A SHARP REVERSE KHINCHIN-TYPE INEQUALITY FOR BIASED BITS: THE OPTIMAL CONSTANT $R(q)$ FOR EVERY $q \in (0,1)$

PAATA IVANISVILI
Department of Mathematics, University of California, Irvine
pivanisv@uci.edu

This proof was generated on October 22, 2026, by Grok Bot using Cursor's agents, guided by several prompts from Paata Ivanisvili

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 $R(q)$ be the best constant in the inequality $\mathbb{E}|\sum_i \alpha_i \chi_i| \le R(q)\,\|\alpha\|_2$. We prove that for every $q \in (0,1)$

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

and that the supremum is attained by equal coefficients on $k = \lfloor 1/(p(2-p)) \rfloor$ coordinates, $p = \min(q, 1-q)$. On $[1-\sqrt{5/6}, \sqrt{5/6}]$ we also determine all extremisers. On this middle range the inequality is proved one regime of k at a time ($k = 1, \dots, 5$): the largest coefficients are split off, and the remainder is controlled by polynomial certificates whose expectations depend only on finitely many moments; the extremisers are handled by separate near-sphere arguments and exact bit lemmas. For $q \le 1 - 2/\sqrt{5}$ (and, by symmetry, $q \ge 2/\sqrt{5}$) a Poissonisation argument reduces the problem to one q-free inequality for centred infinitely divisible laws, which we prove using a localisation of maximisers, a comparison lemma for stop-loss terms near the Dirac laws, and exact moment certificates elsewhere. The finitely many inequalities that remain are decided by computer in exact rational arithmetic or in outward-rounded interval and ball arithmetic.

CONTENTS

1. Introduction 3
1.1. The problem 3
1.2. The main theorem 3
1.3. History 6
1.4. Use of earlier work 6
1.5. The strategy 7
1.6. Computer assistance and organisation 8
2. Notation and conventions 8
3. Structure of the proof and proof of the Main Theorem 9
3.1. Which result covers which values of q 9
3.2. How the small-q chain fits together 10
3.3. Proof of the Main Theorem 10
4. The middle range: common tools 11
4.1. Symmetry and parametrisation 11
4.2. Equal coefficients 12
4.3. The one-coordinate identity 13
4.4. Moments of the remainder 13
4.5. Moment certificates: the objective bounds 14
4.6. Cells: the one-coordinate route 16
4.7. Two coordinates, bits, and the OR region 17
4.8. Box certificates 19

Date: October 2026.

4.9. Vertex certificates 20
4.10. Near the extremisers: tail bound, near-circle and near-sphere bounds 23
4.11. m-split boxes for $k = 2, 3$ 25
5. The central range: $R(q) = 2\sqrt{q(1-q)}$ if and only if $q_2 \le q \le 1 - q_2$ 26
5.1. Six-moment cells 26
5.2. The quartic two-extremiser certificate 26
5.3. The near-dictator range 28
5.4. The certified data 29
5.5. Proof of Theorem 5.1 30
6. The regime $k = 2$: $R(q) = 2\sqrt{2}\,(1-q)\sqrt{q(1-q)}$ for $q_3 \le q \le q_2$ 30
7. The regime $k = 3$, upper part: $R(q) = 2\sqrt{3}\,(1-q)^2\sqrt{q(1-q)}$ for $q_L \le q \le q_3$ 32
8. The regime $k = 3$, lower part: $R(q) = 2\sqrt{3}\,(1-q)^2\sqrt{q(1-q)}$ for $q_4 \le q \le q_L$ 34
8.1. Pieces of type TC, SG and TCS 36
8.2. Certified data and proof 37
9. The regime $k = 4$: $R(q) = 4(1-q)^3\sqrt{q(1-q)}$ exactly for $q_5 \le q \le q_4$ 38
9.1. The m-split for $k = 4$ 40
9.2. Certified data and proof 41
10. The regime $k = 5$: $R(q) = 2\sqrt{5}\,(1-q)^4\sqrt{q(1-q)}$ exactly for $q_6 \le q \le q_5$ 43
10.1. The m-split for $k = 5$: split nodes 44
10.2. Certified data and proof 46
11. Poissonisation: the reduction of $(0, q_5]$ to a q-free inequality 47
11.1. Setting 47
11.2. Level-one form 48
11.3. Poissonisation 48
11.4. Size of the window 49
12. Localisation of maximisers at finite q 50
13. The band around the Dirac laws 51
13.1. Setting 51
13.2. Exact identities 52
13.3. A comparison lemma for stop-loss terms 53
13.4. The jump law and the band bound 54
13.5. The band lemma at $\theta = \frac{17}{20}$, $A = \frac{77}{50}$ 55
13.6. The certified band computation 56
14. The heavy part of the far region 58
14.1. Chord reduction of the positive edge 58
14.2. Reduction to a box of chord rates 59
14.3. The rest: moments, linear functionals, and the certificate inequalities 60
14.4. The certified heavy-region data and the proof 61
15. The light part of the far region 62
15.1. Notation 62
15.2. The split chain 63
15.3. Cells and certificates 64
15.4. Decomposition and cells 64
16. Computer-assisted components 66
16.1. Conventions 66
16.2. Proof method of every numbered statement 67
16.3. The computer-assisted statements 69
16.4. Code and data sizes 72
16.5. Verifications re-run for this paper 72

References 74
Disclosure 74

1. Introduction

1.1. **The problem.** 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

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

the best constant in the reverse Khinchin-type inequality $\mathbb{E}|\sum_i \alpha_i \chi_i| \le R(q)\|\alpha\|_2$. Cauchy–Schwarz gives $R(q) \le 1$, with $R(\frac{1}{2}) = 1$; replacing χ by $-\chi$ gives $R(q) = R(1-q)$ (Lemma 4.1); and one coordinate gives $R(q) \ge 2\tau$. If $q \le \frac{1}{2}$ 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 4.2).

1.2. **The main theorem.**

Theorem 1.1 (Main Theorem)**.** [computer-assisted, see Sec. 16] *For every $q \in (0,1)$,*

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

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 $q_k := 1 - \sqrt{(k-1)/k}$ ($k \ge 2$), 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. Thus

$$R(q) = \begin{cases} 2\tau & q \in [q_2, \frac{1}{2}], \quad q_2 = 1 - \frac{1}{\sqrt{2}} = 0.2928\dots, \\ 2\sqrt{2}\,(1-q)\tau & q \in [q_3, q_2], \quad q_3 = 1 - \sqrt{2/3} = 0.1835\dots, \\ 2\sqrt{3}\,(1-q)^2\tau & q \in [q_4, q_3], \quad q_4 = 1 - \frac{\sqrt{3}}{2} = 0.1339\dots, \\ 4\,(1-q)^3\tau & q \in [q_5, q_4], \quad q_5 = 1 - \frac{2}{\sqrt{5}} = 0.1055\dots, \\ 2\sqrt{k}\,(1-q)^{k-1}\tau & q \in [q_{k+1}, q_k], \ k \ge 5, \end{cases}$$

and $R(1-q) = R(q)$. The theorem holds on the whole range $q \in (0,1)$; as $q \to 0$ (or $q \to 1$), $R(q) \to \sqrt{2/e} = 0.85776\dots$ (by (S) and Theorem 4.2). Figure 1 shows the structure of the proof, and Figure 2 shows $R(q)$, computed from (S), with each range of q shaded by the theorem that proves it. The range $(0, q_5]$ is not subdivided: Sections 11 and 12 reduce this whole range to one q-free claim about measures K, and Sections 13, 14 and 15 prove the claim for three classes of K (Figure 2(d)), so all three are used at every $q \in (0, q_5]$.

Remark 1.2 (an equivalent Boolean form). [computer-assisted, see Sec. 16] By Lemma 11.2, $R(q)^2 = 4q(1-q)\sup_f D(f)$, where f runs over all functions $\{0,1\}^n \to [0,1]$ ($n \ge 1$), the cube carries the

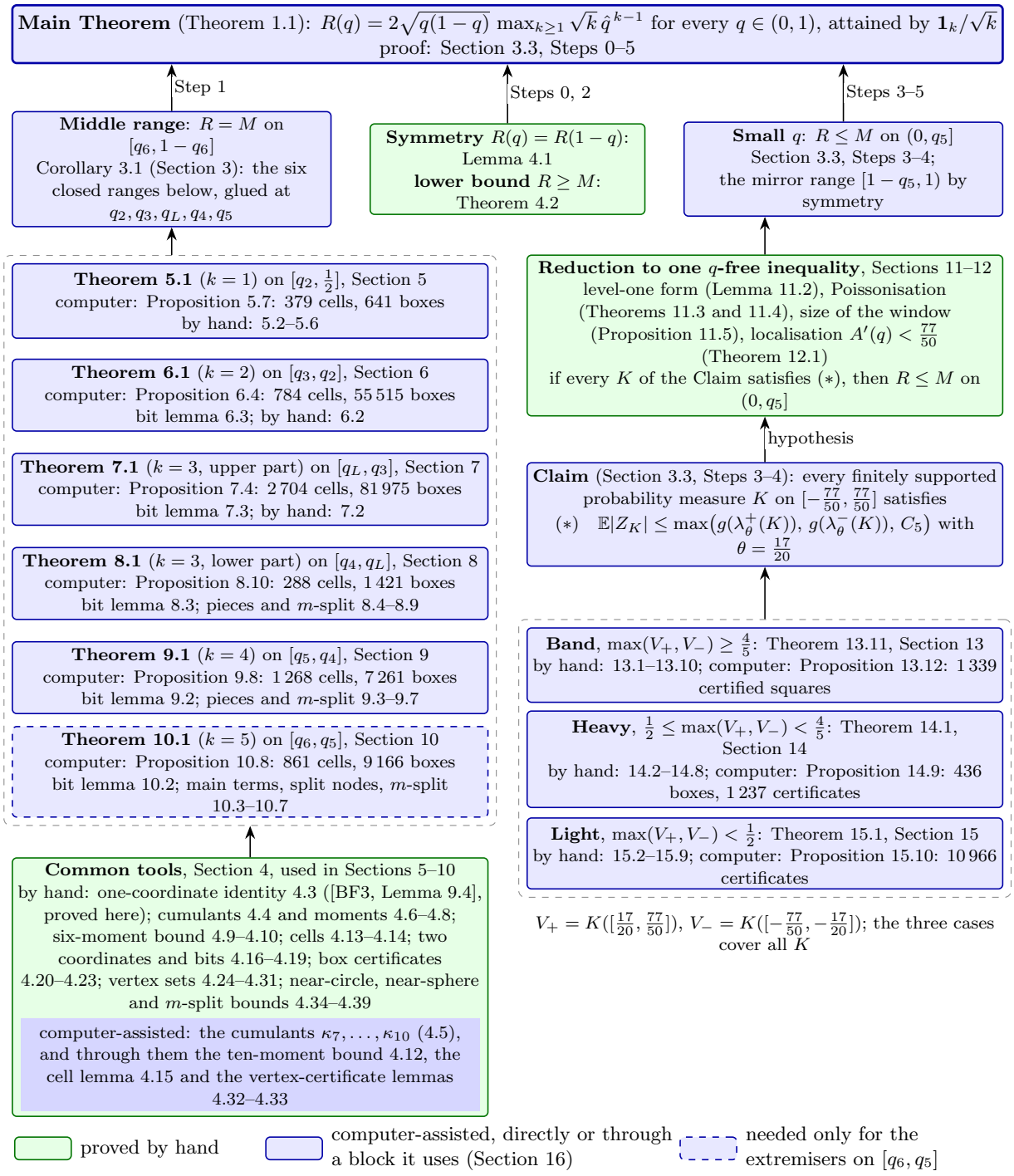

FIGURE 1. Structure of the proof. An arrow means "is used in the proof of". Green blocks are proved by hand; blue blocks are computer-assisted, either directly (a finite computation, described in Section 16) or because they use a blue block. Numbers without a name are statement numbers of this paper; ranges of numbers include the definitions between them. The dashed block is needed only for the extremisers on $[q_6, q_5]$: the value of R there also follows from Sections 11–15 (Section 3.3, Step 1).

