rates. The caps of K_R are $K_R([\theta, A]) \leq \frac{1}{2} - s_{\text{lo}}$ (Lemma 10.6; $s_{\text{lo}} = 0$ unless $b > \theta$, i.e. $k \geq 30$), $K_R([-A, -\theta]) \leq \frac{1}{2}$ and $K_R(W') \leq V_{\text{hi}}$ for near $W' \neq W$ [resp. $K_R([-A, -\theta]) \leq \min(\frac{1}{2}, V_{\text{hi}})$ and $K_R(W') \leq \frac{1}{4}$ for near W']. In case (3), $m_1 = \int x\, dK < \frac{A}{4} + \frac{3\theta}{4} < \frac{6}{5}$, $m_2 = \int x^2 dK < \frac{A^2+\theta^2}{2} < \frac{31}{20}$ and $m_2 \geq m_1^2$; cells of side $\frac{1}{20}$ in (m_1, m_2). A failed box is replaced by the 4×4 subrectangles of its rest rectangle $[-Am_- - \theta(\mu - m_-),\ Am_+ + \theta(\mu - m_+)] \times [0,\ A^2 m_* + \theta^2(\mu - m_*)]$ ($m_+ = \min(\mu, c_+)$, $m_- = \min(\mu, c_-)$, $m_* = \min(\mu, c_+ + c_-)$, c_+ the cap on $[\theta, A]$ plus the atom caps at points $\geq \theta$, c_- the cap on $[-A, -\theta]$), which contains $(\int x\, dK', \int x^2 dK')$; a failed cell by its 2×2 subrectangles.*

Supplement transcribed from RQ-B's `MAIN_RESULT.md`, Section 13.5: Lemma E with its justifications, and the assembly of the proof of Theorem 10.1.

Lemma E (cells; $\delta = 1/20$). In each case, K' (respectively K) lies in the rest class of a cell that is a root of the enumeration below or a descendant of one under the subdivision rule.

- Case 1 (cells N/k/i,j; 7956 boxes): $W = [a, b] = [a_k, b_k]$, (p_a, p_b) in $B_{ij} = [i\delta/a^2, (i+1)\delta/a^2] \times [j\delta/b^2, (j+1)\delta/b^2]$ with $i = \lfloor a^2 p_a/\delta \rfloor$, $j = \lfloor b^2 p_b/\delta \rfloor$. By Lemma S2(ii) and $K(W) \leq 1$, $i + j \leq \lfloor (a+b)^2/(4ab\delta) \rfloor$ ($= 20$). Boxes with $V_{\text{hi}} \leq 1/4$ or $V_{\text{lo}} > 1$ are excluded by Lemma S2(iii). Caps on K_R: $K_R([\theta, A]) \leq 1/2 - s_{\text{lo}}$ ($V_+ < 1/2$ and Lemma S5; $s_{\text{lo}} = 0$ unless $b > \theta$, that is, $k \geq 30$), $K_R([-A, -\theta]) \leq 1/2$ ($V_- < 1/2$), and $K_R(W') \leq V_{\text{hi}}$ for every near $W' \neq W$ (W is heaviest).

- Case 2 (cells C/i,j; 60 boxes): Lemma S1 with $W = [\theta, A]$ (RQ-D's chord reduction); $V_+ = K(W) < 1/2$ gives $i + j \le \lceil v(a+b)^2/(4ab\delta) \rceil - 1 = 10$ with $v = 1/2$; boxes with $V_{\rm hi} < 1/4$ or $V_{\rm lo} \ge 1/2$ are excluded. K_R lives on $[-A, \theta)$; caps: $K_R([-A, -\theta]) \le \min(1/2, V_{\rm hi})$ ($V_- \le V_+ \le V_{\rm hi}$), $K_R(W') \le 1/4$ for every near W'.

- Case 3 (cells L/s,t; 537 cells): $m_1 = \int x\, dK \le AV_+ + \theta(1 - V_+) < A/4 + 3\theta/4 = 1.0225$ and $m_2 = \int x^2 dK \le A^2(V_+ + V_-) + \theta^2(1 - V_+ - V_-) < (A^2 + \theta^2)/2 = 1.547$, so (m_1, m_2) lies in a cell $[s/20, (s+1)/20] \times [t/20, (t+1)/20]$, $s < 24$, $t < 31$; cells with $(t+1)/20 < (s/20)^2$ are empty ($m_2 \ge m_1^2$). Caps: every window $\le 1/4$, $K([\theta, A]) \le 1/2$, $K([-A, -\theta]) \le 1/2$ (weaker than case 3 needs).

- Subdivision rule. A split-type box is replaced by the 4×4 subrectangles of its rest rectangle $R(B) = [-Am_- - \theta(\mu - m_-),\ Am_+ + \theta(\mu - m_+)] \times [0,\ A^2 m_* + \theta^2(\mu - m_*)]$, where $c_+ =$ the cap of K_R on $[\theta, A]$ plus the caps of the atoms at points $\ge \theta$, $c_- =$ the cap on $[-A, -\theta]$, $m_+ = \min(\mu, c_+)$, $m_- = \min(\mu, c_-)$, $m_* = \min(\mu, c_+ + c_-)$. $R(B)$ contains $(\int x\, dK', \int x^2 dK')$ for every K' in the rest class: the mass at points $\ge \theta$ is $\le c_+$, at points $\le -\theta$ it is $\le c_-$, every other point has $|x| < \theta$, and $K'(\mathbb{R}) = \mu$. A cell with a rectangle is replaced by its 2×2 subrectangles; a light child with $U_4 < \max(L_3, 0)^2$ is empty (Jensen) and omitted.

Assembly. By Lemma D, Corollary S4 (cases 1–2) and Lemma E, $\mathbb{E}|Z_K|$ is at most the bound U of a verified cell, or K lies in a cell certified empty; every $U \le 171/200$.[7]

---

case	roots	certificates (empty)	depth	D	largest bound
1 (near splits)	7956	8481 (5)	2	14	0.85499698
2 (chord boxes)	60	1212 (166)	5	14	0.85495525
3 (light set)	537	1273 (60)	4	18	0.85497432

Every certificate was re-verified from the stored files by the independent checker `numerics/cover_check.py`, which regenerates the required roots and the subdivision rule of Lemma 10.9 and uses only `far_verify.py`; every required root is covered and every bound is at most $\frac{171}{200}$ in exact arithmetic (the largest, at the case-1 box $k = 35$, $(i, j) = (0, 6)$, has $\frac{171}{200} - U = 3.02 \cdot 10^{-6}$). In case 1, 7922 boxes are certified at depth 0 and the other 34 by 539 rest cells at depth 1 and 20 at depth 2. Certificate files: `numerics/cover_final/`.

[7] Editorial note. In this supplement, Lemmas S1, S2, S5, C, D, E and Corollary S4 are Lemmas 10.2, 10.3, 10.6, 10.7, 10.8, 10.9 and Corollary 10.5. Items (i)–(iii) of Lemma S2 in the `.md` version are, in order, the two inequalities of the chain in the last sentence of Lemma 10.3 and the statement about the box B in the same sentence.

Appendix A

Computer-assisted steps

This appendix records, for every computer-assisted step of the proof, what the computer decides, in which arithmetic, with which programs and data files, how long the recorded runs took, and who repeated the computation independently. What is checked, and why that suffices, is stated in the chapter that uses the computation; this appendix adds no mathematics and changes no statement.

Which steps are computer-assisted

Nine theorems rest on computations:

- Theorems 1–6 of Part I (the team's MAIN-1 to MAIN-6), in Chapters 1–6; the computations are described in Sections 1.7, 2.9, 3.9, 4.9, 5.9 and 6.9;
- Theorem 9.13 (the band) and Theorem 9.16 (the heavy far region), with the computations in Sections 9.6.1 and 9.7.4;
- Theorem 10.1 (the light far region), with the certificates of Lemma 10.7, the supplement on the exact verifier that follows it, and the table at the end of Chapter 10.

RQ-D's paper also contains a computation for Theorem 9.10 (Section 9.5.1). Theorem 9.10 is not used in the proof of the Main Theorem. Chapters 7 and 8 contain no computer-assisted step; the numerical constants they use were re-checked by machine (section "Numerical constants of Parts II and III" below).

Conventions

- *Decided.* Every inequality on which a proof rests is decided either in exact rational arithmetic (by Sturm sequences, or by exact comparisons of rationals) or in interval or ball arithmetic with outward rounding (mpmath intervals, or the `arb` balls of python-flint), so that the decision is certain. Floating point is used only to find certificates and to choose subdivisions, never to decide an inequality.
- *Generators and verifiers.* The programs that search for certificates (linear programs solved in floating point by HiGHS through scipy, and other floating-point searches) are not trusted. A proof relies only on a verifier, which reads the stored certificates and re-checks every inequality. The one exception, the band computation of Theorem 9.13, is discussed in its section below.

- *md5 sums.* A sum written in full identifies the file used. A sum ending in "..." is a prefix, as quoted in the cited report.
- *Paths.* RQ-A's files are given relative to RQ-A's repository (directories `scripts/` and `outputs/`). The other files are in the team store: RQ-B's programs and certificates in `RQ-B/numerics/`, RQ-D's in `RQ-D/scripts/` and `RQ-D/outputs/`, the auditor's in `RQ-AUD/audit/`, and each referee's programs and logs in `ref/` and `logs/` of its own directory (`RQ-REF1/`, `RQ-REF2/`, `RQ-REF3/`).
- *Times* are wall-clock times of the recorded runs, with the number of cores or processes stated in the source.
- *Independence.* The three referees state that they did not read, import or run the authors' programs; RQ-REF3 adds that it did not run or trust the auditor's programs either (their statements are quoted in Appendix B). The auditor's re-verifications listed below are those that RQ-AUD's `AUDIT.md` reports as made with RQ-AUD's own code.