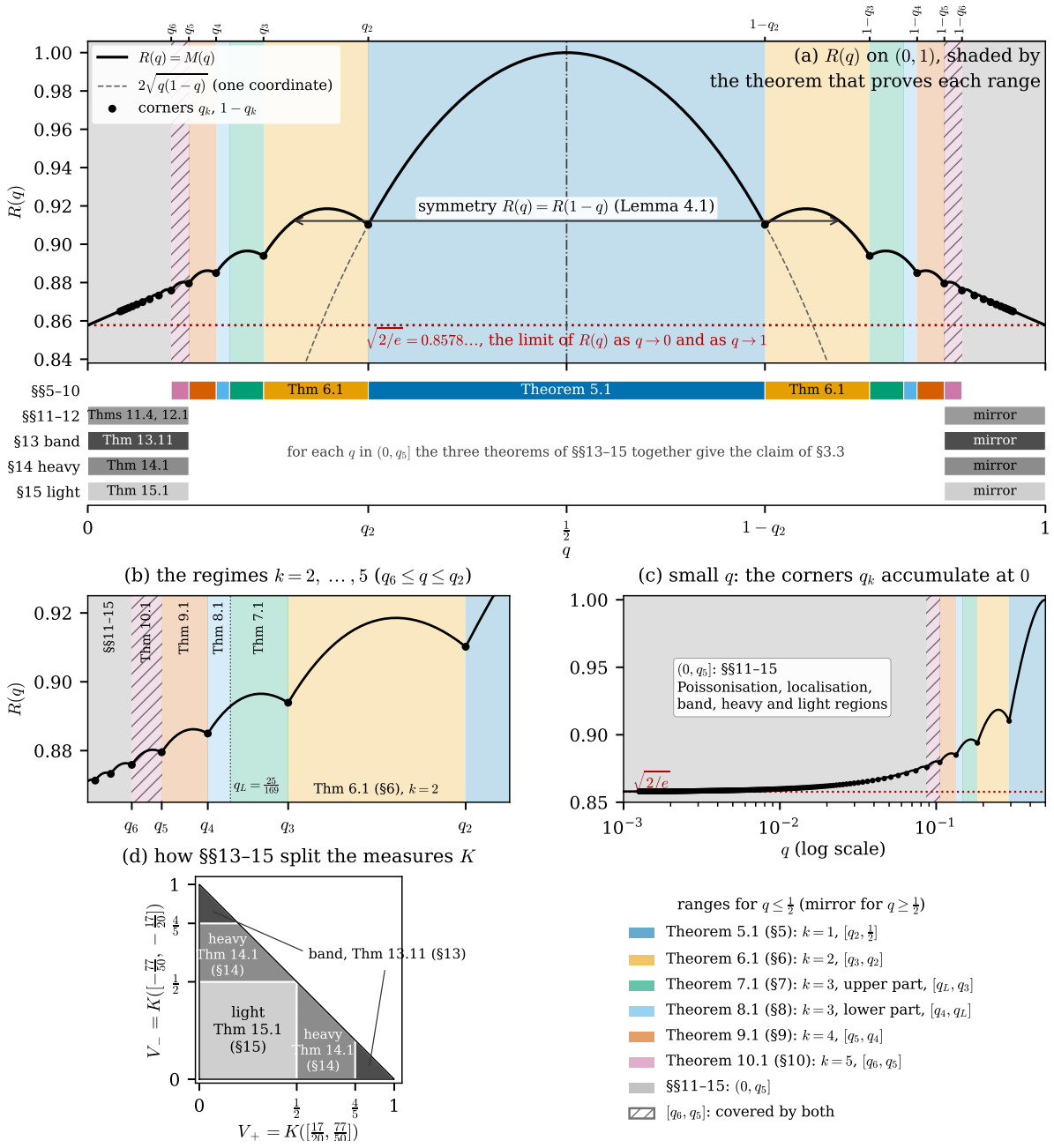

FIGURE 2. The optimal constant $R(q)$ of Theorem 1.1, computed from (S) by `figures/plot_Rq.py`, which checks the closed form against the maximum over all $k \le 2k^* + 10$ and against a complete enumeration, in floating point, of the binomial law of $\chi_1 + \cdots + \chi_k$ (largest difference $3 \cdot 10^{-15}$). Each range of q is shaded by the theorem that proves it; hatched ranges are covered both by Theorem 10.1 and by Sections 11–15; dots are the corners q_k and $1 - q_k$. (a) The whole range, with the symmetry $R(q) = R(1-q)$, the limit $\sqrt{2/e}$ (dotted) and the one-coordinate value $2\sqrt{q(1-q)}$ (dashed), which equals $R(q)$ exactly on $[q_2, 1-q_2]$; the strip lists the sections that prove each range. (b) The regimes $k = 2, \ldots, 5$; $q_L = \frac{25}{169}$ separates Theorems 7.1 and 8.1 and is not a corner. (c) Small q on a logarithmic scale. (d) The three classes of measures K of Sections 13–15 (Section 3).

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 Theorem 1.1 says that

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

for every such f, with equality for the OR of k bits if $q \le \frac{1}{2}$, and for the AND of k bits if $q \ge \frac{1}{2}$, where k attains the maximum.

Remark 1.3 (extremisers). [computer-assisted, see Sec. 16] On $[q_6, 1-q_6]$, $q_6 = 1 - \sqrt{5/6}$, the extremisers are determined completely by Theorems 5.1(c), 6.1(b), 7.1(b), 8.1(b), 9.1(b) and 10.1(b) (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.

1.3. **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 computed two families exactly. For two coefficients, $\alpha = (1,1)/\sqrt{2}$ beats one coordinate for $q < 1 - 1/\sqrt{2}$ ([St, Section 4.2], as cited in [BF3, Remark 9.8(c)]). The value of k equal coefficients, maximised over k, is the right-hand side of (S); it is stated in [IS, (1.10)], with a reference to a forthcoming paper of Stone (as printed there, the formula lacks the factor $(1-p^*)^{1/2}$), 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; it is Theorem 1.1.

For the central range, the report [BF3] proved, in its Theorem K (Section 9.4), that $R(q) = 2\sqrt{q(1-q)}$ for $q \in [\frac{3}{8}, \frac{5}{8}]$, by Stein's method and an exact rational interval computation, and conjectured [BF3, Remark 9.8(c)] that $R(q) = 2\sqrt{q(1-q)}$ holds exactly for $1 - \frac{1}{\sqrt{2}} \le q \le \frac{1}{\sqrt{2}}$, where at $q = 1 - \frac{1}{\sqrt{2}}$ both e_1 and $(e_1 + e_2)/\sqrt{2}$ are extremal. This is Theorem 5.1 below, whose proof does not depend on [BF3]. Theorems 6.1–10.1 extend the formula, regime by regime, to $[q_6, 1-q_6]$, and Sections 11–15 handle all small q at once.

1.4. **Use of earlier work.** The proof of Theorem 1.1 uses no result of [BF3], [ILvHV], [IS] or [St] without proof. The following facts also appear in that earlier work, and each of them is stated and proved in full here.

- The one-coordinate identity $\mathbb{E}|a\chi + Y| = 2\tau a + (2q-1)\mathbb{E}Y + 2\mathbb{E}R_a(Y)$ of Lemma 4.3, the starting point of Sections 5–10. Its case $a > 0$, $Y = bM$ with $b \ge 0$, M bounded and $\mathbb{E}M = 0$ is [BF3, Lemma 9.4], stated there for $\frac{3}{8} \le q \le \frac{1}{2}$.
- The two-coefficient value $\mathbb{E}|\chi_1 + \chi_2|/\sqrt{2} = 2\sqrt{2}\,(1-q)\tau$ ($q \le \frac{1}{2}$), which exceeds 2τ if and only if $q < q_2$ (Lemma 5.2, and Theorem 4.2 with $k = 2$). This is the example of [BF3, Remark 9.8(c)], which attributes it to [St, Section 4.2].
- The value $T_k(q)$ of k equal coefficients and its maximum over k, the right-hand side of (S) (Theorem 4.2); see [IS, (1.10)].
- The equivalence of the inequality with a bound on level-one coefficients (Lemma 11.2). Its special case $R(q) \le 2\tau \iff \sup_f D(f) \le 1$ is the equivalent form of [BF3, Theorem K].

The result [BF3, Theorem K] itself is not used: Theorem 5.1 proves $R(q) = 2\sqrt{q(1-q)}$ on the larger range $[q_2, 1-q_2] \supset [\frac{3}{8}, \frac{5}{8}]$ by a different method. The bounds of [ILvHV] and [IS], and the one quoted in [IS], are cited only for history. Everything else in the proof is either proved here or classical.

1.5. **The strategy.**

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 $M(q)$ is the upper envelope of the curves T_k. The lower bound $R \geq M$ is this computation (Theorem 4.2). All the work is in the upper bound $R \leq M$.

The middle range (Sections 4–10). For each $k = 1, \ldots, 5$ we prove $\mathbb{E}|\sum \alpha_i \chi_i| \leq T_k(q)\|\alpha\|_2$ for q in the band of k. Write the sum as $a_1\chi_1 + a_2\chi_2 +$ (remainder) with the largest coefficients in front. Exact identities reduce the problem to bounding an expectation of a piecewise-linear function of the remainder. The first six (or ten) moments of the remainder are fixed by power sums of its coefficients, and these are controlled by the parameters. A polynomial "moment certificate" then bounds the expectation on a cell of parameter 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 (Section 11). 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 $R_n(q) \leq \sqrt{q/((1-q)s)}\, \mathbb{E}|Z_K|$, 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:

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

where $\lambda_\theta^{\pm}(K)$ is the expected number of jumps of size $\geq \theta$ (resp. $\leq -\theta$), and $g(\lambda) = 2\sqrt{\lambda}\, e^{-\lambda}$ is $\mathbb{E}|Z|$ when all jumps have the same size $a \geq 1$ (then $\lambda = a^{-2}$). With $C = C_5 = g(2\ln\frac{5}{4})$ this yields $R = M$ on all of $(0, q_5]$ (Theorem 11.4).

No huge coefficients (Section 12). The first-order optimality conditions of a maximiser show that no coefficient can be large: for large n, every jump of the measure K produced above lies in $[-A, A]$ for any fixed $A > A'(q)$, and $A'(q) \leq A'(q_5) = 1.53804\ldots < 1.54$ (Theorem 12.1). So $\mathrm{ID}^*(C_5)$ is needed only for K carried by $[-1.54, 1.54]$.

Proving $\mathrm{ID}^*(C_5)$ (Sections 13–15). 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* ($V_+ \geq \frac{4}{5}$ or $V_- \geq \frac{4}{5}$). This region contains the Dirac laws $K = \delta_a$, for which the inequality is an equality whenever $a \geq 1$ and $g(a^{-2}) \geq C_5$, 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 comparison lemma bounds (Theorem 13.11).
- *Heavy far region* ($\frac{1}{2} \leq V_\pm < \frac{4}{5}$). 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 14.1).
- *Light far region* ($V_+ < \frac{1}{2}$ and $V_- < \frac{1}{2}$). Here there is room to spare: $\mathbb{E}|Z_K| \leq \frac{171}{200} = 0.855 < C_5 = 0.85510\ldots$ The proof spreads windows of jumps to two points (a convex-order step) and uses 10 966 exact moment certificates (Theorem 15.1).

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 (Section 3).

1.6. **Computer assistance and organisation.** Several statements rest on finite computations. They are marked [computer-assisted, see Sec. 16] in the text; their proofs reduce them, by hand, to finitely many inequalities, which are decided by computer in exact rational arithmetic (Sturm sequences, exact comparisons of rationals) or in outward-rounded interval or ball arithmetic. Floating point is used only to *find* certificates and subdivisions, never to decide an inequality. Section 16 lists, for every numbered statement, whether it is proved by hand or computer-assisted, and, for the computer-assisted ones, the method, the programs, their sizes, the recorded running times and certified counts, and the commands that reproduce them. The verifying programs are in the code archive, but the recorded certificate data of most computer-assisted propositions are not; Section 16.5 lists which verifications were repeated for this paper, on the archive and on regenerated data.

Section 2 fixes notation. Section 3 explains which result covers which values of q and proves Theorem 1.1 from the results of the later sections. Sections 4–10 prove the formula on the middle range $[q_6, 1 - q_6]$: Section 4 collects the tools common to all regimes, and Sections 5–10 treat $k = 1, 2, 3, 3, 4, 5$ (the regime $k = 3$ in two parts). Section 11 contains the Poissonisation and the reduction of $(0, q_5]$ to $\mathrm{ID}^*(C_5)$, Section 12 the localisation of maximisers, Sections 13 and 14 the band and the heavy far region, and Section 15 the light far region. Section 16 describes the computer-assisted components.

2. Notation and conventions

The following symbols have the same meaning throughout, except where a local meaning is stated in a section.

symbol	meaning
q, $\hat{q}$, p	$q \in (0,1)$; $\hat{q} = \max(q, 1-q)$; $p = \min(q, 1-q)$
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 $X \sim \mathrm{Bernoulli}(q)$; 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; $R_n(q) = \max_{\lvert\alpha\rvert=1,\, \alpha\in\mathbb{R}^n} \mathbb{E}\lvert L\rvert$; $R(q) = \sup_n R_n(q)$
$\lvert\cdot\rvert$, e_i, $\mathbf{1}_S$	$\lvert\alpha\rvert = \lVert\alpha\rVert_2$ for vectors; 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 $kq < 1$, $q \le \frac{1}{2}$; in Sections 5–10, T denotes the target of the regime
$M(q)$	$2\tau \max_{k\ge1} \sqrt{k}\,\hat{q}^{\,k-1}$; 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 $[q_{k+1}, q_k]$; $q_2 = 0.292893\ldots$, $q_3 = 0.183503\ldots$, $q_4 = 0.133974\ldots$, $q_5 = 0.105572\ldots$, $q_6 = 0.087129\ldots$
q_L	$\frac{25}{169} = 0.147928\ldots$, the boundary between Sections 7 and 8
$s = s(q)$	$\ln \frac{1}{1-q}$, 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	$C(q) = \max_{k\ge1} g(ks)$; for $q \le \frac{1}{2}$, $M(q) = \sqrt{q/((1-q)s)}\,C(q)$, equation (11.1); $C_K = \min_{0<q\le q_K} C(q) = C(q_K)$ (Theorem 11.4(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 Sections 11–15 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 $K = \sigma^2\delta_0 + \sum_j w_j\delta_{a_j}$: $Z_K = \sigma G + \sum_j a_j(N_j - w_j/a_j^2)$, $N_j \sim \mathrm{Poisson}(w_j/a_j^2)$

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. $\le-\theta$; also written $\lambda_\pm(K)$, and $\Lambda=\lambda_\theta^+(K)$ in Section 13
$\mathrm{ID}^*(C)$	every finitely supported probability measure K on $\mathbb{R}\setminus\{0\}$ has some $\theta=\theta(K)>0$ with $\mathbb{E}\lvert Z_K\rvert\le\max(g(\lambda_\theta^+(K)),g(\lambda_\theta^-(K)),C)$
θ, A, $V_\pm$	in Sections 13–15: $\theta=\frac{17}{20}$, $A=\frac{77}{50}$, $V_+=K([\theta,A])$, $V_-=K([-A,-\theta])$
$A'(q)$	$\sqrt{2q/s}/(1-q)$ (Theorem 12.1(f)); increasing, with $A'(q_5)=\sqrt{5q_5/\ln\frac54}=1.538044391650755\ldots<\frac{77}{50}$
$\Delta_i(f)$, $D(f)$	for $f:\{0,1\}^n\to[0,1]$ (or $[-1,1]$) under the Bernoulli(q) product measure, $\Delta_i(f)=\mathbb{E}[f\mid x_i=1]-\mathbb{E}[f\mid x_i=0]$, $D(f)=\sum_i\Delta_i(f)^2$
OR_S	$2\cdot\mathbf{1}\{\exists i\in S: x_i=1\}-1$ (in Section 11, the indicator $\mathbf{1}\{\exists i\in S: x_i=1\}$)
N_λ, G	a Poisson(λ) variable ($N_0=0$) and a standard Gaussian, independent of each other and of everything else
$X\le_{cx}Y$	convex order: $\mathbb{E}f(X)\le\mathbb{E}f(Y)$ for every convex f
x_+	$\max(x,0)$

Local notation. In Sections 4–10, M usually denotes the remainder $\sum\beta_i\chi_i$ (a random variable), not the function $M(q)$; in Section 14, $M(a,b)=a\theta^2+bA^2$. In Section 11, K is an integer in q_K, C_K and a measure elsewhere. Further local symbols are introduced where they are used.

Arithmetic conventions. All polynomials in the computer-assisted parts have rational coefficients. "Verified" means verified in exact rational arithmetic or in outward-rounded interval (or ball) arithmetic. For a rational $x\ge0$ and an integer $N\ge1$, the *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; unless stated otherwise $N=10^{15}$, and we write $\lfloor\sqrt{x}\rfloor_{15}$ and $\lceil\sqrt{x}\rceil_{15}$ for them.

3. Structure of the proof and proof of the Main Theorem

3.1. **Which result covers which values of q.** Figure 3 and Table 1 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 $q\in(0,1)$.

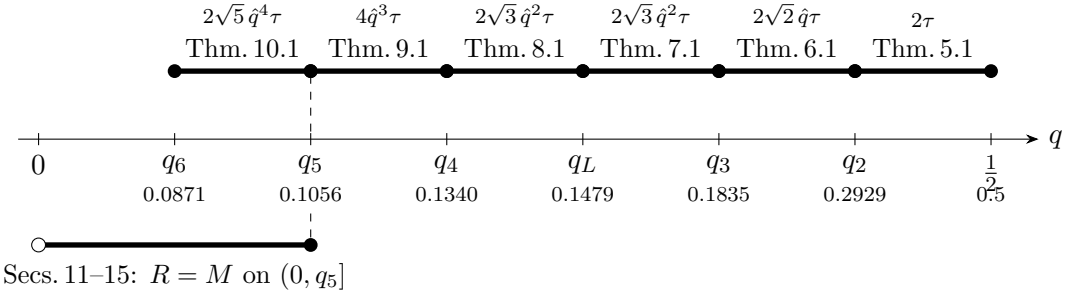

FIGURE 3. The range $(0,\frac12]$, not to scale. Thick bars are closed intervals (filled dots); the small-q chain is open at 0 and closed at q_5. Above each bar is the theorem and the value $M(q)$ there. The range $[\frac12,1)$ is the mirror image under $q\mapsto1-q$: every theorem of Sections 5–10 proves the mirror statement, and $R(q)=R(1-q)$, $M(q)=M(1-q)$ give the rest. The overlap $[q_6,q_5]$ of Theorem 10.1 and the small-q chain is not needed for the value of R.

closed range of q	$R(q)=$	proved in
$[q_2, 1-q_2]$	2τ	Theorem 5.1 (Section 5)
$[q_3, q_2]\cup[1-q_2, 1-q_3]$	$2\sqrt{2}\,\hat{q}\,\tau$	Theorem 6.1 (Section 6)
$[q_L, q_3]\cup[1-q_3, 1-q_L]$	$2\sqrt{3}\,\hat{q}^2\tau$	Theorem 7.1 (Section 7)
$[q_4, q_L]\cup[1-q_L, 1-q_4]$	$2\sqrt{3}\,\hat{q}^2\tau$	Theorem 8.1 (Section 8)
$[q_5, q_4]\cup[1-q_4, 1-q_5]$	$4\hat{q}^3\tau$	Theorem 9.1 (Section 9)
$[q_6, q_5]\cup[1-q_5, 1-q_6]$	$2\sqrt{5}\,\hat{q}^4\tau$	Theorem 10.1 (Section 10)
$[q_6, 1-q_6]$	$M(q)$	Corollary 3.1
$(0, q_5]$	$M(q)$	Sections 11–15, see Table 2
$[1-q_5, 1)$	$M(q)$	mirror (Lemma 4.1)
$(0,1)$	$M(q)$	Theorem 1.1, proved in Section 3.3

TABLE 1. The q-ranges and their proofs.

Corollary 3.1 (the middle range)**.** [computer-assisted, see Sec. 16] $R(q) = M(q)$ *for every* $q \in [q_6, 1-q_6] = [1-\sqrt{5/6}, \sqrt{5/6}]$.

Proof. By Lemma 4.1 let $q \le \frac{1}{2}$, so $\hat{q} = 1-q$ and $M(q) = \max_k T_k(q)$. The interval $[q_6, \frac{1}{2}]$ is the union of $[q_2, \frac{1}{2}]$, $[q_3, q_2]$, $[q_L, q_3]$, $[q_4, q_L]$, $[q_5, q_4]$ and $[q_6, q_5]$, on which Theorems 5.1, 6.1, 7.1, 8.1, 9.1 and 10.1 give $R(q) = T_1$, T_2, T_3, T_3, T_4 and T_5 respectively (with $T_1 = 2\tau$). By Theorem 4.2, the maximum of $T_k(q)$ over $k \ge 1$ is attained at $k = \lfloor 1/(q(2-q))\rfloor$. Since $q(2-q) = 1-(1-q)^2$ is increasing on $(0,1)$ and equals $1/k$ at $q = q_k$, this maximiser is k on $[q_{k+1}, q_k]$ (with the tie of $k-1$ and k at q_k), and $k = 1$ on $[q_2, \frac{1}{2}]$. Hence $R(q) = M(q)$ on each of the six intervals. □

3.2. **How the small-q chain fits together.** Table 2 lists the results used on $(0, q_5]$, and Figure 2(d) shows how the three theorems of Sections 13–15 divide the measures K: 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 $V_\pm \ge 0$ and $V_+ + V_- \le 1$; the light region is $\{V_+ < \frac{1}{2}, V_- < \frac{1}{2}\}$, the heavy region $\{\frac{1}{2} \le V_+ < \frac{4}{5}\} \cup \{\frac{1}{2} \le V_- < \frac{4}{5}\}$ and the band $\{V_+ \ge \frac{4}{5}\} \cup \{V_- \ge \frac{4}{5}\}$. 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.

link	statement used	where
L0	$R(q) \ge M(q)$ for $q \le \frac{1}{2}$ (equal coefficients)	Theorem 4.2
L1	if ID* holds at every K_f with constant $C \le C(q)$, then $R(q) \le M(q)$; $\min_{(0,q_5]} C = C_5$	Lemma 11.2, Theorem 11.4, Proposition 11.5
L2	only K carried by $[-A, A]$ with $A > A'(q)$ are needed; $A'(q) \le A'(q_5) < \frac{77}{50}$	Theorem 12.1(f),(g)
L3	band: $V_+ \ge \frac{4}{5}$ or $V_- \ge \frac{4}{5} \Rightarrow \mathbb{E}\lvert Z_K\rvert \le \max(g(\lambda^{\pm}_{17/20}(K)), C_5)$	Theorem 13.11
L4	heavy: $\frac{1}{2} \le V_+ < \frac{4}{5}$ or $\frac{1}{2} \le V_- < \frac{4}{5} \Rightarrow \mathbb{E}\lvert Z_K\rvert < C_5$	Theorem 14.1
L5	light: $V_+ < \frac{1}{2}$ and $V_- < \frac{1}{2} \Rightarrow \mathbb{E}\lvert Z_K\rvert \le \frac{171}{200} < C_5$	Theorem 15.1

TABLE 2. The links of the small-q chain.

3.3. **Proof of the Main Theorem.**

Proof of Theorem 1.1. Step 0: symmetry. By Lemma 4.1, $R(q) = R(1-q)$, 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 $M(q) = \max_k T_k(q)$.

Step 1: the middle range. Corollary 3.1 gives (S) for every $q \in [q_6, 1-q_6]$, in particular on $[q_5, 1-q_5]$. (Only Theorems 5.1–9.1 are needed for $[q_5, 1-q_5]$; the value of R on $[q_6, q_5]$ is also given by Steps 2–4.)

Step 2: the lower bound on $(0, \frac{1}{2}]$. By Theorem 4.2, 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 12.1(f).

- $A > A'(q)$: by Theorem 12.1(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 11.4(d), $C(q) \geq C_5$ on $(0, q_5]$, and by (11.1), $M(q) = \sqrt{q/((1-q)s)}\, C(q) \geq \sqrt{q/((1-q)s)}\, C_5$.

Theorem 12.1(f) uses the bound

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

only at the single finitely supported probability measure $K = \tilde{K}$ there, which is carried by $[-A, A]$, and for any $\theta > 0$, 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.

(i) $V_+ \geq \frac{4}{5}$ or $V_- \geq \frac{4}{5}$. Theorem 13.11 gives $\mathbb{E}|Z_K| \leq \max(g(\lambda^+_{0.85}(K)), C_5)$, resp. $\mathbb{E}|Z_K| \leq \max(g(\lambda^-_{0.85}(K)), C_5)$, 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 14.1 gives $\mathbb{E}|Z_K| < C_5$.

(iii) $V_+ < \frac{1}{2}$ and $V_- < \frac{1}{2}$. Theorem 15.1 gives $\mathbb{E}|Z_K| \leq \frac{171}{200} < C_5$, 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 $R(1-q)$; together with Theorem 4.2 this proves the remaining statements, with $p = \min(q, 1-q)$. □

4. The middle range: common tools

This section collects the definitions and lemmas used in all six regimes of the middle range. Each regime (Sections 5–10) fixes a target $T = T_k$, a parameter range $[U_-, U_+]$ and a threshold A_S, and supplies the finite data and the regime-specific bounds at the extremisers.

4.1. **Symmetry and parametrisation.**

Lemma 4.1 (symmetry)**.** *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 in Sections 4–10, $q \le \frac{1}{2}$, i.e. $u \ge 1$. We parametrise everything by u:

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

The map $u \mapsto q$ is a decreasing bijection $[1,\infty) \to (0, \frac{1}{2}]$; on $u \ge 1$, τ and q are decreasing and $1-q$ is increasing in u. The thresholds q_k correspond to

$$u_k := \sqrt{\frac{1-q_k}{q_k}} = \sqrt{(k-1) + \sqrt{k(k-1)}}, \qquad \text{so}$$

$$u_2 = \sqrt{1+\sqrt{2}}, \quad u_3 = \sqrt{2+\sqrt{6}}, \quad u_4 = \sqrt{3+2\sqrt{3}}, \quad u_5 = \sqrt{4+2\sqrt{5}}, \quad u_6 = \sqrt{5+\sqrt{30}},$$

numerically $u_2 \approx 1.5537740$, $u_3 \approx 2.1093814$, $u_4 \approx 2.5424598$, $u_5 \approx 2.9106934$, $u_6 \approx 3.2368543$ (indeed $1-q_k = \sqrt{(k-1)/k}$, so $u_k^2 = \sqrt{k-1}/(\sqrt{k}-\sqrt{k-1})$). By (4.1),

$$T_k = 2\sqrt{k}\,(1-q)^{k-1}\tau = \sqrt{k}\,\tilde{T}_k(u), \qquad \tilde{T}_k(u) = \frac{2u^{2k-1}}{(1+u^2)^k}, \qquad \frac{d}{du}\frac{u^{2k-1}}{(1+u^2)^k} = \frac{u^{2k-2}(2k-1-u^2)}{(1+u^2)^{k+1}}, \tag{4.2}$$

so T_k is increasing on $[1, \sqrt{2k-1}]$ and decreasing on $[\sqrt{2k-1}, \infty)$. Hence for $1 \le u_1 < u_2$ and $u \in [u_1, u_2]$ (here u_1, u_2 denote the ends of an interval, not the thresholds),

$$T_k(u) \;\ge\; T^-(u_1,u_2) := S_k \min\{\tilde{T}_k(u_1), \tilde{T}_k(u_2)\}, \tag{4.3}$$

where $S_k \le \sqrt{k}$ is a fixed rational lower bound of $\sqrt{k}$: $S_1 = 1$, $S_4 = 2$, and $S_k = \lfloor \sqrt{k} \rfloor_{15}$ for $k = 2, 3, 5$. (If $u \le \sqrt{2k-1}$ then T_k is increasing on $[u_1, u]$, and if $u \ge \sqrt{2k-1}$ it is decreasing on $[u, u_2]$.) For rational u_1, u_2 the number $T^-(u_1,u_2)$ is rational.

4.2. **Equal coefficients.**

Theorem 4.2 (equal coefficients)**.** *Let $q \in (0, \frac{1}{2}]$ and $k \ge 1$ with $kq < 1$. Then*

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

The maximum of $T_k(q)$ over all $k \ge 1$ 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 $R(q) \ge M(q)$, and $M(q) \to \sqrt{2/e}$ as $q \to 0$.

Proof. Let $S = X_1 + \cdots + X_k$, so $\sum \chi_i = (S - kq)/\tau$. 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 $h(k+1)/h(k) = \sqrt{1+1/k}\,(1-q) \ge 1$ iff $k \le (1-q)^2/(q(2-q)) = 1/(q(2-q)) - 1$, 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 $k^* q \le 1/(2-q) < 1$. Since $T_k(q) = 2\sqrt{q/(1-q)}\,h(k)$, this proves the statements on the maximum, and $R(q) \ge T_{k^*}(q) = M(q)$. 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 $q/((1-q)s) \to 1$. □

The formula of Theorem 4.2 also follows from the level-one identity (4.7) below: if $q < 1/k$ and $S = \chi_1 + \cdots + \chi_k$, then $S \ge u - (k-1)v > 0$ when some $\chi_i = u$ (because $u^2 > k-1$), and $S = -kv < 0$ otherwise; so $|S| = fS$ with $f = 1 - 2\cdot\mathbf{1}\{\text{all } \chi_i = -v\}$, and $\mathbb{E}[f\chi_i] = -2(1-q)^k(-v) = 2(1-q)^{k-1}\tau$. We use the comparisons

$$\frac{T_{j+1}}{T_j} = \sqrt{\frac{j+1}{j}}\,(1-q), \qquad \text{so} \quad T_{j+1} \le T_j \iff 1-q \le \sqrt{\tfrac{j}{j+1}} \iff q \ge q_{j+1}, \tag{4.4}$$

with equality iff $q = q_{j+1}$ ($j \ge 1$, $q \in (0,1)$; $T_1 = 2\tau$).

4.3. **The one-coordinate identity.**

Lemma 4.3 (one-coordinate identity)**.** *For $a \geq 0$ 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, if $a \in [0,1)$, $b = \sqrt{1-a^2}$ and $M = \sum_i \beta_i \chi_i$ is independent of χ_1 with $\sum \beta_i^2 = 1$, then

$$\mathbb{E}|a\chi_1 + bM| = 2\tau a + 2\mathbb{E}R_a(bM).$$

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; for the last statement use $\mathbb{E}M = 0$. □

The case $a > 0$, $Y = bM$ with $b \geq 0$, M bounded and $\mathbb{E}M = 0$ is [BF3, Lemma 9.4], stated there for $\frac{3}{8} \leq q \leq \frac{1}{2}$.