Overview

theorem	what the computer decides	verifier and recorded run	repeated independently by
Theorem 1.1, Section 1.7	379 six-moment cells (Sturm sequences, exact rationals); 641 quartic boxes (outward-rounded intervals, 20 969 sub-boxes); identities; exact coverage; near-dictator inequality	`verify_all.py`, parts A–E: cells 1 s, boxes 13 s; about one minute in all	RQ-AUD (A.6); RQ-REF1
Theorem 2.1, Section 2.9	784 cells; 55 515 two-coordinate boxes: 48 810 six-moment certificates, 4 835 near-circle boxes, 1 189 m-split boxes (1 669 near-sphere pieces), 681 small boxes; three-bit lemma (256 functions)	`verify_k2.py`, parts A–G: certificates 161 s; about 5 minutes on 8 cores in all	RQ-AUD (A.11); RQ-REF1
Theorem 3, Section 3.9	2 704 cells; 81 975 boxes: 57 333 six-moment certificates, 2 534 near-circle boxes, 21 232 m-split boxes (32 932 pieces), 876 small boxes; three-bit lemma	`verify_k2.py` with `RQ_K=3`, parts A–G: certificates 317 s	RQ-AUD (A.14); RQ-REF1
Theorem 4, Section 4.9	288 cells; 1 421 boxes: 1 106 vertex-certificate boxes, 302 m-split boxes (301 four-coordinate pieces), 13 near-circle boxes; 2 845 vertex-certificate sets with 16 544 vertices; three- and four-bit lemmas (256 and 65 536 functions)	`verify_k3b.py`, parts A–G: 93 s on 8 cores	RQ-AUD (A.18); RQ-REF1
Theorem 5, Section 5.9	1 268 cells; 7 261 boxes: 4 543 vertex-certificate boxes, 2 718 m-split boxes (2 533 four- and 383 five-coordinate pieces); 21 014 vertex-certificate sets with 171 488 vertices; three- and four-bit lemmas	`verify_k4.py`, parts A–G: 367 s on 8 cores	RQ-AUD (A.25, with A.20); RQ-REF2
Theorem 6, Section 6.9	861 cells; 9 166 boxes: 4 863 vertex-certificate boxes, 4 303 m-split boxes; 52 292 vertex-certificate sets with 784 616 vertices; three- and four-bit lemmas	`verify_k5.py`, parts A–G: 4 449 s on 8 cores	RQ-AUD (A.37, with A.22); RQ-REF2

theorem	what the computer decides	verifier and recorded run	repeated independently by
Theorem 9.13, Section 9.6.1	every (a, b) square of the band triangle: 1 339 certified squares, 7 874 211 leaf boxes in the (Λ, m) plane; `arb` balls, 80 bits	RQ-D, `verify_bandstar.py`: 793 s, 8 processes (22 October, 18:39:45–18:52:59 UTC)	RQ-AUD (A.34: own cover; replay of RQ-D's box-level record); RQ-REF3 (own cover)
Theorem 9.16, Section 9.7.4	436 leaf boxes tiling the rate rectangle: 156 empty, 280 certified by 1 237 cell certificates of degree 16; `fmpq` and `arb` balls at 128 bits	RQ-D, `verify_plus.py`: 25 s, 8 processes (22 October, 22:34:20–22:34:45 UTC)	RQ-AUD (A.38); RQ-REF3
Theorem 10.1, Lemma 10.7	8 553 roots in three cases, covered by 10 966 exact moment certificates of degrees 14, 14 and 18	RQ-B, `cover_check.py` with `far_verify.py`; computation complete 22 October, 23:20 UTC	RQ-AUD (A.39); RQ-REF3

Safeguards

Generation is separate from verification. Each verifier of Part I states that it shares no code with the programs that produced the certificates. The later verifiers reuse only exact helpers of the earlier ones (Sturm sequences, integer square roots, tilings, moment polynomials, cone normals, envelopes), which share no code with the generators either. RQ-D's heavy-region verifier (`verify_plus.py` with `plus_verify_lib.py`) and RQ-B's exact verifier (`far_verify.py`) read only the stored certificates; RQ-D's generator `plus_cert.py` and RQ-B's generator `far_cert.py` are not trusted. The band computation of Theorem 9.13 is the exception: `verify_bandstar.py` chooses an option and a parameter for each box in floating point and decides the box in ball arithmetic in the same run, and the recorded run kept only per-square summaries. This is RQ-REF3's second robustness remark. The theorem rests on three covers that were each checked box by box: RQ-REF3's, RQ-AUD's, and RQ-D's own run, re-done with a box-level record that RQ-AUD replayed leaf by leaf (section on the band below).

Negative tests and controls. Each paper of Part I has a negative-test script (`break_tests*.py`) that corrupts certificates and data and checks that the verifier rejects them; for Theorem 6, for example, all 799 corrupted records are rejected in 21 tests (A.37). RQ-D and RQ-B ran controls in which targets are lowered or certificates mutated, and the auditor and RQ-REF3 ran their own (below).

Independent repetition. Every computation was repeated from the text and the stored data by the auditor and by a referee, with their own programs and, as a rule, with different algorithms (for example Bernstein bounds or Arb root isolation where the authors used Sturm sequences or Taylor bounds). Their counts agree with the authors' wherever the same objects are counted.

Part I: the middle range (Theorems 1–6)

The verifiers. `verify_all.py` (Theorem 1.1) has five parts: A, symbolic identities (sympy, exact); B, exact coverage of the parameter rectangle $[1, \bar{u}_0] \times [0, 1]$; C, the six-moment cells, with its own Sturm sequences over Python `Fractions`; D, the quartic boxes, in mpmath's outward-rounded interval arithmetic (120 bits) with adaptive subdivision; E, the near-dictator inequality (exact). `verify_k2.py` (Theorem 2.1, and Theorem 3 with the environment variable `RQ_K=3`),

`verify_k3b.py` (Theorem 4), `verify_k4.py` (Theorem 5) and `verify_k5.py` (Theorem 6) have seven parts: A, symbolic identities (sympy); B, exact coverage (the one-coordinate cells tile their rectangle, and for each sign the two-coordinate boxes tile their box); C, the one-coordinate cells (own Sturm code, strict); D, the two-coordinate certificates (six-moment boxes for Theorems 2–3, vertex certificates for Theorems 4–6); E, the near-circle boxes (mpmath outward-rounded intervals, strict); F, the m-split structure and the near-sphere pieces (mpmath intervals, strict); G, the bit lemmas (exact Sturm counts, with the equality cases).

Recorded runs. The outputs are in RQ-A's `outputs/`. Each ends with the line "ALL SELECTED PARTS PASSED" or "ALL REQUESTED PARTS PASS". For Theorem 1 the outputs of parts A, C and D are stored.

theorem	output	what the run reports	time
1	`verify_all_A.txt`, `verify_all_C.txt`, `verify_all_D.txt`	A: identities and quartic closed forms; C: 379 cells re-verified exactly; D: 641 boxes re-verified in interval arithmetic (20 969 sub-boxes). The smallest certified lower bound of $\kappa_3 B_0 - 4c_4$ over the boxes is $1.77 \cdot 10^{-3}$ (Section 1.7.2).	C 1 s, D 13 s
2	`verify_k2_ABCDEFG.txt`	784 cells tile $[\frac{1553773}{1000000}, \frac{1054691}{500000}] \times [0, \frac{9}{20}]$; boxes $s = +1$: 38 631 (33 479 six-moment, 1 680 + 1 909 near-circle, 1 189 m-split, 374 small), $s = -1$: 16 884 (15 331 six-moment, 288 + 958 near-circle, 307 small); D: 49 999 certificates; E: 4 835 near-circle boxes; F: 1 189 boxes, 1 669 pieces; G: 256 functions, equality only as stated	D 161 s
3	`verify_k3_ABCDEFG.txt`	2 704 cells; boxes 69 871 ($s = +1$) and 12 104 ($s = -1$), together 81 975 (six-moment 45 720 + 11 613, near-circle 2 302 + 232, m-split 21 232, small 617 + 259); D: 78 565 certificates; E: 2 534; F: 21 232 boxes, 32 932 pieces; G: 256 functions	D 317 s
4	`verify_k3b_ABCDEFG.txt`	288 cells; boxes 941 + 480 = 1 421; D: 2 845 vertex-certificate sets, 16 544 vertices, on 1 408 boxes; E: 13; F: 302 boxes, 301 four-coordinate pieces; G: 256 functions (39 distinct polynomials) and 65 536 functions (1 630 polynomials)	93 s
5	`verify_k4_ABCDEFG.txt`	1 268 cells; boxes 6 045 + 1 216 = 7 261; D: 21 014 sets, 171 488 vertices; E: none; F: 2 718 boxes, 2 533 four- and 383 five-coordinate pieces; G: three and four bits	367 s
6	`verify_k5_ABCDEFG.txt`	861 cells; boxes 8 107 + 1 059 = 9 166; D: 52 292 sets, 784 616 vertices (9 168, 14 735, 17 399 and 10 990 with 2, 3, 4 and 5 patch parameters); E: none; F: 4 303 boxes; G: three bits strict, four bits with equality only for $\pm\mathrm{OR}_4$ at q_5	4 449 s

Data. The data of Theorem 1 are the eight cell files `outputs/cover/r1a.json`, ..., `r3b.json` and the box file `outputs/quartic_cover.json`. For Theorems 2–6 the manifests `outputs/k2_manifest.json`, `k3_manifest.json`, `k3b_manifest.json`, `k4_manifest.json` and `k5_manifest.json` list the data files, and the md5 lists `outputs/k2_MD5SUMS.txt` (117 entries), `k3_MD5SUMS.txt` (98), `k3b_MD5SUMS.txt` (37), `k4_MD5SUMS.txt` (81) and `k5_MD5SUMS.txt` (106) give their sums; each list contains the data files and the manifest. 54 of the 105 data files of Theorem 6 were computed by RQ-C with an unmodified copy of RQ-A's `scripts/` (Section 6.9); RQ-REF2 notes that this does not matter for the proof, because it verified every file from scratch.

Commands. Each chapter of Part I ends its computer section with the commands that reproduce it. Together, the verifiers are run as follows (times as stated in the papers):

```
pip install numpy scipy sympy mpmath
cd scripts
python3 verify_all.py          # Theorem 1, parts A-E, about one minute
python3 verify_k2.py           # Theorem 2, parts A-G, about 5 minutes on 8 cores
RQ_K=3 python3 verify_k2.py    # Theorem 3, parts A-G
python3 verify_k3b.py          # Theorem 4, parts A-G, about 2 minutes on 8 cores
python3 verify_k4.py           # Theorem 5, parts A-G, about 6 minutes on 8 cores
python3 verify_k5.py           # Theorem 6, parts A-G, about 75 minutes on 8 cores
```

The programs with negative tests are, for Theorem 1, `break_tests.py`; for Theorems 2 and 3, `break_tests_k2.py` (for Theorem 3 run with `RQ_K=3`); and for Theorems 4, 5 and 6, `break_tests_k3b.py`, `break_tests_k4.py` and `break_tests_k5.py`. Further, `fourbit.py`, `bitlemma_k4.py` and `bitlemma_k5.py` are generator-side checks of the bit lemmas, and `run_k3b.sh`, `run_k4.sh` and `run_k5.sh` regenerate the data (about 40 minutes with 8 jobs, 8.5 job-hours and 66 job-hours).