4.4. **Moments of the remainder.**

Lemma 4.4 (cumulants of order at most six)**.** *Let $w = u^2 + v^2$ and $d = u - v$. The cumulants of χ are $\kappa_1 = 0$, $\kappa_2 = 1$, $\kappa_3 = d$, $\kappa_4 = w - 4$, $\kappa_5 = d(w-10)$ and $\kappa_6 = w^2 - 26w + 64$.*

Proof. By (4.1), $m_k := \mathbb{E}\chi^k = qu^k + (1-q)(-u^{-1})^k = \dfrac{u^k + (-1)^k u^{2-k}}{1+u^2}$. 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

$$m_3 = \frac{u^2-1}{u} = u - v, \qquad m_4 = u^2 - 1 + u^{-2} = w - 1,$$
$$m_5 = \frac{(u^2-1)(u^4+1)}{u^3} = (u-v)w, \qquad m_6 = u^4 + u^{-4} - w + 1 = w^2 - w - 1.$$

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 $\kappa_6 = w^2 - w - 1 - 15(w-1) - 10(w-2) + 30 = w^2 - 26w + 64$. □

Lemma 4.5 (cumulants of order seven to ten)**.** [computer-assisted, see Sec. 16] *With w and d as in Lemma 4.4, $\kappa_j = d^{[j \text{ odd}]} G_j(w)$ 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. For $j \leq 6$ this is Lemma 4.4. In general the cumulants are determined by the moments m_k of the proof of Lemma 4.4 through the recursion $\kappa_n = m_n - \sum_{k=1}^{n-1} \binom{n-1}{k-1} \kappa_k m_{n-k}$. The identities for $7 \leq j \leq 10$ are identities of rational functions of u, verified in exact symbolic arithmetic (the difference of the two sides simplifies to 0); the cases $j \leq 6$ are checked in the same way. □

Lemma 4.6 (moments from cumulants)**.** *Let $M = \sum \beta_i \chi_i$ (a finite sum of i.i.d. copies of χ) 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. In particular

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

Proof. Cumulants of independent sums add and $K_j(\beta\chi) = \beta^j \kappa_j$, 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. For $n \le 6$ the relations read $m_3 = K_3$, $m_4 = K_4 + 3K_2^2$, $m_5 = K_5 + 10K_3K_2$ and $m_6 = K_6 + 15K_4K_2 + 10K_3^2 + 15K_2^3$. □

Lemma 4.7 (power sums)**.** *Let $\sum \beta_i^2 = 1$, $\max_i |\beta_i| \le m \le 1$ and $\rho = \sqrt{p_4}$. Then*

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

more generally $0 \le \rho \le m$, $|p_3| \le \rho$, $|p_j| \le m^{j-4}\rho^2$ for $5 \le j \le 10$, and $p_j \ge \rho^{j-2}$ for even $j \ge 4$. (Note that $\max_i |\beta_i| \le 1$ always.)

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, and $p_4^2 = (\sum \beta_i \cdot \beta_i^3)^2 \le \sum \beta_i^2 \sum \beta_i^6 = p_6$. Also $p_4 \le m^2 \sum \beta_i^2 = m^2$, $p_6 \le m^2 p_4$ and, 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 4.8 (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 $1 - m^2 < m^2$. □

4.5. **Moment certificates: the objective bounds.**
Six-moment cumulant enclosures. For $1 \le u_1 \le u \le u_2$ 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 $w^+ < 13$. Then $\kappa_4 \in [w^- - 4, w^+ - 4]$; since $x \mapsto f_6(x) = x^2 - 26x + 64$ is decreasing on $x < 13$, $\kappa_6 \in [f_6(w^+), f_6(w^-)]$; and $|\kappa_5| \le k_5^+ := k_3^+ \max(|w^- - 10|, |w^+ - 10|)$.

Definition 4.9 (six-moment objective bound)**.** For $c = (c_0, \dots, c_6) \in \mathbb{Q}^7$, an interval $[u_1, u_2]$ with $1 \le u_1 < u_2$ and $w^+ < 13$, a number $m^* \in (0, 1]$, an optional number $p^* < 0$ (allowed only if $u_1 > 1$), 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 six-moment 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 4.10 (six-moment expectation bound)**.** *Suppose c satisfies the six-moment 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 4.6,

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

with A the unmodified value. Put $\rho = \sqrt{p_4} \in [0, m^*]$ (Lemma 4.7). We bound each term, using the cumulant enclosures for the actual $u \in [u_1, u_2]$ and Lemma 4.7:

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

Summing, $\mathbb{E}P(M) \leq \Theta - h(\rho) < \Theta$. □

Ten-moment cumulant enclosures. For $1 \leq u_1 \leq u \leq u_2$: $d = u - 1/u$ and $w = u^2 + u^{-2}$ are increasing and $d \geq 0$, so $d \in [d^-, d^+] = [u_1 - \frac{1}{u_1}, u_2 - \frac{1}{u_2}]$ and $w \in [w^-, w^+]$ as above. Let $[G_j^-, G_j^+] \supseteq G_j([w^-, w^+])$ be rational enclosures of the ranges of the polynomials G_j of Lemma 4.5. (The verifiers compute them exactly from the real roots of G_j', isolated by Sturm sequences, or as the hull of exact end values on subintervals on which G_j' has no root and interval Horner enclosures on short subintervals that contain one; see Section 10.) 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 4.11 (ten-moment objective bound)**.** Let $D \leq 10$, $c = (c_0, \ldots, c_D) \in \mathbb{Q}^{D+1}$, $1 < u_1 < u_2$ 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 $e \neq 0$ with $L_e \neq 0$ let $[C_e^-, C_e^+]$ be the interval product $L_e \prod_j [\kappa_j^-, \kappa_j^+]^{e_j}$, and put

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

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, $e = (1, 0, \ldots, 0)$ (i.e. the monomial p_3) and $C_e^- \geq 0$: 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 $C_e^+ \leq 0$: $b_e(\rho) = C_e^+\, \ell_e\, \rho^{l_e}$;
(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 ten-moment 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 4.12 (ten-moment expectation bound)**.** [computer-assisted, see Sec. 16] *Suppose c satisfies the ten-moment 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 4.6, $\mathbb{E}P(M) = \sum_n c_n \mu_n = L_0 + \sum_{e \neq 0} C_e p^e$ with $C_e = L_e \prod_j \kappa_j^{e_j} \in [C_e^-, C_e^+]$ (by Lemma 4.5 and the ten-moment cumulant enclosures) and $p^e = \prod_j p_j^{e_j}$. Let $\rho = \sqrt{p_4} \in [0, m^*]$. By Lemma 4.7, $|p^e| \le \rho^{e_3} (\rho^2)^{e_4} \prod_{j \ge 5} (m^{*\,j-4} \rho^2)^{e_j} = U_e \rho^{u_e}$; 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, $\mathbb{E}P(M) \le \Theta - h(\rho) < \Theta$. □

We say that c *satisfies the objective bound* for $(u_1, u_2, m^*, p^*, \Theta)$ if it satisfies the six-moment bound (when $D = 6$ and this is the bound used in the regime) or the ten-moment bound; in both cases $\mathbb{E}P(M) < \Theta$ under the stated conditions.

4.6. **Cells: the one-coordinate route.** Let $|\alpha| = 1$ 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 $b_1 = \sqrt{1 - a^2} > 0$, $\beta_i = \alpha_i / b_1$ for $i \ge 2$, and

$$M_1 = \sum_{i \ge 2} \beta_i \chi_i, \qquad \sum_{i \ge 2} \beta_i^2 = 1, \qquad \max_{i \ge 2} |\beta_i| \le \min\Big(1, \frac{a}{b_1}\Big).$$

Then $L = a\chi_1 + b_1 M_1$, M_1 is independent of χ_1, $\mathbb{E}M_1 = 0$, $\mathbb{E}M_1^2 = 1$, and by Lemma 4.3, for the target $T = T_k$,

$$\mathbb{E}|L| = 2\tau a + 2\mathbb{E}R_a(b_1 M_1), \qquad \text{so} \qquad \mathbb{E}|L| < T_k \iff \mathbb{E}R_a(b_1 M_1) < \tau\big(\sqrt{k}(1-q)^{k-1} - a\big). \tag{4.5}$$

Definition 4.13 (cell and cell certificate)**.** Let $k \ge 1$. A *cell* is a rectangle $[u_1, u_2] \times [\underline{a}, \overline{a}]$ with rationals $1 \le u_1 < u_2$ and $0 \le \underline{a} < \overline{a} < 1$, together with a rational upper bound $\bar{b}$ of $\sqrt{1 - \underline{a}^2}$ and a rational $\bar{m} \in (0, 1]$ with $\bar{m} \ge \min\{1, \overline{a}/\sqrt{1 - \overline{a}^2}\}$. Put

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

with S_k as in (4.3). A *cell certificate* is a vector $c \in \mathbb{Q}^{D+1}$, $D \le 10$, with $P(y) = \sum_n c_n y^n$, 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) c satisfies the objective bound for $(u_1, u_2, \bar{m}, -, \Theta_1)$.

In the verifiers, $\bar{b} = \lceil \sqrt{1 - \underline{a}^2} \rceil_{15}$ and $\bar{m} = \min\{1, \overline{a}/\lfloor \sqrt{1 - \overline{a}^2} \rfloor_{15}\}$ (for $k = 1$, $\bar{m} = 1$ if $\overline{a}^2 \ge \frac{1}{2}$); these satisfy the requirements, which are asserted exactly.

Lemma 4.14 (domination on a cell)**.** *For every $u \in [u_1, u_2]$, every $a \in [\underline{a}, \overline{a}]$, $b_1 = \sqrt{1 - a^2}$, and every $y \in \mathbb{R}$: $R_a(b_1 y) \le \bar{R}(y) := \max\{0, \bar{\ell}_1(y), \bar{\ell}_2(y)\}$.*

Proof. By (4.1), $R_a(b_1 y) = \max\{0, \ell_1(y), \ell_2(y)\}$ with $\ell_1(y) = \frac{u^2}{1+u^2}(b_1 y - \frac{a}{u})$ and $\ell_2(y) = \frac{1}{1+u^2}(-b_1 y - au)$. Suppose $\ell_1(y) > 0$. Then $b_1 y > a/u \ge 0$, so $y > 0$. Since $a \ge \underline{a}$, $u \le u_2$ and $b_1 \le \bar{b}$, we get $0 < b_1 y - \frac{a}{u} \le \bar{b} y - \frac{\underline{a}}{u_2}$. 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

$-b_1 y > au \geq 0$, so $y < 0$. Since $-y > 0$ and $b_1 \leq \bar{b}$, we have $-b_1 y \leq -\bar{b}y$; since $a \geq \underline{a} \geq 0$ and $u \geq u_1 > 0$, we have $-au \leq -\underline{a}u_1$. So $0 < -b_1 y - au \leq -\bar{b}y - \underline{a}u_1$, and with $\frac{1}{1+u^2} \leq \frac{1}{1+u_1^2}$ we get $\ell_2(y) \leq \bar{\ell}_2(y)$. In all cases $\max\{0, \ell_1, \ell_2\} \leq \max\{0, \bar{\ell}_1, \bar{\ell}_2\}$. □

Lemma 4.15 (cell lemma)**.** [computer-assisted, see Sec. 16] *Let a cell have a cell certificate, and suppose $\Theta_1 > 0$. Then $\mathbb{E}|L| < T_k(u)$ for every $u \in [u_1, u_2]$ and every unit α with $\underline{a} \leq \max_i |\alpha_i| \leq \overline{a}$.*

Proof. Reduce α as above, so $a = \alpha_1 \in [\underline{a}, \overline{a}]$. By (V1)–(V3), $P > \bar{R}$ on $\mathbb{R}$, so by Lemma 4.14, $\mathbb{E}R_a(b_1 M_1) \leq \mathbb{E}\bar{R}(M_1) \leq \mathbb{E}P(M_1)$. Since $a/\sqrt{1-a^2}$ is increasing, the coefficients of M_1 are at most $\min(1, \overline{a}/\sqrt{1-\overline{a}^2}) \leq \bar{m}$ in absolute value. By Lemma 4.10 or 4.12 and (V4), $\mathbb{E}P(M_1) < \Theta_1$. Finally $\Theta_1 \leq \tau(u)(\sqrt{k}(1-q)^{k-1} - a)$: indeed $0 < \Theta_1$, $\tau(u) \geq \tau(u_2)$, $(1-q)^{k-1} \geq (\frac{u_1^2}{1+u_1^2})^{k-1}$, $S_k \leq \sqrt{k}$ and $a \leq \overline{a}$. By (4.5), $\mathbb{E}|L| < T_k$. □

For $k = 1$ the target is $T_1 = 2\tau$ and $\Theta_1 = \tau(u_2)(1 - \overline{a}) > 0$; Lemma 4.15 then says $\mathbb{E}R_a(b_1 M_1) < \tau(u)(1-a)$.

4.7. **Two coordinates, bits, and the OR region.**
Splitting off the two largest coefficients. Let $|\alpha| = 1$ 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 $\tan \vartheta = a_2/a_1$ is in $[0, \pi/4]$ and $t = \tan(\vartheta/2) \in [0, \sqrt{2} - 1]$. 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

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

whenever $u \in [U_-, U_+]$. Each regime fixes a threshold A_S: if $a_1 \leq A_S$ we use the one-coordinate route (Lemma 4.15); otherwise $r \geq a_1 > A_S$ and we use the two-coordinate route.

Lemma 4.16 (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*

$$g = \big(q(c + sd),\ (1-q)c - s\, q\, d,\ -q\, c + s(1-q)d,\ -(1-q)(c + sd)\big), \tag{4.6}$$

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, with $\rho = \sqrt{c^2 + d^2} > 0$: $2\tau \max(c, d) \leq T_1 \rho$, with equality iff $cd = 0$; and $2\tau(1-q)(c+d) \leq T_2 \rho$, with equality iff $c = d$. In particular $\mathbb{E}|X| \leq \max(T_1, T_2)\rho$.