Independent repetition. The auditor and the referees re-did every step of Part I with their own programs, on the filed data.

theorem	RQ-AUD (own code)	referee (own code)
1	A.6: Arb root isolation for the cells (379/379), and a second method with sympy Sturm sequences (379/379); Arb intervals at 120 bits for the boxes (641/641; 75 008 sub-boxes, depth ≤ 5), hull tiled; 25 identities; negative tests; replay of RQ-A's 160 corruptions (all 120 decreases rejected; 34 of the 40 increases accepted, as the slack allows); the nine data files match. Addendum 2: $\kappa_3 B_0 - 4c_4 \geq 6.1597 \cdot 10^{-3}$ on the sample box of the appendix of Chapter 1.	RQ-REF1: exact Bernstein (de Casteljau) bounds, with the substitution $x = z/(1-z)$ for half-lines; 379/379 cells, 641/641 boxes (none needed subdivision); coverage by 769 and 669 leaves; 35/35 identities; negative tests 40/40 (boxes) and 60/60 (cells)
2	A.11: exact rationals and Arb root isolation; 117 md5s, 0 mismatches; tilings; 784/784 cells; 48 810/48 810 six-moment boxes; 4 835/4 835 near-circle; 1 189/1 189 m-split (1 669 pieces); three-bit lemma; second method with sympy Sturm sequences (83 s); negative tests	RQ-REF1: 784/784 cells, 48 810 six-moment boxes, 4 835 near-circle boxes (exact rationals), 1 189 m-split boxes (1 669 pieces), 681 small boxes, three-bit lemma; 29 s on 8 cores
3	A.14: 98 md5s; tilings; 2 704/2 704 cells; 57 333 six-moment boxes; 2 534 near-circle; 21 232 m-split (32 932 pieces); three-bit lemma; second method with sympy Sturm sequences (709 395 calls, 139 s); a planted false inequality is rejected	RQ-REF1: 2 704/2 704 cells, 81 975/81 975 boxes, 32 932 pieces; 62 s
4	A.18: 17 s on 8 cores; 37 md5s; 288/288 cells; 2 845/2 845 vertex-certificate sets (16 544 vertices); 13/13 near-circle; 302/302 m-split; bit lemmas (39 and 1 630 polynomials)	RQ-REF1: 288/288 cells, 1 421/1 421 boxes (2 845 vertex certificates, 16 544 vertices), bit lemmas; 113 s
5	A.25: part D in 2 min 6 s on 8 cores; 81 md5s; 1 268/1 268 cells; 21 014/21 014 sets (171 488 vertices); 2 718/2 718 m-split; bit lemmas (A.20); negative tests	RQ-REF2 (3 125 lines of its own code): 1 268 cells, 7 261 boxes, 21 014 sets with 171 488 vertices, 3 017 near-sphere pieces; 35 s wall clock, 274 s CPU

theorem	RQ-AUD (own code)	referee (own code)
6	A.37: 24.6 minutes on 8 cores; 106 md5s; 861/861 cells; 52 292/52 292 sets; 4 303/4 303 split trees; all corrupted records rejected; semantic test on 40 800 samples with no violation	RQ-REF2: 861 cells, 9 166 boxes, 52 292 sets with 784 616 vertices, 4 029 near-sphere pieces; 489 s wall clock, 3 894 s CPU; smallest exact margin in the vertex test $1.24 \cdot 10^{-9}$

Versions of RQ-A's programs. The md5 sums in the register below are those of the programs in RQ-A's repository when this document was assembled. By the repository's history, each recorded output was committed together with or after the last revision of its verifier, with two exceptions that do not affect the recorded parts: `verify_all_C.txt` predates a revision of `verify_all.py` that made one test of part D strict (part D was re-run with it), and `verify_k3b_ABCDEFG.txt` predates a revision of `verify_k3b.py` that changed only its docstring. No verdict depends on RQ-A's programs: the auditor and the referees used their own.

Part IV: the band (Theorem 9.13)

RQ-D's run. The verifier of RQ-D is `RQ-D/scripts/verify_bandstar.py` (md5 `b5b55ceec828f01debc6c1a422e7270f`). It decides every inequality in `arb` ball arithmetic at 80 bits, with θ, A and C_5 as balls. The recorded run (22 October, 18:39:45–18:52:59 UTC, 8 processes, 793 s; output `RQ-D/outputs/verify_bandstar.txt`, per-square log `verify_bandstar_squares.jsonl`, environment `verify_bandstar_env.txt`) certifies every square of the triangle $\{a, b \geq 0,\ a+b \leq \frac{1}{5}\}$: 351, 837, 408 and 80 squares of sides $\frac{1}{128}$ to $\frac{1}{1024}$, of which 215, 102, 20 and 0 needed refinement, so 1 339 certified squares; 14 894 034 (Λ, m) boxes were examined. The 7 874 211 leaf boxes of the certified squares are 3 114 781 infeasible boxes and boxes certified by (O1) (551 105), (O3) (2 876 016), (O4) (128 597), (O2) (1 203 286) and the slope check (426). An earlier run (18:25–18:38 UTC) of a copy that differs only in inessential details gave the same counts. Controls (`verify_bandstar_controls.py`, 60 s) and a floating-point soundness test (400 + 400 random laws) are described in Section 9.6.1.

The missing box-level record and how it was replaced. RQ-REF3 remarked that this run stores no box-level certificate (its second robustness remark). Three covers, each checked box by box, answer it.

- *RQ-REF3's cover.* `ref/band_verify.py` (md5 `18a0f70d...`) with `ref/chi.py` (`4de87131...`) and `ref/rig.py`: its own design, exact rationals (gmpy2) with outward rounding to 64 bits, 510 s on 8 processes. Squares 351, 796, 336 and 24 per level, of which 205, 84, 6 and 0 needed refinement, so 1 212 certified squares carrying 9 077 343 leaf boxes (2 051 477 infeasible; (O1) 447 902; (O2) 2 137 115; (O3) 4 105 282; (O4) 334 983; slope check 584; (O5) never needed). Coverage re-check from the per-square log; controls C1–C5 (with the target lowered by 0.0005 the origin squares fail on the Dirac curve; 15 of the 24 last-level squares along the hypotenuse fail at 0.001); self-tests of the enclosures against mpmath; semantic test on 1 500 random laws (seed 20261023), no violation.
- *RQ-AUD's cover* (A.34). `a34_bandstar_verify.py` (md5 `c69392de...`), Arb at 128 bits, 235 s on 8 cores: 1 303 squares (351/213, 829/94, 376/18, 72/0 per level), 13 083 096 boxes, 0 uncertified, smallest margin $7.9 \cdot 10^{-10}$; separate coverage check (a34e); controls (a34c: 62 of the 72 last-level squares fail at 10^{-3}); semantic and hostile tests (a34b, a34d).

- *RQ-D's record, replayed.* After RQ-REF3's report RQ-D re-ran `verify_bandstar.py` unchanged through `bandstar_record.py` and stored every leaf box with its method and parameters in `RQ-D/outputs/bandstar_cert/` (`bandstar_leaves.npz`, `record_squares.jsonl`, and six more files), with its own replay checker `bandstar_replay.py`; no proof depends on these new files. RQ-AUD replayed the record leaf by leaf with its own verifier (A.34, addendum of 23 October 04:51 UTC; checks a34f, a34g, a34h): the 1 339 squares (136, 735, 388 and 80 certified per level) cover the triangle, and all 7 874 211 leaves are certified, 7 862 263 of them with RQ-AUD's own grid of h values (161 s) and the other 11 948, in 7 squares, with a finer grid (13 s). With the target lowered by $\frac{1}{1000}$, all 80 hypotenuse squares fail. RQ-AUD concluded that the record is VALID.

Part IV: the heavy far region (Theorem 9.16)

RQ-D's run. The verifier of RQ-D consists of the program `RQ-D/scripts/verify_plus.py` (md5 `c754a7305654c6635025f7e405dd98bb`) and its library `plus_verify_lib.py` (md5 `a7db98d4dac237f52493f6d085b97d15`). It uses only python-flint: `fmpq` for exact rationals and `arb` balls at 128 bits. The recorded run (22 October, 22:34:20–22:34:45 UTC, 8 processes, Python 3.12.3, python-flint 0.9.0; output `RQ-D/outputs/plus_cert/verify_v1.txt`) on the five certificate files `certs_v1_r0.jsonl`, ..., `certs_v1_r4.jsonl` reports 436 leaves tiling the rate rectangle (certified 96, 71, 66, 44, 3 and empty 134, 12, 6, 3, 1 at levels 0–4), 0 failures, and 1 237 cell certificates (1 236 of type 'ok', 1 of type 'empty_farkas'; depths 0, 1, 2: 109, 536, 592). The largest bound is $0.854883 < C_5$, in the box $[0.0525, 0.0700] \times [0.2072, 0.2125]$. The certificates were generated by `plus_cert.py` (HiGHS linear programs) and `plus_driver.py` with target $C_5 - 2 \cdot 10^{-4}$; the generators are not trusted. An earlier verifier version (21:47 UTC) gave the same counts but lacked the grid-index check and the stop on a non-finite bound; the recorded version has both. Controls (`verify_plus_controls.py`): with the target lowered by 0, 10^{-4}, $3 \cdot 10^{-4}$, 10^{-3} and $3 \cdot 10^{-3}$, respectively 0, 0, 9, 50 and 187 of the 280 certified boxes fail.

Independent repetition. RQ-AUD (A.38): `a38_heavy_verify.py` (md5 `cdeac9f5...`), exact rationals and 200-bit Arb with Sturm-certified suprema, 70 s on 8 cores: tiling by 436 leaves, 156 empty, 280 certified with 1 237 cells, 0 failures, worst bound 0.8548832 (margin $2.17 \cdot 10^{-4}$); its bounds differ from RQ-D's by between $-9.7 \cdot 10^{-10}$ and $+1.0 \cdot 10^{-12}$; controls; semantic test on 800 laws. RQ-REF3: `ref/heavy_verify.py`, exact rationals throughout, with Bernstein subdivision for polynomial suprema, a set-partition formula for moments, its own Poisson enclosures and an exact lower bound for C_5; 19 s on 8 processes: box tiling OK (436 leaves), 280 certified and 156 empty boxes, 0 failures, 1 237 cells, worst bound 0.8548832 in the same box and cell as RQ-D's; its bounds lie below RQ-D's stored float bounds by $2 \cdot 10^{-13}$ to $1.2 \cdot 10^{-9}$. Lowering the target makes 0, 9 and 50 boxes fail at 10^{-4}, $3 \cdot 10^{-4}$ and 10^{-3}, as RQ-D reports; other negative controls are rejected.

Part V: the light far region (Theorem 10.1)

RQ-B's programs and data. In `RQ-B/numerics/`: `cover_common.py` (exact definitions), `far_verify.py` (the exact verifier), `cover_check.py` (coverage checker: it regenerates the required roots and the subdivision rule of Lemma 10.9, compares the specification of every used certificate with the expected cell, and re-verifies each certificate with `far_verify.py` only), `far_cert.py` (generator; not trusted) and `cover_driver.py` (jobs and refinement). The verifier decides in exact

rationals and `arb` balls (160 bits for the Poisson weights in (V1), truncation at $P + 14\sqrt{P} + 25$); the supplement after Lemma 10.7 describes what it checks. The certificates are `cover_final/nsplit_D14.jsonl.xz` (case 1), `chord_D14.jsonl.xz` (case 2) and `light_vl025_D18.jsonl.xz` (case 3).

Results. As the table at the end of Chapter 10 states, case 1 has 7 956 roots and 8 481 certificates (5 certified empty, maximal depth 2, degree 14, largest bound $U = 0.85499698$), case 2 has 60 roots and 1 212 certificates (166 empty, depth 5, degree 14, $U = 0.85495525$), and case 3 has 537 roots and 1 273 certificates (60 empty, depth 4, degree 18, $U = 0.85497432$): 8 553 roots and 10 966 certificates, all accepted, every root covered. In case 1, 7 922 roots are certified at depth 0 and the other 34 (13 in windows 18–29 and 21 in windows 30–35) by 539 rest cells at depth 1 and 20 at depth 2. RQ-B's `MAIN_RESULT.md` (Section 13.6) gives the reproduction commands `python3 cover_check.py chord cover_final/chord_D14.jsonl.xz NPROC` (about 5 minutes on 2 cores) and, for case 1, `nsplit cover_final/nsplit_D14.jsonl.xz` (about 8 minutes on 8 cores). Controls (`cover_controls.py`): on 40 certificates each of cases 1 and 2, every mutation is rejected, except 2 mutations in case 2 that are the identity. A semantic test (`cover_semantic.py`; 200 laws in cases 2–3 and 300 in case 1) found no violation.

The windows 30–35, computed on RQ-A's cores. RQ-B posted the job script `rqa_nsplit_k30_35.sh` (md5 `aaec54c470133f856be19903d815dc49`), and RQ-A ran it unmodified on 8 cores on 22 October, finishing at 23:09 UTC. The script checks the md5 sums of RQ-B's four programs before running (`cover_common.py 8dcd1e43...`, `cover_driver.py 97df2c94...`, `far_cert.py e29c117d...`, `far_verify.py 250b89cc...`; recorded in `MD5SUMS_used.txt`) and records the versions (Python 3.12.3, python-flint 0.9.0, scipy 1.18.1, numpy 2.5.4). Its three stages took 244 s (1 326 jobs: 1 305 certified, 21 refined), 94 s (336 child jobs: 327 certified, 5 certified empty, 4 refined) and 6 s (16 certified), giving 1 653 certificates; the largest bound is 0.854997, at N/k35/i0j6. RQ-A's cross-check (`scripts/far_job_crosscheck.py`, output `crosscheck.txt`) found that the 1 653 certificates of windows 30–35 in RQ-B's final file are byte-identical to these. The outputs are in RQ-A's `outputs/far_jobs/nsplit_k30_35/` and in the team store under `RQ-A/far_jobs/nsplit_k30_35/`. These certificates are trusted only through the verifiers: RQ-B's `cover_check.py`, and the independent verifiers below, re-checked every one of them.

Independent repetition. RQ-AUD (A.39): `a39_lib.py` (md5 `2a200134...`) and `a39_light_verify.py` (md5 `2f23a255...`), exact rationals and 200-bit Arb with RQ-AUD's own Poisson truncation $P + 14\sqrt{P} + 30$: all 10 966 certificates accepted on exactly the filed data, all $7\,956 + 60 + 537$ roots covered, 0 failures, worst bound $0.8549969806 < \frac{171}{200}$; controls 72/72; semantic tests on 6 000 random and 189 fixed laws, no violation; length controls 35/35 (addendum of 02:29 UTC). RQ-REF3: `ref/light_verify.py` regenerates the roots, caps, atoms, masses, breakpoints and the subdivision rule from Lemmas S2, S5 and E, and re-checks Lemma C for every certificate in exact rational arithmetic, with its own majorant, Bernstein subdivision and a set-partition formula for the moments (7 s, 19 s and 37 s on 8 processes). Its table: case 1, 8 476 certified, 5 empty, 0 rejected, worst $U = 0.8549969805515450$ at N/k35/i0j6 ($\frac{171}{200} - U = 3.02 \cdot 10^{-6}$); case 2, 1 046/166/0, $U = 0.8549552502410571$ at C/i1j3/q32 ($4.47 \cdot 10^{-5}$); case 3, 1 213/60/0, $U = 0.8549743150463496$ at L/s15t15 ($2.57 \cdot 10^{-5}$); every root covered. The three largest bounds agree with RQ-B's to all 16 printed digits. Negative controls (40 certificates per case) and a semantic test on 4 500 laws behave as they must. The largest bound in case 1 belongs to one of the certificates computed on RQ-A's cores.

RQ-REF3's first robustness remark. RQ-B's `far_verify.check_linear_dual` does not enforce the lengths of the atom and rectangle multiplier lists. The verifiers of RQ-REF3 and of RQ-AUD enforce them (for RQ-AUD, the length controls a39o), and every certificate passes, so the data do not trigger the hazard.

Numerical constants of Parts II and III

RQ-REF3's `ref/constants.py` (output `logs/constants.txt`: 27 PASS, 0 FAIL) checks exactly, among others: $C_5 = 0.855100455470819\ldots$; $\frac{171}{200} < C_5$ (margin $1.005 \cdot 10^{-4}$); $C_4 < C_5 < C_6$ and C_K strictly increasing for $4 \le K \le 40$; $q_6 < q_5$; $A'(q_5) = \sqrt{5q_5/\ln\frac{5}{4}} = 1.538044391650755\ldots < \frac{77}{50}$; $\sqrt{2} < \frac{77}{50}$. RQ-AUD's seam check for A.40 (`audit/chain/a40_chain_seams.py`, md5 `b4cce911...`, 24 PASS, Arb at 256 bits) checks the order of the endpoints, the ties at the ends of the bands, $C(q) \ge C_5$ on $(0, q_5]$, $A'(q_5) < \frac{77}{50}$ (J4), $\frac{171}{200} < C_5$, and $\theta = \frac{17}{20} < \theta_{\max} = 1.0062780$ (J6). The sweep a40f (79 PASS) re-checked the figures quoted in the texts of the links of Parts II, III and V.

Tight margins

RQ-REF3: "the margins are genuinely tight. They are 0 on the Dirac curve, handled at first order in rho^2 by the slope check and Lemma 12, and below 1e-3 along the hypotenuse of the band, and about 3e-6 in the light region (171/200 - U). All of these are decided exactly, so the tightness is no defect." In Part I the verifiers decide every inequality strictly where the proofs need strictness, and RQ-REF2 lists the tight exact margins of Theorems 5 and 6 among its remarks that need no fix.

Evidence that is not part of the proof

The following support the computations but carry no logical weight: the floating-point soundness tests of RQ-D's band bounds; the semantic tests of RQ-B, RQ-D, RQ-AUD and RQ-REF3, which push random laws through the proofs and compare with exact values; the controls with lowered targets; and RQ-AUD's hostile searches (A.40 addenda of 02:00, 03:57, 04:51, 05:42, 06:00 and 06:09 UTC on 23 October), which found no vector above $M(q)$ and no Kolmogorov measure violating the proved bounds, and found that at first order every perturbation of a Dirac law on the arc lowers the band bound.

Register of programs and data files

All sums were recomputed when this document was assembled (23 October 2026), in the team store for the files of RQ-B and RQ-D and in RQ-A's repository for RQ-A's. Environment of RQ-A's machine: Python 3.12.3, sympy 1.14.0, mpmath 1.3.0, numpy 2.5.4, scipy 1.18.1, python-flint 0.9.0. The verifiers were not re-run for this document.

file	md5	role
RQ-A, `scripts/` (Part I and the batch for Part V)		
`verify_all.py`	`9616edc67081ea4707eae44644abef3b`	verifier, Theorem 1
`quartic_verify.py`	`2f4323dcc2234822a23e76fcf613309e`	generator of the quartic boxes
`exactcert.py`	`54e01df25eaba2e3763f70d91f9359bb`	exact certificate helper (generator side)

file	md5	role
quartic_appendix_bounds.py	07246602e397ea70b70a36893acce2c0	checks the figures quoted in the appendix of Chapter 1
verify_k2.py	156c5e1af098a0db4d5f38723008f867	verifier, Theorems 2 and 3
verify_k3b.py	c1ccbc0559944ad230dcc44b20f7b851	verifier, Theorem 4
verify_k4.py	3bb94d3365195bcb790be286c4c52ce5	verifier, Theorem 5
verify_k5.py	498c4f43812ea1dae44314bfbb8adea0	verifier, Theorem 6
break_tests.py	4482e7fea8d231ef5272351931794c2b	negative tests, Theorem 1
break_tests_k2.py	1ecb3e02ffc47f50940df88deda5e006	negative tests, Theorems 2 and 3
break_tests_k3b.py	0b4b7902bbba1a9a9cfeb1c9ca1cc0a4	negative tests, Theorem 4
break_tests_k4.py	5655ad91febcde61e38a13d968e1a50e	negative tests, Theorem 5
break_tests_k5.py	61d3db20904801d4fef30a0e4a24ab5a	negative tests, Theorem 6
fourbit.py	7a3f745e9bd78285d12774cc21b0929f	four-bit lemma, generator side (Theorem 4)
bitlemma_k4.py	25e17494bdfdac4c710ec35d829b82f9	bit lemmas, generator side (Theorem 5)
bitlemma_k5.py	8b8f00ebbaa9e1d14d793d37a0f73051	bit lemmas, generator side (Theorem 6)
k4_kinds_check.py	38351967d22475e5929996876417d057	check of the box kinds (Theorem 5)
run_k3b.sh, run_k4.sh, run_k5.sh	d5ba7dde6f6ba658c57eb211daa953df, 63315a98fecdb506034c12998b8a2093, 6e6ee2ed3e3658a80e27bf1f2f380b54	regeneration of the data of Theorems 4–6
far_job_crosscheck.py	e0cad0aa50a0e3165775c4326777cdf8	compares the batch for windows 30–35 with RQ-B's final file
RQ-A, outputs/		
verify_all_A.txt, _C.txt, _D.txt	0399f724ff906652b3255abf4ac5f210, 287430f664208aa666c97cb8b64bdcb1, b7f4a32b81808ae71d0ff0dfef4d01c2	recorded run, Theorem 1
break_tests.txt	a5f4439868fd0bef48097b9e4ff1067b	negative tests, Theorem 1
quartic_cover.json	f528c4c3a350924d8f878d9375c58af1	641 quartic boxes
quartic_appendix_bounds.txt	0b0bfb6b483cda07d55ad8e9b7e40169	output of the check of the appendix figures
cover/r1a.json	3cf50baab1b303eadec7b2225920446c	cells, Theorem 1
cover/r1b.json	adaa33cb7073f4aa7cd15c0f353a9899	cells, Theorem 1
cover/r1c.json	b72637cdb18725601f06acb31fe770f8	cells, Theorem 1
cover/r1d.json	45ba2f8a264ec38acfd461a9c10f9c37	cells, Theorem 1
cover/r2a.json	856e58eb52b1169be1366f5440a7285a	cells, Theorem 1
cover/r2b.json	2674e008c69b51c2682ca373e001846e	cells, Theorem 1
cover/r3a.json	ece11000a1f7d27371633d5dd71892e1	cells, Theorem 1
cover/r3b.json	d91a1536ee11082f990ed9636f304ddf	cells, Theorem 1
verify_k2_ABCDEFG.txt	bc24250bddb651a6597b6b38a4e83d65	recorded run, Theorem 2
break_tests_k2.txt	d3639d37b430ed8f1b16f9840aba946c	negative tests, Theorem 2
k2_manifest.json	659b6f25fd6a18286dee08aec36635ae	data list, Theorem 2
k2_MD5SUMS.txt	c6184a11513351ac713baa4f1f487ff3	md5 list, Theorem 2 (117 entries)
verify_k3_ABCDEFG.txt	670684606a92b2f1645efa8954d3f2b8	recorded run, Theorem 3
break_tests_k3.txt	7a74cd9fcb84f8e3b557aaf5ab24c7b8	negative tests, Theorem 3
k3_manifest.json	81c2d718d0fe4b622c941a8614014a6c	data list, Theorem 3
k3_MD5SUMS.txt	613f681e46cb54101bc65817c03cedf4	md5 list, Theorem 3 (98 entries)
verify_k3b_ABCDEFG.txt	f67f5757814b193eb8533fa2b4394fe5	recorded run, Theorem 4
break_tests_k3b.txt	9e81c3f589e91ab68acf5e87aae06dd8	negative tests, Theorem 4
k3b_manifest.json	127ef15a05501afce16df6959bf0b17b	data list, Theorem 4
k3b_MD5SUMS.txt	2074adcc86771803cae8dfc0d8e44382	md5 list, Theorem 4 (37 entries)
verify_k4_ABCDEFG.txt	fc576841709fb9ca812af9c006085df8	recorded run, Theorem 5
break_tests_k4.txt	ec5b7aa9733a5b20ec9cc305eb8c31f9	negative tests, Theorem 5
k4_kinds_check.txt	974e9f25dbeda24d58c0143810548af4	box kinds, Theorem 5
bitlemma_k4.txt	e2571f3b37b6e2b10f06095b67500641	bit lemmas (generator side), Theorem 5
k4_manifest.json	e7ecde052c3cdfb8aa9ff66a4a77c4f4	data list, Theorem 5