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 $c \geq d$ (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 $q \leq \frac{1}{2}$. 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 $\mathbb{E}X_+/\tau = \max(c, d)$. Finally $\max(c, d) \leq \rho$ with equality iff $cd = 0$, and $(1-q)(c+d) \leq \sqrt{2}(1-q)\rho$ with equality iff $c = d$; note $T_1 = 2\tau$ and $T_2 = 2\sqrt{2}(1-q)\tau$. □

The level-one identity and OR functions. 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 (4.1),

$$\mathbb{E}[f\chi_i] = qu\,\mathbb{E}[f \mid x_i = 1] - (1-q)v\,\mathbb{E}[f \mid x_i = 0] = \tau\,\Delta_i(f). \tag{4.7}$$

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 $\mathrm{OR}_S = 2 \cdot \mathbf{1}\{\exists i \in S : x_i = 1\} - 1$. Then

$$\Delta_i(\mathrm{OR}_S) = 2(1-q)^{|S|-1}\ (i \in S), \qquad \Delta_i(\mathrm{OR}_S) = 0\ (i \notin S)\,: \tag{4.8}$$

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 4.17 (bit reduction)**.** *Let $n \geq 1$ and $B > 0$, and suppose that $\sum_{i=1}^n \Delta_i(f)^2 \leq B^2$ for every $f : \{0,1\}^n \to \{-1, 1\}$. Then $G_n(c) \leq \tau B\,|c|$ for every $c \in \mathbb{R}^n$. If $c \neq 0$ and $G_n(c) = \tau B|c|$, then $f^* = \mathrm{sgn}(c \cdot \chi)$ (with $\mathrm{sgn}\,0 = 1$), a function of $(x_1, \ldots, x_n)$ with values ± 1, satisfies $\sum_i \Delta_i(f^*)^2 = B^2$, and c is a positive multiple of $\Delta(f^*)$.*

Proof. Let $X = c \cdot \chi$; then $|X| = f^*X$. By (4.7) and Cauchy–Schwarz, $G_n(c) = \mathbb{E}[f^*X] = \tau\sum_i c_i\Delta_i(f^*) \leq \tau|c|\,|\Delta(f^*)| \leq \tau B|c|$. If equality holds with $c \neq 0$, then $|\Delta(f^*)| = B$, and equality holds in Cauchy–Schwarz with $\sum_i c_i\Delta_i(f^*) = G_n(c)/\tau > 0$ (as X is centred and not a.s. 0), so c is a positive multiple of $\Delta(f^*)$. □

How bit claims are checked. The bit lemmas of Sections 6–10 apply Lemma 4.17 with $B = \tau^{-1}T_k$, i.e. $B^2 = 4k(1-q)^{2k-2}$, so they need the sign of

$$H_f(q) = 4k(1-q)^{2k-2} - \sum_{i=1}^n \Delta_i(f)^2$$

on an interval of q whose ends are among the thresholds q_j (or are rational). 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 an integer polynomial, and the distinct polynomials H_f are tested (39 for $n = 3$, 1 630 for $n = 4$). The threshold q_j is the root in $(0,1)$ of $g_j(q) = jq^2 - 2jq + 1$ (that is, $j(1-q)^2 = j - 1$); g_j is decreasing on $[0,1]$, its other root $1 + \sqrt{(j-1)/j}$ exceeds 1, and it is irreducible over $\mathbb{Q}$ because its discriminant $4j(j-1)$ is not a square. Rational enclosures $q_j^- < q_j < q_j^+$ (from rational bounds of $\sqrt{(j-1)/j}$) are fixed, with the signs of g_j at their ends asserted. On subintervals with rational ends, positivity is shown by an exact Sturm count (no root) and the sign at one end; at an irrational end q_j, either $g_j \nmid H_f$, and H_f has no root in $[q_j^-, q_j^+]$ and the correct sign at a rational end, or $g_j \mid H_f$, $H_f = g_j Q$, and Q has no root in $[q_j^-, q_j^+]$ and the correct sign. Since g_j is irreducible, $H_f(q_j) = 0$ iff $g_j \mid H_f$. The lists of functions with $H_f \equiv 0$ and with $g_j \mid H_f$ are compared with the truth tables of the OR functions.

Lemma 4.18 (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*

$$G_n(c) = 2\tau(1-q)^{n-1}\sum_{i=1}^n c_i \;\leq\; 2\sqrt{n}\,(1-q)^{n-1}\tau\,|c| = T_n|c|,$$

with equality in the inequality if and only if $c_1 = \cdots = c_n$.

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 (4.1), $u + v = (1+u^2)/u = v/q$, 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 (4.7) and (4.8), $G_n(c) = \sum_i c_i\mathbb{E}[\mathrm{OR}\,\chi_i] = \tau\sum_i c_i\cdot 2(1-q)^{n-1}$. The inequality is Cauchy–Schwarz, $\sum_i c_i \leq \sqrt{n}|c|$, with equality iff all c_i are equal. □

4.8. **Box certificates.** This subsection is used for $k = 2, 3$ (Sections 6 and 7). A *box* is $B = [u_1,u_2]\times[t_1,t_2]\times[r_1,r_2]$ with rationals $1 < u_1 < u_2$, $0 \leq t_1 < t_2 \leq 1$, $0 \leq r_1 < r_2 \leq 1$, 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 4.7.

Lemma 4.19 (conditional expectation, box form)**.** *For a point of B with $r < 1$, $\mathbb{E}|L| = \mathbb{E}F(M)$, where*

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

x_j and p_j are the atoms and probabilities of $a_1\chi_1 + sa_2\chi_2$, and $p_jx_j = r\tau g_j$ with g as in (4.6) *(with $c = c(t)$, $d = d(t)$).*

Proof. Condition on (χ_1,χ_2) (independent of M), and use Lemma 4.16 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 $p_jx_j \in [\pi_j^-,\pi_j^+]$ and $p_jb \in [\beta_j^-,\beta_j^+]$ with $\beta_j^- \geq 0$. We define $\bar m(B) = 1$ if $b^- = 0$ or $r_2d(t_2) \geq b^-$, and otherwise $\bar m(B)$ is a rational with $\bar m(B) \geq r_2d(t_2)/b^-$. Then $m \leq \min(1, a_2/b) \leq \min(1,\bar m(B))$ at every point of B with $r < 1$.

Definition 4.20 (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 4.21 (box 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. $|p_jx_j + p_jby| = \max(p_jx_j + p_jby,\ -p_jx_j - p_jby)$. For $y \geq 0$: $p_jx_j + p_jby \leq \pi_j^+ + \beta_j^+y$ and $-p_jx_j - p_jby \leq -\pi_j^- - \beta_j^-y$. For $y < 0$: $p_jby \leq \beta_j^-y$ and $-p_jby \leq -\beta_j^+y$. A sum of maxima is the maximum over all choices. □

Definition 4.22 (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 $P(y) = \sum c_ky^k$ such that (W1) $P(y) > F_B(y)$ for all $y \in \mathbb{R}$, and (W2) c satisfies the six-moment objective bound for $(u_1,u_2,m^*,p^*,T^-(u_1,u_2))$, with T^- as in (4.3).

Lemma 4.23 (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 4.19 and 4.21 and (W1), $\mathbb{E}|L| = \mathbb{E}F(M) \leq \mathbb{E}P(M)$. By Lemma 4.10 and (W2), $\mathbb{E}P(M) < T^-(u_1,u_2) \leq T(u)$, using (4.3). □

With $m^* = \min(1, \bar{m}(B))$ and no p^*, Lemma 4.23 covers every remainder. These are the boxes of kind lp. A box of kind small satisfies $r_2 c(t_1) \le A_S$, so $a_1 = rc(t) \le A_S$ on it, and it is left to the one-coordinate route.

4.9. **Vertex certificates.** This subsection is used for $k = 3, 4, 5$ in Sections 8–10. 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 the ς_i are the signs of peeled coefficients (Lemma 4.25).

Lemma 4.24 (convexity in the coefficients)**.** *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 $p_2(t, r) = (rc, rd, b_0)$, $p_3(t, r, \mu_1) = (rc, rd, b_0\mu_1, b_1)$, $p_4(t, r, \mu_1, \mu_2) = (rc, rd, b_0\mu_1, b_1\mu_2, b_2)$, 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

$$N = \varsigma\mu\chi_{i^*} + \sqrt{1 - \mu^2}\, N^\flat, \qquad \sum_{i \ne i^*} \frac{\gamma_i^2}{1 - \mu^2} = 1, \qquad \mu(N^\flat) \le \kappa(\mu) := \min\Big(1, \frac{\mu}{\sqrt{1 - \mu^2}}\Big), \tag{4.9}$$

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). We put $\kappa(1) = 1$; κ is nondecreasing, and a rational $\kappa' \ge 0$ satisfies $\kappa' \ge \kappa(\mu)$ iff $\kappa' \ge 1$, or $\mu < 1$ and $\kappa'^2(1 - \mu^2) \ge \mu^2$.

Lemma 4.25 (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, the squares of its coefficients sum to 1, and $\mu(M^{(j)}) \le \kappa(\mu_j)$ if $j \ge 1$.*
- *(ii) If $j \ge 1$, $\mu_1, \dots, \mu_{j-1} < 1$ 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 (4.9), 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 (4.9). 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 $\mathbb{E}|L|$. □

Definition 4.26 (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) $|n_0|^2 \geq 1$ 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 $h_{i,\delta} \cdot \bar{c} \neq 0$ is required);
(P4) (enclosure) $h_{i,\delta} \cdot p(\xi) \geq 0$ for all i, δ and all $\xi \in X$.

Lemma 4.27 (cone lemma)**.** *Let $(n_0, (V_\epsilon))$ be a vertex set for X. Then for every $\xi \in X$ there are $\nu_\epsilon \geq 0$ with $p(\xi) = \sum_\epsilon \nu_\epsilon V_\epsilon$ and $\sum_\epsilon \nu_\epsilon \leq 1/|n_0| \leq 1$.*

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 $V_0 \cdot n_0 = |n_0|^2 \neq 0$, so $V_0 \notin \operatorname{span}\{E_i\}$. By (P2) the face $\{\epsilon_i = 0\}$ spans $S_i = \operatorname{span}(V_0, \{E_j\}_{j \neq i})$, which has dimension k' by (P3); hence the k' vectors $V_0, \{E_j\}_{j \neq i}$ are linearly independent. Moreover $\bar{c} - V_0 - \frac{1}{2}\sum_{j \neq i} E_j = \frac{1}{2}E_i$ and $h_{i,0} \cdot \bar{c} \neq 0$ 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 $h_{i,\delta} \cdot z \geq 0$ 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 $\mu_i \geq 0$. The face $\{\epsilon_i = 1\}$ spans $\operatorname{span}(V_0 + E_i, \{E_j\}_{j \neq i})$, so $h_{i,1} \cdot E_j = 0$ $(j \neq i)$ 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 $\mu_i \leq \lambda$. 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 $\nu = \lambda\omega \geq 0$ and $\sum \nu_\epsilon = \lambda$. Finally $z \cdot n_0 = \lambda |n_0|^2$, so $\lambda = z \cdot n_0/|n_0|^2 \leq |z|/|n_0|$. By (P4), $z = p(\xi)$ satisfies the hypothesis, and $|p(\xi)| = 1$. □

Condition (P4) can be 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 4.28 (facet minima)**.** *For $\alpha, \beta \in \mathbb{R}$ and $-1 \leq x^- < x^+ \leq 1$ 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 $i = j, j-1, \dots, 1$, $A = \mathfrak{m}(h_1, h_2; c(t^+), c(t^-))$ 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 $w_{i-1}(\mu_i, \dots, \mu_j) = h_{i+2}\mu_i + \sqrt{1-\mu_i^2}\; w_i(\mu_{i+1}, \dots, \mu_j)$ for $i = j, \dots, 1$. 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

$$h \cdot p_{k'}(t, r, \mu_1, \dots, \mu_j) = r\left(h_1 c(t) + h_2 d(t)\right) + b_0\, w_0(\mu_1, \dots, \mu_j), \qquad b_0 = \sqrt{1-r^2}.$$

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 $\mu_{i+1}, \dots, \mu_j$ 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 4.28 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 $p - q'R$ 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 $p - q'R \geq 0$ for $(p, q') = (-\alpha, x^-)$, and $x^* \leq x^+$ if and only if $p - q'R \leq 0$ for $(p, q') = (-\alpha, x^+)$. (P4) is accepted if the lower bound is ≥ 0 for every facet normal. (For $k = 3$, Section 8, (P4) was checked instead by interval bisection of the parameter box against the $2k'$ facet normals.)

Vertex envelopes. 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 4.29 (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 4.30 (vertex 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 4.31 (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 $c^{(\epsilon)} \in \mathbb{Q}^{D+1}$, $D \le 10$, 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 ten-moment 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 4.32 (vertex certificate lemma)**.** [computer-assisted, see Sec. 16] *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 $\sum \beta_i^2 = 1$, $\max|\beta_i| \le m^*$ and, if p^* is given, $p_3 \le p^*$. Then for every $u \in [u_1, u_2]$, every $\xi \in X$ and every $Z \in \mathcal{Z}$,*

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

Proof. By Lemma 4.27, $p(\xi) = \sum \nu_\epsilon V_\epsilon$ with $\nu \ge 0$ and $\sum \nu_\epsilon \le 1$. By Lemmas 4.24 and 4.30 and (W1), for every y, $F_{p(\xi)}(y) \le \sum_\epsilon \nu_\epsilon F_{V_\epsilon}(y) \le \sum_\epsilon \nu_\epsilon P_\epsilon(y)$. Taking expectations over Z, $\mathbb{E}F_{p(\xi)}(Z) \le \sum_\epsilon \nu_\epsilon \mathbb{E}P_\epsilon(Z)$. By (W1) and Lemma 4.30, $\mathbb{E}P_\epsilon(Z) > \mathbb{E}F_{V_\epsilon}(Z) \ge 0$, and by (W2) and Lemma 4.12, $\mathbb{E}P_\epsilon(Z) < T^-$. Since $\sum \nu_\epsilon \le 1$ and $\max_\epsilon \mathbb{E}P_\epsilon(Z) \ge 0$, $\sum_\epsilon \nu_\epsilon \mathbb{E}P_\epsilon(Z) \le \max_\epsilon \mathbb{E}P_\epsilon(Z) < T^-$. Finally $T^- \le T(u)$ by (4.3). □

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^*).

Boxes. In Sections 8–10 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 $a_2 = r d(t) \le r_2 d(t_2)$ 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 $a_1 = r c(t) \le A_S$ on it.

Lemma 4.33 (lpv boxes)**.** [computer-assisted, see Sec. 16] *At every point of an lpv box with $r < 1$, $\mathbb{E}|L| < T$.*

Proof. By Lemma 4.25 ($j = 0$), $\mathbb{E}|L| = \mathbb{E}F_{p_2(t,r)}(M)$, and $M \in \mathcal{Z}$ since $m \le \bar{m}(B)$. Apply Lemma 4.32. □

4.10. **Near the extremisers: tail bound, near-circle and near-sphere bounds.**

Lemma 4.34 (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 $\mathbb{E}[\operatorname{sgn}(y) b Z] = 0$. 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 $\mathbb{E}|y + bZ| - |y| \le 2 \cdot \frac{27}{256}\, b^4 \mathbb{E}Z^4/|y|^3$. □

For any remainder $N = \sum \gamma_i \chi_i$ with $\sum \gamma_i^2 = 1$ we have $\mathbb{E}|N| \le 1$ and $\mathbb{E}N^4 = 3 + \kappa_4 \sum \gamma_i^4 \le E_4' := 3 + \max(0, \kappa_4)$ by Lemma 4.6 (as $0 \le \sum \gamma_i^4 \le 1$).