file	md5	role
k4_MD5SUMS.txt	3a8fd36640604e59a84e541305296d46	md5 list, Theorem 5 (81 entries)
verify_k5_ABCDEFG.txt	618f03d11e540a51ccf687d18aadcc5d	recorded run, Theorem 6
break_tests_k5.txt	25a283213ec8c5e9692ae03a4e969543	negative tests, Theorem 6
bitlemma_k5.txt	3d3579c3e5f34115c4f18be23ab9e792	bit lemmas (generator side), Theorem 6
k5_manifest.json	7c92bc42548526e7fe9273b04cdefbe8	data list, Theorem 6
k5_MD5SUMS.txt	918eb069b8149fe62613baaaffca2c9d	md5 list, Theorem 6 (106 entries)
RQ-A, outputs/far_jobs/nsplit_k30_35/ (also in the team store)		
rqa_nsplit_k30_35.sh	aaec54c470133f856be19903d815dc49	RQ-B's job script, run unmodified
certs.jsonl.xz	f04f84350660538f2a14516139777122	the 1 653 certificates
results.jsonl.xz	92ff2f63a897343305efa2bd3b8c4675	job results
run.log	500d0768a3c034a74d1f1afdf1269015	log of the three stages
versions.txt	03d4d659474d4305cac589d09ec27a1d	software versions
MD5SUMS_used.txt	11fd60e0b1f182ea704eb3cf55ce3f5c	md5 sums of RQ-B's programs as run
OUTPUT_MD5SUMS.txt	f24d5815a7abc4b9538fda7b8255cf64	md5 sums of the outputs
crosscheck.txt	58e6b85ad43429461f8988f48c33acf5	1 653 of 1 653 lines byte-identical
RQ-B, RQ-B/numerics/ (Part V)		
far_verify.py	250b89cc7dc294e54f6cb10af67d6ced	exact verifier
cover_common.py	8dcd1e43eb9ce1f1f5baad0d15f0f67c	exact definitions of the cells
cover_check.py	a103517918c78086d91cee288c910b74	coverage checker
far_cert.py	e29c117d5b44010ebc605708d5064ef3	generator (not trusted)
cover_driver.py	97df2c94ce2201be971b63422192fc67	jobs and refinement
cover_controls.py	be976156b27fdd9dd281de3983055c6a	controls
cover_semantic.py	1fbbc95d55fb5492c3733d2e4f2917bc	semantic test (evidence)
cover_final/nsplit_D14.jsonl.xz	0883b5d96a037a6a4d88e64d5a4b9929	certificates, case 1
cover_final/chord_D14.jsonl.xz	3d7366f952b6d159df4f9dc5cc90b48d	certificates, case 2
cover_final/light_vl025_D18.jsonl.xz	2bbb7484a1b420a0b22dade39448c6fc	certificates, case 3
RQ-D, RQ-D/scripts/ and RQ-D/outputs/ (Part IV)		
scripts/verify_bandstar.py	b5b55ceec828f01debc6c1a422e7270f	band verifier
scripts/verify_bandstar_controls.py	7427d4c4be4ccd5d30e804360336f06f	band controls
scripts/verify_plus.py	c754a7305654c6635025f7e405dd98bb	heavy-region verifier
scripts/plus_verify_lib.py	a7db98d4dac237f52493f6d085b97d15	its library
scripts/verify_plus_controls.py	da7aa1c57b8a364901a82066e14968f0	heavy-region controls
scripts/bandstar_record.py	6fcfd2e81fafcfad3c27ca7da0422359	box-level record of the band run (after the report; not audited as a program)
scripts/bandstar_replay.py	e38a1a9e187cba0fda225ca415c91a14	RQ-D's replay checker (not audited as a program)
outputs/verify_bandstar.txt	c36c17e52bb29948ebd55119097e2732	recorded band run
outputs/verify_bandstar_squares.jsonl	73a8da42b2c739cc01713566199d7250	per-square log
outputs/verify_bandstar_env.txt	2d40d19e7d642ef687367b1c8dd9b8fa	environment of the band run
outputs/plus_cert/verify_v1.txt	4b52e38e2b67422a54da43ad752ad550	recorded heavy-region run
outputs/plus_cert/certs_v1_r0.jsonl	e23d52dd72764e98fb579ae6dba2b85c	certificates
outputs/plus_cert/certs_v1_r1.jsonl	ee9307ee5d40850c0e6199df6478b610	certificates
outputs/plus_cert/certs_v1_r2.jsonl	f5fe9a23f7ddd05ff70b7217731aa1af	certificates
outputs/plus_cert/certs_v1_r3.jsonl	6d495261e3af634ebc32ef8c7ef18c63	certificates
outputs/plus_cert/certs_v1_r4.jsonl	3033710b0d34ca792aaa15feae577299	certificates

file	md5	role
outputs/bandstar_cert/bandstar_leaves.npz	170d0ba8c98c8fbed9575f3c1525a452	box-level record (leaves)
outputs/bandstar_cert/bandstar_slope.json	353cfe2ad87153637ca05129df7ee4e8	box-level record (slope pieces)
outputs/bandstar_cert/record_squares.jsonl	8d4d2db30e96cba715bf9f1605c5f94e	box-level record (squares)
outputs/bandstar_cert/record_summary.json	2f94be6809c772ca014aa5a3a93c9aad	summary of the record
outputs/bandstar_cert/record.txt	d3ae2b0731a98170c99e7780efbd7444	log of the recording run
outputs/bandstar_cert/record_env.txt	11c9c8fd26e75b87cf0986970299833b	environment of the recording run
outputs/bandstar_cert/replay.txt	13c696a1b3f76c9a6da35e9f159cb1fa	output of RQ-D's replay
outputs/bandstar_cert/replay_selftest.txt	bcffaef62cef7da92868ad0d433d0c2f	self-test of RQ-D's replay

Appendix B

Audit and referee ledger

This appendix lists the verdicts on which the proof rests, with their identifiers, times and report files, and the remarks of the auditor and the referees. All times are UTC unless marked PT (Pacific time, UTC−7 on these dates).

Sources of this ledger

- RQ-AUD's `AUDIT.md` in the team store, read at about 08:10 UTC on 23 October (md5 `989ed72e6a6b322cce254619ce69ced0`; last entry the A.40 addendum of 07:58 UTC).
- The three referee reports, each called `REFEREE.md`: the report of RQ-REF1 has md5 `369c1cfb30e99367178317bdfdb3c494`, the report of RQ-REF2 has md5 `bd18da81cc4c1c35ccb99c07047c06ba`, and the final report of RQ-REF3 has md5 `6ac713c05dd3a1b74e71d5c959ac0ceb`.
- The coordinator's `LOCKED_NOTE.md` (md5 `0a104a410e272d775b37ca2fc353ac46`) for the reporting rule and the times of the reports, and `COMMON.md` for the claim tags.

Vocabulary

RQ-AUD rates each claim VALID, VALID WITH FIXES, INVALID or NOT YET AUDITED; a claim rated VALID WITH FIXES is re-rated after the fixes are posted. Novelty is recorded separately (NEW or KNOWN, with sources). The solvers tag claims PROVED, CONDITIONAL, NUMERICAL, CONJECTURE or FAILED (`COMMON.md`). Audit identifiers "A.n" are those of the ledger table at the top of `AUDIT.md`; each has a section with the details.

The reporting rule and how it was met

The locked note says: "Report to Paata ONLY results rated VALID by the auditor AND an independent referee." The proof was reported in three steps.

- Theorems 1–4 ($R(q)$ on $[q_4, 1-q_4]$): A.6, A.11, A.14, A.18 and RQ-REF1, VALID with no fixes; reported on 22 October at 08:38 PT (15:38 UTC).
- Theorems 5–6 ($R(q)$ on $[q_6, 1-q_6]$): A.25, A.37 and RQ-REF2, VALID with no fixes; reported at 18:05 PT (01:05 UTC on 23 October).

- The small-q chain and the composition (Conjecture S for all q): A.7a, A.10, A.26, A.28, A.30, A.32, A.34, A.38, A.39, A.40 and RQ-REF3 (FINAL, 03:09 UTC on 23 October); reported at 20:10 PT on 22 October (03:10 UTC on 23 October).

Audit verdicts on the links of the proof

audit	subject (here)	verdict, fixes and remarks	time	used in
A.6	Theorem 1.1 (RQ-A MAIN, Theorem 1)	VALID, no mathematical fix; typos f1–f2 fixed in the refereed text; f3 (appendix figure $6.2 \cdot 10^{-3} \to 6.1 \cdot 10^{-3}$, text only) applied by RQ-A at 03:04 and checked at 03:30 on 23 October	22 Oct 06:52; addenda 23 Oct 02:55, 03:30	Step 1
A.11	Theorem 2.1 (MAIN-2)	VALID, no fix	22 Oct 08:52	Step 1
A.14	Theorem 3 (MAIN-3)	VALID, no fix	22 Oct 10:37	Step 1
A.18	Theorem 4 (MAIN-4)	VALID, no fix	22 Oct 12:41	Step 1
A.20	the bit lemmas of Theorem 5	VALID, no fix	22 Oct 13:22	Step 1
A.25	Theorem 5 (MAIN-5)	VALID, no fix to the mathematics; status remarks r1–r2 applied at 17:47; addendum: RQ-A's text corrections c1–c2 are text only; r3 cosmetic (a quoted md5)	22 Oct 16:53; addendum 21:19	Step 1
A.22	the bit lemmas of Theorem 6	VALID, no fix	22 Oct 14:29	Cor. 6.2
A.37	Theorem 6 (MAIN-6)	VALID, no fix; cosmetic remark r1 on the height counts of Table 1, applied at 23:04–23:06	22 Oct 22:58; addendum 23 Oct 01:05	Cor. 6.2
A.7a	Lemma 7.5 (RQ-B C1, level-one form)	VALID WITH FIXES (a typo); the proof that C1 now cites has the fix (recorded in A.10); re-rated VALID; cosmetic r1: RQ-B's C1 cites the lemma as 2.1, its PDF numbers it 3.1	22 Oct 06:59; 23 Oct 07:48	Step 3
A.10	RQ-B's paper: A.10a Theorem 7.6; A.10c, including Proposition 7.11; Theorem 7.4	A.10a VALID; A.10c VALID as implications; Theorem 7.4 re-proved correctly (it is Stone's theorem)	22 Oct 08:11	Steps 2–3
A.26	Theorem 7.9(a)–(e) (RQ-B C19) = RQ-A U.1–U.2 (Section 7.6)	VALID, NEW; fix f1 to RQ-A's U.3 (a decimal of C_4 rounded up) posted at 16:33 and checked at 16:55; addendum 2 at 20:37	22 Oct 16:14, 16:55, 20:37	Step 3
A.28	Theorem 8.1 (RQ-C C15)	VALID, NEW, no fix	22 Oct 16:14	Step 3
A.30	Lemmas 9.1 and 9.3 (RQ-D D1–D2)	VALID; Lemma 9.3 after fix f1 ($K_S \neq 0$), posted at 17:18	22 Oct 16:14, 17:23	Step 4
A.32	Lemmas 9.2, 9.4, 9.6–9.8, Proposition 9.9, Theorem 9.10, Corollary 9.11 (D6–D12)	VALID, no fix (own verifier for Theorem 9.10: 767 boxes, 489 squares and 369 066 boxes); the theorem and the corollary are not used	22 Oct 18:17	Step 4
A.34	Lemma 9.7(c), (O1)–(O5), Lemma 9.12, Theorem 9.13, Corollaries 9.14–9.15 (D16–D20)	VALID, no mathematical fix; two cosmetic remarks; f1, a slip in a remark of Section 9.6.1 (text); the box-level record replayed, VALID; RQ-D's two figure corrections checked (a34i)	22 Oct 20:19; addenda 23 Oct 03:02, 04:51, 06:58, 07:48	Step 4
A.38	Lemmas 9.18–9.24, Theorem 9.16, Corollary 9.17 (D21–D23)	VALID, no fix; three remarks, two settled by the filing, r3 settled at 23:25 (text)	22 Oct 22:51	Step 4

audit	subject (here)	verdict, fixes and remarks	time	used in
A.39	Theorem 10.1 and Lemmas 10.2–10.9 (RQ-B F18)	VALID, NEW, no fix; text remarks r1, r2, r4; r3 informational; addendum: RQ-REF3's counts equal RQ-AUD's, length controls 35/35	23 Oct 01:05; addendum 02:29	Step 4
A.40	the composition (proof of the Main Theorem)	VALID at audit level; seam check 24 PASS; refereed VALID by RQ-REF3; addenda: hostile searches, sweep of quoted figures (79 PASS), literature re-check, freshness of the sources (a40q, a40r)	23 Oct 01:29; addenda 02:00 to 07:58	proof

Other audits cited in the text. The source papers also cite audits that the proof does not use: A.0 and A.3 (BF3's Lemma 9.4, which is Lemma 1.3 and is proved in Chapter 1); A.5 and A.5b (RQ-C's claim C6, $R_n(q)$ for $n \le 7$, cited in Chapters 2–6 for comparison; each chapter's own check is independent of it); A.7 (RQ-B's claims C1–C4, of which only A.7a is used); A.8 (RQ-C's claim C7, the limit $q \to 0$); A.9 (RQ-C's claim C11, an earlier proof on part of the range of Theorem 2.1); A.13 and A.13a (RQ-B's localisation of an infinitely divisible maximiser, cited in Chapters 8 and 9); and A.29 (RQ-C's claim C16, cited in Section 7.6). All of them are rated VALID.

The referees

RQ-REF1 (Theorems 1–4; launched at 07:15 PT on 22 October; VALID, no fixes, reported at 08:38 PT). It wrote: "I did not contact the authors or the auditor and did not use their conclusions. I read only the manuscripts and the certificate data files. I did not read, import or run any of the authors' scripts. Every verification below uses my own code (directory `ref/`), written from the manuscript text." Its remarks, none requiring a fix: Theorem 1 defines $\bar{b}$ with a ceiling where the K2/K3 papers use floor plus one (both valid); some decimals in the manuscripts' remarks are labelled numerical and unused; the attribution of Lemma 1.3 to BF3 is not needed for validity; the negative-test counts of Theorem 2 depend on the enclosures; a check $u_1 \ge 2$ in the verifier of Theorem 2 is not used by the logic; for Theorem 4, the description of the test (P4) leaves the acceptance condition implicit, the stored `mtop` is rounded up by less than 10^{-11} in 197 of the 302 `ms5` records, and the boxes extend beyond u_4 where the statement is not used.

RQ-REF2 (Theorems 5–6; launched at 16:10 PT on 22 October; report written at 01:05 UTC on 23 October; VALID, no fixes, reported at 18:05 PT). It wrote: "I did not write these results, and I did not read, import or run any of the authors' scripts." and "No fixes are required. The remarks in Section 6 are optional and change no statement or proof." It refereed `MAIN_RESULT_K4.tex` (md5 `158934d2...`) and `MAIN_RESULT_K5.tex` (md5 `5b13f960...`) with their 80 and 105 data files. Its remarks: a vestigial check $u_1 \ge 2$; unused machinery; tight exact margins; the status items "Not yet refereed" could now say "refereed VALID by RQ-REF2" (cosmetic; this is the change in the status items of the papers used here, Appendix C); the description of one test.

RQ-REF3 (the small-q chain and the composition; launched at 18:24 PT on 22 October; interim report at 01:58 UTC; FINAL at 03:09 UTC on 23 October; reported at 20:10 PT). It wrote: "Referee: RQ-REF3 (independent, hostile). I did not write any of the refereed material and did not run or trust the authors' or the auditor's code. Every computer step below is re-done with my own code in `ref/`, and every decision is an exact comparison of rationals." Its verdicts are VALID

for each link and for the whole: link 1, the reduction (Lemma 7.5, Theorem 7.6, Theorem 7.9(a)–(d) = RQ-A U.1–U.3), "by hand; constants re-checked exactly"; link 2, the localisation (Theorem 8.1); link 3, RQ-D's Sections 2–7 (Chapter 9), with the certificates of Theorem 9.16 re-verified and the computation of Theorem 9.13 re-done with its own cover; link 4, RQ-B's Section 13 (Chapter 10), with all 10 966 certificates re-verified. Overall: "This takes RQ-A MAIN-1..6 on [1 - sqrt(5/6), sqrt(5/6)] as given, as instructed." Those theorems are covered by RQ-REF1 and RQ-REF2. On circularity: "Nothing in the chain is circular. No link uses Conjecture S, RQ-D's C5 statement (R_ID = sqrt(2/e)), Theorem 10 or Corollary 11, or RQ-C's chain check, which I did not use." It read RQ-AUD's `AUDIT.md` (copy of 01:22 UTC, md5 `ee9a1bb1...`) "for orientation only". Its two robustness remarks, neither affecting validity, are discussed in Appendix A: the multiplier-list lengths in RQ-B's verifier, and the missing box-level record of RQ-D's band run.

The links of RQ-REF3 and of Table 3. RQ-REF3's link 1 covers the rows L0–L1 of Table 3, link 2 the row L2, link 3 the rows L3–L4, and link 4 the row L5; its overall verdict covers the composition.

Fixes and remarks

item	content	status in this document
A.6 f1–f2	typos in Theorem 1's paper	fixed in the refereed text
A.6 f3	the appendix of Theorem 1's paper quoted $\kappa_3 B_0 - 4c_4 \geq 6.2 \cdot 10^{-3}$ on its sample box, a nearest rounding of the certified $6.158 \cdot 10^{-3}$	corrected to $6.1 \cdot 10^{-3}$; editorial note in Chapter 1
A.7a, typo	$\sqrt{W^1} = \mathbb{E}[fL]$, not W^1, in RQ-B's C1	fixed in the proof reproduced as Lemma 7.5
A.7a r1	RQ-B's `CLAIMS.md` cites the level-one lemma as Lemma 2.1, its PDF numbers it 3.1	cosmetic; this document gives both numbers (source tags)
A.25 r1–r2, c1–c2, r3	status wording and text corrections in Theorem 5's paper; r3, a quoted md5	applied before the refereed version
A.26 f1	RQ-A's U.3 used a decimal of C_4 rounded up	applied; Section 7.6 contains the fix
A.30 f1	Lemma 9.3 needs $K_S \neq 0$	applied in RQ-D's text
A.34 f1	the range $0.4463 < \Lambda < 0.5599$ in a remark of Section 9.6.1 should end at 0.5579	corrected; editorial note
A.34, replay	the 80 last-level squares have $a + b \geq \frac{101}{512} = 0.197265625 < 0.1973$	corrected to 0.1972; editorial note
A.37 r1	height counts in Table 1 of Theorem 6's paper	applied before the refereed version
A.38 r3	a remark of RQ-D's Section 7	settled at 23:25 (text)
A.39 r1	conventions not stated in RQ-B's Section 13 (cap orders, row order of (C3), tangent points, safety term)	open, text only; editorial note in Chapter 10
A.39 r2	"any root in the interval: rejected" versus 47 910 and 156 exact touchings	open, text only; editorial note
A.39 r3	170 full certificates in empty classes; s_{lo} up to 0.9974; Lemma 10.6 is load-bearing	informational
A.39 r4	the heading of RQ-B's Section 13 (`.md`) still says that case 1 is running	open, text only; the status line of Theorem 10.1 has an editorial note
RQ-REF3, 1	RQ-B's verifier does not enforce the lengths of the multiplier lists	not triggered by the data; editorial note in Chapter 10
RQ-REF3, 2	RQ-D's band run stores no box-level certificate	answered by three covers; editorial note in Chapter 9

item	content	status in this document
RQ-REF1, RQ-REF2	remarks listed above	no fix required

Open items elsewhere in the ledger concern claims that the proof does not use (for example A.19's f1, a threshold in RQ-B's `CLAIMS.md`).