Lemma 4.35 (near-circle tests)**.** *Let B be a box with $r_1 > 0$ (of either kind). 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, b^+ an upper bound of $\sqrt{1-r_1^2}$, 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 $\mathbb{E}|L| < T$ at every point of B with $r < 1$ at which $G := \mathbb{E}|c\chi_1 + sd\chi_2| \leq T$.

(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 $e_j^+ = \min\left(b^+, \frac{27}{128}(b^+)^4 E_4/(r_1^3 \eta_j^3)\right)$ ($e_j^+ = b^+$ 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 4.34 with $Z = M$. Here $\mathbb{E}M^4 = 3 + \kappa_4 p_4 \leq E_4$ by Lemma 4.6, since $p_4 \leq m^2 \leq \min(1, \bar{m}(B))^2$ and $\kappa_4 = w - 4 \leq w^+ - 4$; also $\mathbb{E}|M| \leq 1$. This gives $\mathbb{E}|L| \leq rG + \sum_j p_j e_j$, where $e_j = \min(b, \frac{27}{128} b^4 E_4/(r^3|y_j|^3))$. (A) Since $1 - r = b^2/(1+r)$ and $b > 0$, $\sum_j p_j e_j \leq \frac{27}{128} \frac{b^4 E_4}{r^3} \sum_j \frac{p_j}{|y_j|^3} \leq b^2 \cdot \frac{27}{128} E_4 (b^+)^2 \frac{1}{r_1^3} \sum_j \frac{p_j^+}{\eta_j^3} < \frac{b^2 T^-}{1+r_2} \leq T(1-r)$. With $G \leq T$, $\mathbb{E}|L| < rT + T(1-r) = T$. (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 $T^- - G^+ \geq 0$. □

Boxes of kind ncA pass test (A) or test (B); boxes of kind ncB pass test (B). The hypothesis $G \leq T$ of (A) is supplied in each regime by Lemma 4.16.

Positive peeling. At a point with $r < 1$ we use the peeling of Lemma 4.25, 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 4.25, 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). For $j = 1$, "positively peeled through $[m_1, m_2]$" means $\beta_{i_0} = +m$ for some $i_0 \geq 3$ with $m \in [m_1, m_2]$; then $a_3 = bm$ and $b_1 = b\sqrt{1-m^2}$.

Lemma 4.36 (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*

$$\mathbb{E}|L| \leq \mathbb{E}|Y_n| + \sum_l p_l \min\left(b_j,\ \frac{27}{128}\frac{b_j^4 E_4'}{|y_l|^3}\right). \tag{4.10}$$

Suppose moreover that all $y_l \neq 0$, that $\frac{27}{128} E_4' b_j^2 (1 + r_n) \sum_l p_l |y_l|^{-3} < T$, and that the main-term bound *$G_n(c) \leq T|c|$ holds for $c = (a_1, sa_2, a_3, \dots, a_n)$. Then $\mathbb{E}|L| < T$ if $b_j > 0$, and $\mathbb{E}|L| = \mathbb{E}|Y_n| = G_n(c) \leq T$ if $b_j = 0$.*

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 4.34 with $Z = M^{(j)}$ gives (4.10). Under the extra hypotheses, $\mathbb{E}|Y_n| = G_n(c) \leq Tr_n$, as $|c| = r_n$. If $b_j > 0$, the hypothesis and

$1-r_n = b_j^2/(1+r_n)$ give $\sum_l p_l \frac{27}{128}\frac{b_j^4 E_4'}{|y_l|^3} < T\frac{b_j^2}{1+r_n} = T(1-r_n)$, hence $\mathbb{E}|L| < Tr_n + T(1-r_n) = T$ by (4.10). If $b_j = 0$, then $r_n = 1$ and $\mathbb{E}|L| = \mathbb{E}|Y_n| = G_n(c) \le T$. □

In the applications 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 $a_2 \ge |\alpha_{l_1}| = a_3$.
Piece tests (A_n), (B_n). Let B be a box with sign s and $b^- > 0$, let $j \ge 1$, $n = j+2$, 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 $r_n \le r_n^+ := \min(1, \sqrt{1-(b_j^2)^-})$. The 2^n atoms y_l, the probabilities p_l and the products $p_l y_l = \tau \sum_i (\pm c_i) \prod_{i' \ne i} \mathbb{P}[\cdot]$ (by $qu = (1-q)v = \tau$, as in Lemma 4.16; $c = (a_1, sa_2, a_3, \dots, a_n)$) 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 $\eta_l > 0$ and $\frac{27}{128} E_4'^+ (b_j^2)^+ (1+r_n^+) \sum_l p_l^+ \eta_l^{-3} < T^-$;
- test ($\mathrm{A}_n^{\mathrm{OR}}$) if it passes ($\mathrm{A}_n$), $s = 1$, and $a_i^- > q^+ \sum_{i'=1}^n a_{i'}^+$ for $i = 1, \dots, n$;
- 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 $\eta_l = 0$.

Lemma 4.37 (piece tests)**.** *Consider a point of B that is positively peeled through $I_1, \dots, I_j$, with $u \in [u_1, u_2]$.*

(i) If the piece passes (B_n), then $\mathbb{E}|L| < T$ (for either sign s).
(ii) If the piece passes (A_n) and the main-term bound $G_n(c) \le T|c|$ holds at the point, then $\mathbb{E}|L| < T$ if $b_j > 0$, and $\mathbb{E}|L| = G_n(c) \le T$ if $b_j = 0$.
(iii) If the piece passes ($\mathrm{A}_n^{\mathrm{OR}}$), then $a_i > q \sum_{i'} a_{i'}$ for all i, and $G_n(c) = 2\tau(1-q)^{n-1} \sum_i a_i \le T_n|c|$ (Lemma 4.18).

Proof. All quantities above lie in their enclosures, $E_4' \le E_4'^+$ (as $\kappa_4 = w - 4$ and $w \le w^+$), and $T^- \le T(u)$ by (4.3). (i) follows from (4.10), since $\mathbb{E}|Y_n| = \sum_l |p_l y_l|$. (ii) is Lemma 4.36. (iii) $\sum_{i'} a_{i'}^+ > 0$, so $a_i \ge a_i^- > q^+ \sum_{i'} a_{i'}^+ \ge q \sum_{i'} a_{i'}$, and $s = 1$ gives $c = (a_1, \dots, a_n)$ with positive entries. □

4.11. ***m*-split boxes for $k = 2, 3$.** In Sections 6 and 7 the extremiser $(e_1 + e_2 + e_3)/\sqrt{3}$ is, in the coordinates of Section 4.7, 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 $m = \max_{i \ge 3} |\beta_i|$ and the sign of a largest remaining coefficient.

Definition 4.38 (*m*-split box, first kind)**.** 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 $2m_c^2 > 1$ by Lemma 4.8; 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 (A_3) or (B_3), whose union contains $[m_c, \min(1, \bar{m}(B))]$.

Lemma 4.39 (*m*-split lemma, first kind)**.** *Let B be an m-split box, and suppose that $G_3(c) \le T|c|$ for all $c \in \mathbb{R}^3$ at the values of q considered. At every point of B with $r < 1$ we have $\mathbb{E}|L| \le T$. Equality forces $m = 1$, $\beta_{i_0} = +1$ for some i_0 (that is, $\alpha = a_1 e_1 + sa_2 e_2 + be_{i_0}$), 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 4.23: $\mathbb{E}|L| < T$. 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 4.8; use $c^{(2)}$ and Lemma 4.23: $\mathbb{E}|L| < T$. Otherwise $\beta_{i_0} = +m$ for some i_0, and $m \in [m_c, \min(1, \bar{m}(B))]$ lies in a piece, through which the point is positively peeled. Lemma 4.37 gives $\mathbb{E}|L| < T$ unless $b_1 = 0$, i.e. $m = 1$, and then $\mathbb{E}|L| = G_3(a_1, sa_2, b) \le T$. □

5. The central range: $R(q) = 2\sqrt{q(1-q)}$ if and only if $q_2 \le q \le 1 - q_2$

Theorem 5.1 (the central range)**.** [computer-assisted, see Sec. 16]

(a) For every $q \in [q_2, 1-q_2]$, every $n \ge 1$ and every $\alpha \in \mathbb{R}^n$ with $|\alpha| = 1$,

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

Consequently $R(q) = 2\sqrt{q(1-q)}$ for $q \in [q_2, 1-q_2]$.

(b) For $q \in (0, q_2) \cup (1-q_2, 1)$, $R(q) \ge 2\sqrt{2}\max(q, 1-q)\sqrt{q(1-q)} > 2\sqrt{q(1-q)}$. Hence $\{q : R(q) = 2\sqrt{q(1-q)}\} = [q_2, 1-q_2]$.

(c) (Extremisers.) For $q \in (q_2, 1-q_2)$, equality in (a) holds if and only if $\alpha = \pm e_j$. For $q \in \{q_2, 1-q_2\}$, 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 two-coefficient example of [BF3, Remark 9.8(c)] (see also [St, Section 4.2]), proved in Lemma 5.2. Part (a) for $q \in [\frac{3}{8}, \frac{5}{8}]$ is [BF3, Theorem K]; the proof below does not use it. By Lemma 4.1 we take $q \le \frac{1}{2}$, i.e. $u \ge 1$, in (4.1). The interval $q \in [q_2, \frac{1}{2}]$ corresponds to $u \in [1, u_2]$, $u_2 = \sqrt{1+\sqrt{2}}$, since $(1-q_2)/q_2 = 1/(\sqrt{2}-1) = 1+\sqrt{2}$. We fix the rational number

$$\bar{u}_0 = \frac{776887}{500000} = 1.553774 > u_2$$

(indeed $\bar{u}_0^4 - 2\bar{u}_0^2 - 1 > 0$, which is equivalent to $\bar{u}_0^2 > 1+\sqrt{2}$). The target is $T = T_1 = 2\tau$, and by Lemma 4.3, for $|\alpha| = 1$ reduced as in Section 4.6 ($a = \alpha_1 = \max|\alpha_i| \in (0,1)$, $L = a\chi_1 + bM$ with $b = \sqrt{1-a^2}$ and $\max_{i\ge 2}|\beta_i| \le \min(1, a/b)$),

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

5.1. **Six-moment cells.** The one-coordinate route of Section 4.6 is used with $k = 1$, $D = 6$ and the six-moment objective bound. On $u \le \bar{u}_0$ we have $w^+ < 2.83 < 13$. For $k = 1$ and a cell $[u_1, u_2] \times [\underline{a}, \overline{a}]$ (here u_1, u_2 are the ends of the cell, not thresholds), Definition 4.13 reads: (V1)–(V3) as stated, and (V4) the polynomial $h(r) = \tau(u_2)(1-\overline{a}) - A - \bar{B}r - \Gamma r^2 - \varepsilon r^4$ of Definition 4.9 (with $m^* = \bar{m}$) satisfies $h > 0$ on $[0, \bar{m}]$; and Lemma 4.15 gives $\mathbb{E}R_a(bM) < \tau(u)(1-a)$ for $u \in [u_1, u_2]$, $a \in [\underline{a}, \overline{a}]$.

5.2. **The quartic two-extremiser certificate.** Near $(q, a) = (q_2, 1/\sqrt{2})$ two configurations are extremal: e_1 and $(e_1+e_2)/\sqrt{2}$. No six-moment certificate can work at that point, because the target $\tau(1-a)$ is attained there with $M = \chi_2$: a law with the first four moments of χ is the law of χ, since $\mathbb{E}[(M-u)^2(M+v)^2]$ is determined by these moments and vanishes, so the six-moment relaxation is exact at $(e_1+e_2)/\sqrt{2}$. Instead we compare L with $a\chi_1 + b\chi_2$.

Lemma 5.2 (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 $q \le \frac{1}{2}$, $\mathbb{E}|\chi_1 + \chi_2|/\sqrt{2} = 2\sqrt{2}(1-q)\tau$, which exceeds 2τ if and only if $q < q_2$.*

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 4.3, $\mathbb{E}|a\chi_1 + b\chi_2| = 2\tau a + 2q(1-q)(bu - av) = 2\tau a + 2(1-q)\tau b - 2q\tau a = 2\tau(1-q)(a+b)$, 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. $q \le \frac{1}{2}$. 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

$$B_0 = \tau^4\big(2a - b(u^2-1)\big), \quad s = \tau^3(bu^2 - a), \quad B = B_0 - 2c_4u, \quad G = s - B_0u + c_4u^2, \tag{5.1}$$

and

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

(Here s and G are local symbols.) 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 5.3 (algebraic identities)**.** *The following hold identically in u, a, b, c_4 (with q, v, τ given by (4.1)):*

(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) $P(y) - \ell_1(y) = (y-u)^2 S_1(y)$ *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 $z_0 = au/b$*,* $\delta = z_0 - v$*,* $g_1 = 2c_4z_0 - B$ *and* $g_0 = c_4z_0^2 - Bz_0 + G$*. Then for all* x*,*

$$P(-z_0 - x) - \ell_2(-z_0 - x) = e_0 + e_1x + e_2x^2 + e_3x^3 + c_4x^4,$$

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 $\kappa_3c_3 + 2\kappa_4c_4 = \kappa_3B_0 - 2c_4(\kappa_3^2 - \kappa_4)$, and $\kappa_3^2 - \kappa_4 = u^2 - 2uv + v^2 - u^2 - v^2 + 4 = 2$ because $uv = 1$.

(ii): $4c_4G - B^2 = 4c_4s - 4c_4B_0u + 4c_4^2u^2 - (B_0^2 - 4c_4uB_0 + 4c_4^2u^2) = 4c_4s - B_0^2$.

(i): $P(u) = (u+v)^2 S_0(u)$ and $S_0(u) = c_4u^2 + Bu + G = s$ by (5.1), 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 $S_0'(u) = 2c_4u + B = B_0$. This gives

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

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 $P - \ell_1 = (y-u)^2(c_4y^2 + d_1y + d_0)$. Comparing coefficients of y^3 and y^2 gives $d_1 = c_3 + 2uc_4 = B_0 + 2vc_4$ and $d_0 = c_2 + 2ud_1 - u^2c_4$, where $c_2 = G + 2vB + v^2c_4$. Substituting: $d_0 = s + B_0(u + 2v) + c_4v^2$. Then $d_1^2 - 4c_4d_0 = B_0^2 + 4c_4vB_0 + 4c_4^2v^2 - 4c_4s - 4c_4B_0(u+2v) - 4c_4^2v^2 = B_0^2 - 4c_4(s + B_0(u+v))$.