Timeline

time (UTC)	event
21 Oct, 22:40 PT	the attack starts at Paata Ivanisvili's request ("can you find R(q) for all q?")
22 Oct, 06:52	A.6: Theorem 1 VALID
08:52	A.11: Theorem 2 VALID
10:37	A.14: Theorem 3 VALID
12:41	A.18: Theorem 4 VALID
14:15	RQ-REF1 launched (07:15 PT) on Theorems 1–4
15:38	RQ-REF1: VALID, no fixes; Theorems 1–4 reported (08:38 PT)
16:14–16:55	A.26 (the reduction) and A.28 (localisation) VALID; A.26 f1 applied and checked
16:53	A.25: Theorem 5 VALID
17:23	A.30 re-rated VALID after f1
18:17	A.32 VALID
18:39–18:53	RQ-D's recorded band run (793 s)
20:19	A.34: the band theorem VALID
22:34	RQ-D's recorded heavy-region run
22:51	A.38: the heavy far region VALID
22:58	A.37: Theorem 6 VALID
23:10	RQ-REF2 launched (16:10 PT) on Theorems 5–6
23:20	RQ-B's light-region computation complete (windows 30–35 computed on RQ-A's cores, finished 23:09)
23 Oct, 01:05	A.39: the light far region VALID; RQ-REF2: VALID, no fixes; Theorems 5–6 reported (18:05 PT)
01:24	RQ-REF3 launched (18:24 PT) on the chain
01:29	A.40: the composition VALID at audit level
01:58	RQ-REF3 interim: links 1–2 and the certificates of Theorem 9.16 VALID
02:23	RQ-REF3: link 4 VALID
02:55–03:30	A.6 f3 raised, applied and checked
03:09	RQ-REF3 FINAL: links 1–4 and the whole VALID
03:10	Conjecture S for all q reported (20:10 PT)
03:02–07:58	A.34 addenda (f1; replay of RQ-D's box-level record at 04:51, VALID; corrections checked at 06:58); A.40 addenda (hostile searches, sweep of quoted figures, freshness of the sources); A.2 and A.7a re-rated VALID at 07:48

Appendix C

Transcription notes

This appendix lists every difference between this document and its sources, and the machine checks that confirm the list.

Source files

The script `scripts/build_full_proof.py` reads the following files, stops if an md5 sum differs from the one pinned in it, and also compares the team-store copies of the sources of RQ-B, RQ-C, RQ-D and RQ-REF3 with the pinned files.

source	md5 of the file used	relation to the refereed file
RQ-A, `MAIN_RESULT.tex` (Chapter 1)	`38b69350c47c472d401153eac2a270e7`	refereed `6816732f3c313392 f6b5ec547e1747f0`; differs in one line, the appendix figure (A.6 f3)
RQ-A, `MAIN_RESULT_K2.tex` (Chapter 2)	`280e80ed1839752895c6874873ec8c12`	refereed `1cb83e45df78e366 846d520996c3ea32`; differs only in the status item of the closing remarks
RQ-A, `MAIN_RESULT_K3.tex` (Chapter 3)	`00720a0c083de2020282ed4635e00c0c`	refereed `9f20afc71aadef43 fc877694bca3755c`; status item only
RQ-A, `MAIN_RESULT_K3B.tex` (Chapter 4)	`efa33947fa2293a078c7aa805b4d1ab2`	refereed `53aa11d14ea1f70b 944843aaff8de1ce`; status item only
RQ-A, `MAIN_RESULT_K4.tex` (Chapter 5)	`01d916597bedd8f9ee25a40a66f33768`	refereed `158934d2ea9f18df 4f717b169dc52292`; status item only
RQ-A, `MAIN_RESULT_K5.tex` (Chapter 6)	`bc42dd0f7e4382da9668403529a0b747`	refereed `5b13f960a228c590 3de80534ce7ba7b1`; status item only
RQ-B, `rq/MAIN_RESULT.tex` (Sections 7.1–7.5, Chapter 10)	`e41938426653fabb413484e593485ccf`	the refereed file
RQ-B, `rq/MAIN_RESULT.md` (three supplements in Chapter 10)	`b47f294573d030edf79f8022a14d0346`	the version audited in A.39; same content as the `.tex`
RQ-C, `CLAIMS.md` (Chapter 8)	`4b1e22a4fb96d0a383a1d8f5395edc06`	the refereed file

source	md5 of the file used	relation to the refereed file
RQ-D, `MAIN_RESULT.tex` (Chapter 9)	`ac0ecf4ff81feba53f6b8d8567a35a3b`	refereed `212c6f230b7bd8b8 ef0c377b21f7c937`; differs in two figures of Section 9.6.1 (lines 617 and 652)
RQ-A, `CLAIMS.md` (Section 7.6)	`67c3f27be651b187a3f5889ebcaa7827`	the text of U.1–U.3 is byte-identical to the audited version `3a8a0c64...` (RQ-AUD, check a40r)
RQ-REF3, `REFEREE.md` (cited)	`6ac713c05dd3a1b74e71d5c959ac0ceb`	the FINAL report

The refereed versions of RQ-A's papers are read from commit `6ecd564` of RQ-A's repository, and the refereed version of RQ-D's paper is kept as `full_proof/sources/RQD_MAIN_RESULT_refereed.tex`. RQ-REF2's remark 4 asked for exactly the change in the status items, and RQ-AUD checked the corrected figures of RQ-D's paper (A.34, check a34i) and wrote that this file "is the refereed 212c6f23… with the two corrected figures, so it is the version to quote in FULL_PROOF.pdf".

Mechanical changes

- Every `\label`, `\ref`, `\eqref` and `\pageref` of a source carries the prefix of its chapter (`ch01:` to `ch10:`).
- The title of each whole paper becomes the chapter title, and its abstract becomes a quoted block headed "Abstract of the source paper". The preambles are replaced by one common preamble; the sources define no macro in two different ways.
- Sections become sections of the chapter (Section n of a paper of Chapters 1–6 or 9 is Section $c.n$), and the four subsections of RQ-B's Section 12 become Sections 10.1–10.4.
- One theorem counter per chapter is used: in Chapters 1–6 and 9 item n of the source is item $c.n$; in Chapter 7 the items are numbered in order; in Chapter 10 item $12.n$ of the source is item $10.n$. Theorems 3–6 keep their names.
- The appendix of Theorem 1's paper ("A sample certificate") becomes an unnumbered section, since this document has its own appendices.

The editorial apparatus

Editorial material is set in sans-serif: the source box at the head of each chapter, 26 footnotes headed "Editorial note", 22 bracketed source tags, 5 omission notes "[Not reproduced here: …]", and 3 framed supplements. The editorial notes are distributed as follows: Chapter 1, 2; Chapter 7, 9; Chapter 8, 5; Chapter 9, 3; Chapter 10, 7.

no.	place	content
1	Ch. 1, proof of Theorem 1.1	"Section 2" of the source is Section 1.2; the reference is kept
2	Ch. 1, appendix of the source	the refereed figure $6.2 \cdot 10^{-3}$ and its correction (A.6 f3); the proof does not use the figure
3	Ch. 7, Remark 7.8	$q_0 = 1 - 1/\sqrt{2}$, which is q_2 here
4	Ch. 7, Remark 7.10, item (4)	the status of $\mathrm{ID}^*(C)$ in RQ-B's text; the Claim in the proof of the Main Theorem proves the instance needed
5	Ch. 7, Remark 7.10	RQ-B's Remark 9.7 and Section 11, written out as text (not reproduced)

no.	place	content
6	Ch. 7, proof of Proposition 7.11	RQ-B's Theorem 6.1, written out as text; the two displays of its proof, which hold for every q and do not use C5
7	Section 7.6, U.1	RQ-B's Theorem 3.4 is Theorem 7.9; RQ-C's C16 (A.29) is not reproduced; $\theta = \frac{17}{20} < \theta_{\max}$ (A.40, J6)
8	Section 7.6, proof of U.1	RQ-B's Lemma 2.1, Theorem 3 and "equal coefficients" are Lemma 7.5, Theorem 7.6 and Theorem 7.4
9	Section 7.6, proof of U.1	the audit of RQ-B's Theorem 3 is A.10a; the history of A.7 and A.7a
10	Section 7.6, U.3	MAIN-1 to MAIN-6 are Theorems 1–6; the Main Theorem uses the case "With MAIN-5"
11	Section 7.6, after U.3	RQ-B's Theorem 4 is not reproduced; the band lemma is Theorem 9.13; the far region is Chapter 10 and Theorem 9.16
12	Ch. 8, introduction	RQ-B's Lemma 8.2 and Proposition 8.3 are not reproduced and not used
13	Ch. 8, Theorem 8.1(f)	the closed form $A'(q_5) = \sqrt{5q_5/\ln\frac{5}{4}}$, checked by A.40 (J4) and RQ-REF3
14	Ch. 8, Theorem 8.1	A.40's display remark on the figures 1.538 and 1.576; RQ-B's Theorem 8.5 is not used
15	Ch. 8, proof of (d)	the meaning of L^- and L^+
16	Ch. 8, proof of (f)	the first inequality is Theorem 7.9(a); the identities are Theorem 7.9(b)
17	Section 9.6.1, list of output files	RQ-REF3's second robustness remark and its resolution
18	Section 9.6.1, slope check	the refereed figure 0.5599, corrected to 0.5579 (A.34 f1)
19	Section 9.6.1, controls	the refereed figure 0.1973, corrected to 0.1972
20	Ch. 10, Theorem 10.1	RQ-D's Corollary 14 and heavy-region bound; the status line; audited and refereed VALID
21	Ch. 10, Lemma 10.6	items (i)–(iii) of Lemma S2 in RQ-B's `.md`
22	Ch. 10, supplement on the verifier	A.39, remark r1 (unstated conventions)
23	same supplement, (V1)	q is a local ratio there
24	same supplement	RQ-REF3's first robustness remark
25	same supplement	A.39, remark r2 (exact touchings)
26	Ch. 10, end of the Lemma E supplement	the `.md` names of the lemmas and the items of Lemma S2

Source tags. Each tag gives the number of an item in RQ-B's `.tex` and, where it differs, in its `.md`. In Chapter 7 (13 tags): Section 1 (without the summary), Definition 1.1, Conjectures 1.2 and 1.3, Theorem 2.1 (md Theorem 1), Lemma 3.1 (md 2.1), Theorem 4.1 (md 3), Remarks 4.2 and 4.3 (md 3.2, 3.3), Theorem 4.4 (md 3.4), Remark 4.5 (md "Remarks on Theorem 3.4"), Section 6 (Proposition 6.2 only) and Proposition 6.2 (md 5.1). In Chapter 10 (9 tags): Theorem 12.1 (md 13.1), Lemmas 12.2–12.4 (md S1–S3), Corollary 12.5 (md S4), Lemmas 12.6–12.9 (md S5, C, D, E).

Omission notes. All five are in Chapter 7: the summary paragraph of RQ-B's Section 1; Remark 2.2; Theorem 2.3 (md Theorem 1.2) with its proof and Remark 2.4; Section 5 and Theorem 6.1 with the paragraph after it; Sections 7–11 and 13–14. None of these is used by the proof.

Supplements. Three passages of RQ-B's `MAIN_RESULT.md` that are more detailed than the `.tex` are transcribed into Chapter 10: Section 13.4 (what the exact verifier checks), the windows with Lemma D and its proof (Section 13.5), and Lemma E with its justifications and the assembly of the proof (Section 13.5).

Edits to source text

The build script applies 35 edits, each to a text that occurs exactly once in its source: 3 in Theorem 1's paper, 13 in the excerpts of RQ-B's paper in Chapter 7, 3 in RQ-D's paper and 16 in RQ-B's Section 12 (Chapter 10). Thirty-two of them only insert editorial material: an editorial note, a source tag, the label of Definition 7.1, or a marker that is replaced by a supplement. Deleting the insertion gives back the source text. The other three rewrite source text:

- the heading of the appendix of Theorem 1's paper, which becomes an unnumbered section;
- in Remark 7.10, the references to RQ-B's labels `rem:slicelimits` and `sec:fail` become "Remark 9.7 and Section 11 of RQ-B's paper";
- in the proof of Proposition 7.11, the reference to RQ-B's label `thm:cond` becomes "Theorem 6.1 of RQ-B's paper".

The numbers in the last two are those that RQ-B's own compiled paper prints for these labels, and the words "of RQ-B's paper" are editorial (editorial notes 5 and 6).

Plain-text sources

RQ-C's claim C15 (Chapter 8), RQ-A's U.1–U.3 (Section 7.6) and the three supplements are plain text in their sources. They were transcribed into LaTeX symbol by symbol: ASCII and Unicode formulas became mathematics, emphasis became italics or bold as in the source, and lists became paragraphs or lists. No word was changed except where an editorial note says so. The proofs in C15 and U.1 are set in proof environments. Check 7 below compares the sequence of numerals of each source passage with that of its transcription.

Machine checks

`scripts/check_full_proof.py` makes eight checks; the document is released only if all of them pass.

1. Every pinned source has its listed md5 sum, and so does its copy in the team store.
2. `FULL_PROOF.tex` is byte for byte what the build script assembles from the pinned sources and the hand-written parts in `full_proof/`.
3. Each of the 13 source blocks (six papers of RQ-A, six excerpts of RQ-B's paper, RQ-D's paper) is turned back into source text: the supplements are replaced by their markers, the edits are reverted, the chapter prefixes are removed, and the sections of Chapter 10 become subsections again. The result is identical to the body of the source paper, or, for RQ-B's paper, occurs exactly once in it; the six excerpts are disjoint and in source order.
4. Every edit either only inserts editorial material or is one of the three listed rewrites.
5. The apparatus has the stated size: 26 editorial notes (2, 9, 5, 3, 7 in Chapters 1, 7, 8, 9, 10), 22 source tags (13 and 9 in Chapters 7 and 10), 5 omission notes and 3 supplements, and none in the front matter or the appendices.

6. RQ-B's paper is compiled, and every source tag on a labelled item (18 of them) gives the number of its label in RQ-B's `.aux`; so do the three rewritten references.

7. For each plain-text source the sequence of numerals of the source passage equals that of the transcription (311 numerals for C15, 118 for U.1–U.3, 26, 37 and 109 for the three supplements).

8. The refereed versions have their refereed md5 sums, and the sources used differ from them only as stated above: Theorem 1's paper in one line (the figure $6.2 \cdot 10^{-3} \to 6.1 \cdot 10^{-3}$), the other papers of RQ-A only inside their status items, and RQ-D's paper only in lines 617 ($0.5599 \to 0.5579$) and 652 ($0.1973 \to 0.1972$).

How this document is built

In RQ-A's repository, `python3 scripts/build_full_proof.py` writes `FULL_PROOF.tex`, checks that no label is defined twice and that no reference or citation is undefined, and compiles it with pdflatex until the cross-references are stable; it stops if the log reports an undefined or multiply defined reference. `python3 scripts/check_full_proof.py` then runs the eight checks above. The hand-written parts (preamble, front matter, chapter source boxes, Chapter 8, Section 7.6, the supplements and these appendices) are in `full_proof/`, and the pinned copies of the other teams' files in `full_proof/sources/`.

Appendix D

Concordances

The sources cite each other by file name, team name, claim identifier or audit identifier, and these citations are kept as written. The tables below translate them into the numbering of this document. Within a chapter, cross-references are live; between chapters, the source boxes and the editorial notes give the translation.

RQ-A's papers and claims

file, team name	statement	here	audit	referee
`MAIN_RESULT`, MAIN, "Theorem 1"	$R = 2\tau$ exactly on $[q_2, 1-q_2]$, with the extremisers	Chapter 1, Theorem 1.1	A.6	RQ-REF1
`MAIN_RESULT_K2`, MAIN-2, "Theorem 2"	$R = 2\sqrt{2}\,\hat{q}\tau$ on $[q_3, q_2]$ and the mirror	Chapter 2, Theorem 2.1	A.11	RQ-REF1
`MAIN_RESULT_K3`, MAIN-3, "Theorem 3"	$R = 2\sqrt{3}\,\hat{q}^2\tau$ on $[q_L, q_3]$ and the mirror	Chapter 3	A.14	RQ-REF1
`MAIN_RESULT_K3B`, MAIN-4, "Theorem 4"	$R = 2\sqrt{3}\,\hat{q}^2\tau$ on $[q_4, q_L]$ and the mirror	Chapter 4	A.18	RQ-REF1
`MAIN_RESULT_K4`, MAIN-5, "Theorem 5"	$R = 4\hat{q}^3\tau$ on $[q_5, q_4]$ and the mirror; Corollary 5.2: $R = M$ on $[q_5, 1-q_5]$	Chapter 5	A.25, A.20	RQ-REF2
`MAIN_RESULT_K5`, MAIN-6, "Theorem 6"	$R = 2\sqrt{5}\,\hat{q}^4\tau$ on $[q_6, q_5]$ and the mirror; Corollary 6.2: $R = M$ on $[q_6, 1-q_6]$	Chapter 6	A.37, A.22	RQ-REF2
`CLAIMS.md`, U.1–U.3	the reduction to $\mathrm{ID}^*(C)$; the constants C_K; the corollaries	Section 7.6	A.26	RQ-REF3, link 1

RQ-B's paper

RQ-B's `MAIN_RESULT.md` and `MAIN_RESULT.tex` have the same content with different numbering: the `.md`'s Sections 1–10 are the `.tex`'s Sections 2–11, and its Section 13 is the `.tex`'s Section 12. The team cites RQ-B's results by the `.md` numbers. The source tags of this document give both numbers. A dash in the table means that the `.md` has no numbered counterpart.

RQ-B `.tex`	RQ-B `.md`, claim	here	audit
Definition 1.1	—	Definition 7.1	
Conjecture 1.2 (C0)	—	Conjecture 7.2	
Conjecture 1.3 (C5)	—	Conjecture 7.3 (not used)	

RQ-B `.tex`	RQ-B `.md`, claim	here	audit
Theorem 2.1	Theorem 1	Theorem 7.4	A.10
Theorem 2.3	Theorem 1.2, claim C20	not reproduced	A.27
Lemma 3.1	Lemma 2.1, claim C1	Lemma 7.5	A.7a
Theorem 4.1	Theorem 3, claim C6	Theorem 7.6	A.10a
Remarks 4.2, 4.3	Remarks 3.2, 3.3	Remarks 7.7 and 7.8	A.15 (Remark 4.3)
Theorem 4.4	Theorem 3.4, claim C19	Theorem 7.9	A.26
Remark 4.5	"Remarks on Theorem 3.4"	Remark 7.10	
Theorem 5.1	Theorem 4, claim C7	not reproduced	A.10b
Theorem 6.1	Theorem 5, claim C8	not reproduced	A.10c
Proposition 6.2	Proposition 5.1	Proposition 7.11	A.10c
Lemma 9.2, Proposition 9.3	Lemma 8.2, Proposition 8.3, claim C11	not reproduced	A.13a
Theorem 9.6	Theorem 8.5, claim C18	not reproduced	A.23
Theorem 12.1	Theorem 13.1, claim F18	Theorem 10.1	A.39
Lemmas 12.2–12.4	Lemmas S1–S3	Lemmas 10.2–10.4	A.39
Corollary 12.5	Corollary S4	Corollary 10.5	A.39
Lemma 12.6	Lemma S5	Lemma 10.6	A.39
Lemmas 12.7–12.9	Lemmas C, D, E	Lemmas 10.7–10.9	A.39

RQ-D's paper

RQ-D's paper is reproduced whole in Chapter 9, and its Lemma, Theorem or Corollary n is item 9.n here. Its claims and audits are as follows.

claims	items of RQ-D's paper	here	audit
D1–D2	Lemma 1 (flip formula), Lemma 3 (OR-region identity)	Lemmas 9.1, 9.3	A.30
D6–D12	Lemmas 2, 4, 6–8, Proposition 9, Theorem 10, Corollary 11	Lemmas 9.2, 9.4, 9.6–9.8, Proposition 9.9, Theorem 9.10, Corollary 9.11	A.32
D16–D20	Lemma 7(c), options (O1)–(O5), Lemma 12, Theorem 13, Corollaries 14–15	Lemma 9.7(c), Section 9.6, Lemma 9.12, Theorem 9.13, Corollaries 9.14, 9.15	A.34
D21–D23	Section 7: Lemmas 18–24, Theorem 16, Corollary 17	Lemmas 9.18–9.24, Theorem 9.16, Corollary 9.17	A.38

Remark 5 of RQ-D's paper is Remark 9.5. The team's names "band lemma", "Theorem 13" and "T1" refer to Theorem 9.13; "Theorem 16" and "F_heavy" to Theorem 9.16; "Theorem 13.1" and "F_light" to Theorem 10.1.

RQ-C's claim C15

RQ-C's claim C15 in its `CLAIMS.md` is Theorem 8.1, items (a)–(g) in the order of the source (audit A.28; RQ-REF3, link 2).

RQ-REF3's links and this document

link	what RQ-REF3 refereed	here
1	RQ-B Lemma 2.1, Theorem 3, Theorem 3.4(a)–(d) = RQ-A U.1–U.3	Lemma 7.5, Theorems 7.6, 7.9, Section 7.6; rows L0–L1 of Table 3
2	RQ-C C15	Theorem 8.1; row L2
3	RQ-D Sections 2–7: Theorem 13, Corollaries 14–15, Theorem 16, Corollary 17	Chapter 9; rows L3–L4
4	RQ-B Section 13: Theorem 13.1, Lemmas S1–S5, C, D, E	Chapter 10; row L5
all	Conjecture S for all q (with MAIN-1 to MAIN-6 as given)	the proof of the Main Theorem (page xiii)

References

[BF3] BF3 (a team of AI agents), "List-decoding thresholds of approximate polymorphisms: $s_g^{\mathrm{L}} < s_g^{\mathrm{U}}$, $s_g < s_g^{\mathrm{U}}$, an exact characterisation of s_g, and when s_g is nontrivial", report of a 24-hour research attack on Open Questions 5–6 of Chase–Filmus–Minzer–Mossel–Saurabh, 22 October 2026, 76 pp.; supplied as `BF3_approx_polymorphisms_final.pdf` (md5 `dfabb62258613f2fd0f2fb0218954c5d`).

[ILvHV] P. Ivanisvili, D. Li, R. van Handel, A. Volberg, "Improving constant in end-point Poincaré inequality on Hamming cube", arXiv:1811.05584, 2018.

[IS] P. Ivanisvili, Y. Stone, "Sharpening the gap between L^1 and L^2 norms", arXiv:2407.04835, 2024.

[St] Y. Stone, "The Poincaré inequality on the Hamming cube for vector-valued functions", PhD thesis, University of California, Irvine, 2025 (eScholarship 2wv0w7cz). [The thesis could not be downloaded where this document was assembled (HTTP 403). The citation of its Theorem 4.3.1 follows RQ-C's `CLAIMS.md` (claim C2, "Equal coefficients: Stone's Thm 4.3.1 reproduced") and RQ-AUD's `AUDIT.md` (among others A.14 and A.27).]