(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 $S_0(-z_0 - x) = c_4(z_0 + x)^2 - B(z_0 + x) + G = c_4x^2 + g_1x + g_0$. Expanding $(\delta^2 + 2\delta x + x^2)(c_4x^2 + g_1x + g_0) - qbx$ gives the stated coefficients. □

Lemma 5.4 (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* $4c_4s - B_0^2 > 0$*;*
(Q3) $e_0 > 0$ *and* $e_2 - \dfrac{(e_1^-)^2}{4e_0} - \dfrac{(e_3^-)^2}{4c_4} > 0$*, where* $x^- = \min(x, 0)$*;*
(Q4) $\kappa_3B_0 - 4c_4 > 0$.

(There is no condition (Q2): the positivity of S_1 follows from (Q1), see Step 2.) 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: $P \ge 0$. Since $bu^2 > a$, $s > 0$; by Lemma 5.3(ii) the discriminant of S_0 is $B_0^2 - 4c_4 s$, which is negative by (Q1). With $c_4 > 0$ this gives $S_0 > 0$ on $\mathbb{R}$, hence $P = (y+v)^2 S_0 \ge 0$.

Step 2: $P \ge \ell_1$. By Lemma 5.3(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 $P - \ell_1 = (y-u)^2 S_1 \ge 0$.

Step 3: $P \ge \ell_2$. If $y \ge -z_0 = -au/b$, then $\ell_2(y) = -q(by + au) \le 0 \le P(y)$. If $y < -z_0$, write $y = -z_0 - x$ with $x > 0$. By Lemma 5.3(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 $\ge e_0 > 0$ if $e_1 \ge 0$, and equals $(\sqrt{e_0} + e_1 x/(2\sqrt{e_0}))^2 \ge 0$ if $e_1 < 0$. In the second bracket, $D := e_2 - \eta > (e_3^-)^2/(4c_4) \ge 0$ by (Q3). If $e_3 \ge 0$ the bracket is $\ge D > 0$ for $x \ge 0$. If $e_3 < 0$ it is $\ge D - e_3^2/(4c_4) > 0$. Hence $f(x) > 0$ for $x > 0$. So $P \ge \max\{0, \ell_1, \ell_2\} = R_a(b\,\cdot)$ on $\mathbb{R}$, and $\mathbb{E}R_a(bM) \le \mathbb{E}P(M)$.

Step 4: comparison with χ. P has degree 4. By Lemma 4.6, $\mathbb{E}P(M) = c_0 + c_2 + c_3\kappa_3 p_3 + c_4(3 + \kappa_4 p_4)$, 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 $p_3^2 \le p_4 \le 1$ (Lemma 4.7), so $|p_3| \le 1$. Therefore

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

The first inequality uses $c_4\kappa_4 \le 0$ and $1 - p_4 \le 1 - p_3^2$. The second uses $1 - p_3 \ge 0$, $c_4\kappa_4 \le 0$ and $1 + p_3 \le 2$. The last equality is Lemma 5.3(iv).

Step 5. By Lemma 5.3(v), $\mathbb{E}R_a(bM) \le \mathbb{E}P(M) \le q(1-q)(bu - av) - (1-p_3)(\kappa_3 B_0 - 4c_4)$. By Lemma 4.3 and Lemma 5.3(v), $\mathbb{E}|a\chi_1 + bM| \le 2\tau a + 2q(1-q)(bu - av) - 2(1-p_3)(\kappa_3 B_0 - 4c_4) \le 2\tau(1-q)(a+b)$, with strict inequality if $p_3 < 1$, by (Q4). □

Corollary 5.5 (quartic bound for $q \ge q_2$)**.** *Under the hypotheses of Lemma 5.4, if moreover $q \ge q_2$ (i.e. $u \le u_2$), then $\mathbb{E}|a\chi_1 + bM| \le 2\tau$. Equality forces $q = q_2$, $a = b = 1/\sqrt{2}$ and $M = \chi_j$ for a single j.*

Proof. $(1-q)(a+b) \le (1-q)\sqrt{2(a^2+b^2)} = \sqrt{2}(1-q) \le \sqrt{2}(1-q_2) = 1$. Equality needs $a = b$, $q = q_2$ 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 $\beta_i \le 1$; so every $\beta_i \in \{0, 1\}$, and exactly one $\beta_j = 1$. □

5.3. **The near-dictator range.**

Lemma 5.6 (near-dictator bound)**.** *Let $u \in [1, u_2]$, $a \in [\frac{9}{10}, 1)$, $b = \sqrt{1-a^2}$, and let $M = \sum \beta_i \chi_i$ with $\sum \beta_i^2 = 1$. Then $\mathbb{E}R_a(bM) \le 0.9402\,\tau(1-a)$.*

Proof. For $t > 0$ and all real x we have $(x-t)_+ \le \frac{27}{256\,t^3} x^4$. 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

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

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 4.6, $\mathbb{E}M^4 = 3+\kappa_4 p_4 \le 3$, 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_2. 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 $\frac{486}{256}\cdot\frac{(1/10)(19/10)^2}{(9/10)^3} = 0.940104\ldots < 0.9402$. □

5.4. **The certified data.** The region

$$\mathcal{S} = [1,\bar{u}_0]\times[0,\tfrac{9}{10}]\setminus\big((\tfrac{611}{400},\bar{u}_0]\times(\tfrac{16}{25},\tfrac{77}{100})\big)$$

is the union of the eight rectangles in Table 3.

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 3. The six-moment cover of $\mathcal{S}$ (Theorem 5.1). Cell widths range from 0.0079 to 0.139 in u and from 0.0040 to 0.0325 in a.

For the quartic boxes we 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 $[0,1]$. Since $a(\frac{9}{25}) = \frac{225}{353} < \frac{16}{25}$ and $a(\frac{471}{1000}) = \frac{942000}{1221841} > \frac{77}{100}$, the box $\mathcal{Q} = [\frac{611}{400},\bar{u}_0]\times[\frac{9}{25},\frac{471}{1000}]$ in the (u,t)-plane contains a preimage of every $(u,a) \in [\frac{611}{400},\bar{u}_0]\times[\frac{16}{25},\frac{77}{100}]$.

Proposition 5.7 (certified data for Theorem 5.1)**.** [computer-assisted, see Sec. 16]

(i) Each of the eight rectangles of Table 3 is tiled by cells $[u_1,u_2]\times[\underline{a},\overline{a}]$ (379 in all), each of which has a cell certificate (Definition 4.13 with $k=1$, $D=6$, the six-moment objective bound, $\bar{b} = \lceil\sqrt{1-\underline{a}^2}\rceil_{15}$, and $\bar{m} = 1$ if $\overline{a}^2 \ge \frac{1}{2}$, otherwise $\bar{m} = \min\{1, \overline{a}/\lfloor\sqrt{1-\overline{a}^2}\rfloor_{15}\}$).

(ii) $\mathcal{Q}$ is tiled by 641 boxes in the (u,t)-plane (widths 0.0008 to 0.0033 in u and 0.0017 to 0.0069 in t), each with a rational constant $c_4 > 0$ such that $bu^2-a>0$, $au^2-b>0$, (Q1), (Q3) and (Q4) of Lemma 5.4 hold at every (u,t) of the box.

(iii) 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 $[1,\bar{u}_0]\times[0,1]$.

How it is verified. (i) For each cell, 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; this is (V1)–(V3). (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 $(0,\bar{m}]$. The numbers $\bar{b},\bar{m}$, the lines and the cumulant enclosures are recomputed from the cell corners, and $\bar{b}^2 \ge 1-\underline{a}^2$ and $\lfloor\sqrt{1-\overline{a}^2}\rfloor_{15}^2 \le 1-\overline{a}^2$ are asserted exactly. (ii) For each box, with its c_4, all quantities are evaluated in outward-rounded interval arithmetic (120 bits) from the formulas (5.1): the coefficients of P by

expanding $(y+v)^2 S_0$, and the e_k by a Taylor shift of P at $-z_0$; each stored box is subdivided (with the same c_4) until all conditions hold (20 969 sub-boxes in all). For (Q3) the conservative form $e_2 - \sigma_1 e_1^2/(4e_0) - \sigma_3 e_3^2/(4c_4) > 0$ is used, 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 $e \ge 0$. (Q4) is required strictly; the smallest certified lower bound of $\kappa_3 B_0 - 4c_4$ over all boxes is $1.77 \cdot 10^{-3}$. (iii) Within each rectangle and within $\mathcal{Q}$, the cells lie in the rectangle, have pairwise disjoint interiors and total area equal to the area of the rectangle, in exact arithmetic; then their closed union is the whole rectangle, since a closed subset of full measure of a rectangle is dense. The cover of $[1, \bar{u}_0] \times [0, 1]$ is checked on the grid formed by all breakpoints. The cumulant identities used in (V4) are those of Lemma 4.4. The recorded data are not in the code archive; data regenerated for this paper (a tiling of the eight rectangles by 348 cells, and the same 641 boxes) are accepted by the same verifier (Section 16.5). □

5.5. **Proof of Theorem 5.1.** *(a)* By Lemma 4.1 we may assume $q \in [q_2, \frac{1}{2}]$, i.e. $u \in [1, u_2]$. Let $|\alpha| = 1$ and reduce to $a = \alpha_1 = \max|\alpha_i| > 0$ as in Section 4.6. If $a = 1$ then $\mathbb{E}|L| = 2\tau$. Let $0 < a < 1$. It suffices to show $\mathbb{E}R_a(bM) \le \tau(1-a)$. Since $u \le u_2 < \bar{u}_0$, the point (u, a) lies in $[1, \bar{u}_0] \times (0, 1)$, and by Proposition 5.7(iii) one of the following applies (we take the first that applies).

(1) $a \ge \frac{9}{10}$: Lemma 5.6 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 box of Proposition 5.7(ii), so the hypotheses of Lemma 5.4 hold at (u, a, b) with that box's c_4 (note $1 < \frac{611}{400} \le u < \frac{19}{10}$). By Corollary 5.5 (here $q \ge q_2$), $\mathbb{E}|L| \le 2\tau$.
(3) Otherwise $(u, a) \in \mathcal{S}$, so it lies in a cell of Proposition 5.7(i), and Lemma 4.15 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 4.1 let $q < q_2 \le \frac{1}{2}$. Lemma 5.2 with $a = b = 1/\sqrt{2}$ gives $R(q) \ge \sqrt{2}(1-q)\,2\tau > 2\tau$.

(c) Let $q \in [q_2, \frac{1}{2}]$ 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 5.5 gives $q = q_2$, $a = b = 1/\sqrt{2}$ 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_2 by Lemma 5.2, since $\sqrt{2}(1-q_2) = 1$. If $a = 1$ then $\alpha = \pm e_j$. For $q \in [\frac{1}{2}, 1-q_2]$ use Lemma 4.1. □

6. The regime $k = 2$: $R(q) = 2\sqrt{2}\,(1-q)\sqrt{q(1-q)}$ for $q_3 \le q \le q_2$

Theorem 6.1 (the regime $k = 2$)**.** [computer-assisted, see Sec. 16] *Let $T = T_2 = 2\sqrt{2}\,(1-q)\tau$.*

(a) For every $q \in [q_3, q_2]$, every $n \ge 1$ and every $\alpha \in \mathbb{R}^n$ with $|\alpha| = 1$,

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

For $q \in [1-q_2, 1-q_3]$ the same holds with $1-q$ replaced by q. Consequently $R(q) = 2\sqrt{2}\max(q, 1-q)\sqrt{q(1-q)}$ for $q \in [q_3, q_2] \cup [1-q_2, 1-q_3]$.

(b) (Extremisers.) Let $q \in [q_3, q_2] \cup [1-q_2, 1-q_3]$. Equality in (a) holds if and only if $\alpha = \pm\frac{1}{\sqrt{2}}(e_i + e_j)$ with $i \ne j$, or $q \in \{q_2, 1-q_2\}$ 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 $q \in (0, q_3)$, $R(q) \ge 2\sqrt{3}\,(1-q)^2\tau > T(q)$. For $q \in (q_2, \frac{1}{2}]$, $R(q) \ge 2\tau > T(q)$. Hence $\{q \in (0, \frac{1}{2}] : R(q) = T(q)\} = [q_3, q_2]$.

Parameters. By Lemma 4.1 we take $q \le \frac{1}{2}$. The range $q \in [q_3, q_2]$ corresponds to $u \in [u_2, u_3]$. We fix the rationals

$$U_- = \frac{1553773}{1000000} < u_2, \qquad U_+ = \frac{1054691}{500000} = 2.109382 > u_3$$

(indeed $U_-^4 - 2U_-^2 - 1 < 0$, and $U_+^2 > 2$ with $(U_+^2 - 2)^2 > 6$), and $A_S = \frac{9}{20}$. The computations cover $u \in [U_-, U_+]$; the theorem uses only $u \in [u_2, u_3]$. The lower bound $T^-(u_1, u_2)$ is (4.3) with $k = 2$ and $S_2 = \lfloor\sqrt{2}\rfloor_{15}$. By (4.4): for $q \le \frac{1}{2}$, $2\tau \le T$ iff $q \le q_2$; and for $q < \frac{1}{3}$, $T_3 \le T$ iff $q \ge q_3$.

Lemma 6.2 (two coordinates for $k = 2$)**.** *If $q \le q_2$, then $\mathbb{E}|c\chi_1 + sd\chi_2| \le T\sqrt{c^2 + d^2}$ for $c, d \ge 0$, and for $(c, d) \ne 0$ equality holds if and only if $s = 1$ and $c = d$, or $q = q_2$ and $cd = 0$.*

Proof. By Lemma 4.16, $\mathbb{E}|X| = \max(2\tau \max(c, d), [s = 1]\, 2\tau(1 - q)(c + d))$, with $2\tau \max(c, d) \le T_1\rho \le T\rho$ (equality iff $cd = 0$ and $T_1 = T_2$, i.e. $q = q_2$) and $2\tau(1 - q)(c + d) \le T\rho$ (equality iff $c = d$). □

Lemma 6.3 (three-bit lemma, $k = 2$)**.** [computer-assisted, see Sec. 16] *Let $q \in [q_3, q_2]$ 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 one of: $\pm(e_i + e_j)$ $(i \ne j)$; $\pm(e_1 + e_2 + e_3)$, and then $q = q_3$; $\pm e_i$, and then $q = q_2$.*

Proof. 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 $[q_3, q_2]$. Moreover $P_f \equiv 0$ exactly for $f = \pm(2 \cdot \mathbf{1}\{x_i \vee x_j\} - 1)$ (six functions); $P_f(q_3) = 0 \ne P_f$ exactly for $f = \pm(2 \cdot \mathbf{1}\{x_1 \vee x_2 \vee x_3\} - 1)$; and $P_f(q_2) = 0 \ne P_f$ exactly for $f = \pm(2x_i - 1)$. Given the claim, Lemma 4.17 with $B^2 = 8(1-q)^2$ gives $G_3(c) \le \tau|c|\sqrt{8}(1-q) = T|c|$.

The claim is a finite exact computation, carried out as described in Section 4.7: P_f is a polynomial with rational coefficients of degree ≤ 4; with $g_3 = 3q^2 - 6q + 1$ and $g_2 = 2q^2 - 4q + 1$, the minimal polynomials of q_3 and q_2, and rational enclosures $q_3 \in [q_3^-, q_3^+]$, $q_2 \in [q_2^-, q_2^+]$ of width 10^{-15}: (i) by Sturm sequences, P_f has no root in $[q_3^+, q_2^-]$, and $P_f(q_3^+) > 0$; (ii) near q_3: if $g_3 \mid P_f$, write $P_f = g_3 Q$; then Q has no root in $[q_3^-, q_3^+]$ and $Q(q_3^+) < 0$, so $P_f \ge 0$ on $[q_3, q_3^+]$ (as $g_3 \le 0$ on $[q_3, 1]$); otherwise P_f has no root in $[q_3^-, q_3^+]$ and $P_f(q_3^+) > 0$; (iii) near q_2, in the same way with g_2 (which is ≥ 0 on $[0, q_2]$) and $Q(q_2^-) > 0$. The six functions with $P_f \equiv 0$ are $\pm$ the OR of two bits, by (4.8) ($\Delta(f) = 2(1 - q)(e_i + e_j)$).

Equality. Suppose $G_3(c) = T|c|$ with $c \ne 0$. By Lemma 4.17, $P_{f^*}(q) = 0$ 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 $q = q_2$ and $f^* = \pm(2x_i - 1)$, with $\Delta = \pm 2e_i$. Conversely, these c attain $T|c|$ by Theorem 4.2 and Lemma 6.2. □

For $k = 2$ the near-circle test (A) of Lemma 4.35 applies at points with $u \ge u_2$ (where $G \le T$ by Lemma 6.2), and the m-split lemma 4.39 at points with $u \in [u_2, u_3]$ (where Lemma 6.3 holds). The piece test (A_3) and the near-circle test (A) bound only the error term; the main term is bounded by Lemma 6.3, valid only for $q \ge q_3$, and by Lemma 6.2, valid only for $q \le q_2$. This is why the theorem stops at u_2 and u_3.

Proposition 6.4 (certified data for Theorem 6.1)**.** [computer-assisted, see Sec. 16]

(i) The rectangle $[U_-, U_+] \times [0, \frac{9}{20}]$ is tiled by 784 cells (450 with $u \in [U_-, 2]$, 334 with $u \in [2, U_+]$), each with a cell certificate (Definition 4.13, $k = 2$, $D = 6$, six-moment objective bound) and $\Theta_1 > 0$.

(ii) For each sign s, the box $[U_-, U_+] \times [0, T_8] \times [\frac{9}{20}, 1]$ is tiled by boxes B (Section 4.8), each of one of the kinds: lp (a box certificate for $(B, s, \min(1, \bar{m}(B)), -)$); ncA/ncB (the box passes test (A) or (B) of Lemma 4.35); small ($r_2 c(t_1) \le \frac{9}{20}$); ms (an m-split box of the first kind, Definition 4.38, with $u_1 \ge 2$). The counts are in Table 4.

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 4. Two-coordinate boxes for Theorem 6.1 (55 515 in all). Widths range from $1.25\cdot10^{-3}$ to 0.01 in u, from $8.1\cdot10^{-4}$ to 0.052 in t and from $1.6\cdot10^{-3}$ to 0.05 in r. All ms boxes have $u\ge 2.09$; they carry 1 669 pieces (1 659 of type (A_3), 10 of type (B_3)), with $m_c\in\{\frac{31}{40},\frac{4}{5},\frac{33}{40},\frac{17}{20},\frac{7}{8},\frac{9}{10}\}$.

How it is verified. Cells: (V1)–(V3) by Sturm sequences; $\Theta_1>0$; (V4) strictly by Sturm on $[0,\bar m]$. (In fact $S_2\frac{u_1^2}{1+u_1^2}\ge 1.414\cdot 0.707>\frac{9}{20}\ge\overline{a}$, so $\Theta_1>0$.) 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; the verifier recomputes $\bar m(B)$ as the exact quotient $r_2d(t_2)/b^-$. For ms boxes also $0<m_c\le 1$, $2m_c^2>1$, $p^*<0$, $p^*\ge\varphi(m_c)$ (as $(p^*+m_c^3)^2\ge(1-m_c^2)^3$ with $p^*+m_c^3\ge 0$), and $m^*=\min(m_c,\bar m)$ for $c^{(1)}$; the pieces cover $[m_c,\min(1,\bar m)]$, and each passes (A_3) or (B_3) in outward-rounded interval arithmetic (120 bits). Near-circle boxes: tests (A)/(B) strictly in interval arithmetic (120 bits). Coverage (exact): the cells and, for each sign, the boxes lie in their region, have pairwise disjoint interiors and total volume equal to the volume of the region, so their closed union is the region. Also $U_-<u_2$, $U_+\ge u_3$, $T_8\ge\sqrt{2}-1$, and every small box has $r_2c(t_1)\le\frac{9}{20}$. □

Proof of Theorem 6.1. *(a)* By Lemma 4.1 let $q\in[q_3,q_2]$, i.e. $u\in[u_2,u_3]\subset[U_-,U_+]$. Reduce α as in Section 4.7.

(1) $a_1=1$: $\alpha=e_1$ and $\mathbb{E}|L|=2\tau\le T$, with equality iff $q=q_2$.
(2) $a_1\le\frac{9}{20}$: (u,a_1) lies in a cell, and Lemma 4.15 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 6.2 gives $\mathbb{E}|L|\le T$, with equality iff $s=1$ and $a_1=a_2$, or $q=q_2$ 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, and the box is not small, because $a_1>\frac{9}{20}$. If it is lp, Lemma 4.23 with $m^*=\min(1,\bar m(B))\ge m$ gives $\mathbb{E}|L|<T$. If it is ncA or ncB, Lemma 4.35 gives $\mathbb{E}|L|<T$ (here $u\ge u_2$). If it is ms, Lemma 4.39 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 (Theorem 4.2). Hence $R(q)=T(q)$. For $q\in[1-q_2,1-q_3]$ use Lemma 4.1: $R(q)=R(1-q)=2\sqrt{2}\,q\,\tau$.

(b) Equality can occur only in cases (1), (3) and the ms case of (4). Case (1) gives $\alpha=\pm e_j$ at $q=q_2$. Case (3) gives $\alpha=\pm(e_i+e_j)/\sqrt{2}$, or $\alpha=\pm e_j$ at $q=q_2$. In the ms case, Lemma 4.39 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 6.3, (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 (Theorem 4.2). For $q\ge\frac12$ use Lemma 4.1.

(c) For $q<q_3<\frac13$, Theorem 4.2 with $k=3$ and (4.4) give $R(q)\ge 2\sqrt{3}(1-q)^2\tau>T$. For $q\in(q_2,\frac12]$, $R(q)\ge\mathbb{E}|\chi_1|=2\tau>T$. Together with (a) this gives $\{q\le\frac12: R(q)=T(q)\}=[q_3,q_2]$.□

7. The regime $k=3$, upper part: $R(q)=2\sqrt{3}\,(1-q)^2\sqrt{q(1-q)}$ for $q_L\le q\le q_3$

Theorem 7.1 (the regime $k=3$, upper part)**.** [computer-assisted, see Sec. 16] *Let* $T=T_3=2\sqrt{3}\,(1-q)^2\tau$ *and* $q_L=\frac{25}{169}$.

(a) For every $q \in [q_L, q_3]$, every $n \geq 1$ and every $\alpha \in \mathbb{R}^n$ with $|\alpha| = 1$,

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

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 $i \neq j$.

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

Parameters. The range $q \in [q_L, q_3]$ corresponds to $u \in [u_3, \frac{12}{5}]$, since $1/(1+(12/5)^2) = \frac{25}{169}$. We fix

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

(indeed $U_-^2 > 2$ with $(U_-^2-2)^2 < 6$, and $U_+^2 = 5.76 < 3+2\sqrt{3}$), and $A_S = \frac{2}{5}$. The computations cover $u \in [U_-, U_+]$; the theorem uses only $u \in [u_3, U_+]$. The lower bound T^- is (4.3) with $k=3$, $S_3 = \lfloor\sqrt{3}\rfloor_{15}$. By (4.4): (i) for $q \leq \frac{1}{2}$, $T_2 \leq T$ iff $q \leq q_3$, with equality iff $q = q_3$; (ii) for $q \leq q_3$, $2\tau < T_2 \leq T$; (iii) for $q < \frac{1}{4}$, $T_4 > T$ iff $q < q_4$.

Lemma 7.2 (two coordinates for $k=3$)**.** *If $q \leq q_3$, then $\mathbb{E}|c\chi_1 + sd\chi_2| \leq T\sqrt{c^2+d^2}$ for $c,d \geq 0$, and for $(c,d) \neq 0$ equality holds if and only if $q = q_3$, $s = 1$ and $c = d$.*

Proof. By Lemma 4.16: $2\tau\max(c,d) \leq 2\tau\rho < T\rho$ by (ii), and $2\tau(1-q)(c+d) \leq T_2\rho \leq T\rho$ by (i), with equality iff $c = d$ and $q = q_3$; the last entry is present only for $s = 1$. □

Lemma 7.3 (three-bit lemma, $k=3$)**.** [computer-assisted, see Sec. 16] *Let $q \in [q_L, q_3]$ and $c \in \mathbb{R}^3$. Then $G_3(c) \leq T\,|c|$. 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. Claim: for each of the 256 functions $f : \{0,1\}^3 \to \{-1,1\}$, $P_f(q) = 12(1-q)^4 - \sum_{i=1}^{3}\Delta_i(f)^2$ is ≥ 0 on $[q_L, q_3]$. Moreover $P_f \equiv 0$ exactly for $f = \pm\mathrm{OR}_{\{1,2,3\}}$ (two functions); $P_f(q_3) = 0 \neq P_f$ exactly for $f = \pm\mathrm{OR}_{\{i,j\}}$ (six functions); and no $P_f \not\equiv 0$ has a zero in $[q_L, q_3)$. Given the claim, Lemma 4.17 with $B^2 = 12(1-q)^4$ gives $G_3(c) \leq T|c|$.

The claim is checked as in Section 4.7, with g_3 and a rational enclosure $q_3 \in [q_3^-, q_3^+]$ of width 10^{-15} ($g_3(q_3^-) > 0 > g_3(q_3^+)$ and $q_L < q_3^-$ are asserted): (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 $g_3 \mid P_f$, $P_f = g_3 Q$, 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 $P_f(q_3^-) > 0$. The two functions with $P_f \equiv 0$ are $\pm\mathrm{OR}_3$ ($\Delta(\mathrm{OR}_3) = 2(1-q)^2(e_1+e_2+e_3)$), and $\Delta(\mathrm{OR}_{ij}) = 2(1-q)(e_i+e_j)$ gives $P = 12(1-q)^4 - 8(1-q)^2 = 4(1-q)^2 g_3(q)$.

Equality. If $G_3(c) = T|c|$ with $c \neq 0$, Lemma 4.17 and the claim give $f^* = \pm\mathrm{OR}_3$, with $\Delta = \pm 2(1-q)^2(1,1,1)$, or $q = q_3$ and $f^* = \pm\mathrm{OR}_{ij}$, with $\Delta = \pm 2(1-q)(e_i+e_j)$. Conversely, these c attain $T|c|$ by Theorem 4.2 and Lemma 7.2 (at $q = q_3$, $T_2 = T$). □

For $k=3$ the near-circle test (A) applies at points with $u \geq u_3$ (Lemma 7.2), and Lemma 4.39 at points with $u \in [u_3, U_+]$ (Lemma 7.3). In this regime the extremiser $(e_1+e_2+e_3)/\sqrt{3}$ is an interior point of the parameter region for every u in the range, so the m-split is needed throughout; and at $(e_1+e_2)/\sqrt{2}$ we have $\mathbb{E}|L| = T_2 < T$ for $q < q_3$. Both main-term bounds hold only for $q \leq q_3$, which is why the theorem stops at u_3.

Proposition 7.4 (certified data for Theorem 7.1)**.** [computer-assisted, see Sec. 16]

(i) The rectangle $[U_-, U_+] \times [0, \frac{2}{5}]$ is tiled by 2 704 cells, each with a cell certificate ($k = 3$, $D = 6$, six-moment objective bound) and $\Theta_1 > 0$.

(ii) For each sign s, the box $[U_-, U_+] \times [0, T_8] \times [\frac{2}{5}, 1]$ is tiled by boxes of the kinds lp, ncA/ncB, small *($r_2 c(t_1) \le \frac{2}{5}$) and* ms *(with $u_1 \ge 2$), as in Proposition 6.4(ii); the counts are in Table 5.*

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 5. Two-coordinate boxes for Theorem 7.1 (81 975 in all). 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 (A_3), 546 of type (B_3)), with $m_c \in \{\frac{3}{4}, \frac{31}{40}, \frac{4}{5}, \frac{33}{40}, \frac{17}{20}, \frac{7}{8}, \frac{9}{10}\}$.

How it is verified. As for Proposition 6.4, with the target $T^-(u_1, u_2)$ of (4.3) for $k = 3$ (in the interval parts, T^- is computed from an interval enclosure of $\sqrt{3}$). The verifier also asserts $\Theta_1 > 0$ for every cell; indeed $S_3(\frac{u_1^2}{1+u_1^2})^2 \ge S_3(\frac{U_-^2}{1+U_-^2})^2 > 1.15 > \frac{2}{5} \ge \overline{a}$. Also $U_- < u_3$, $U_+ < u_4$ and $T_8 \ge \sqrt{2} - 1$ are asserted. □

Proof of Theorem 7.1. *(a)* By Lemma 4.1 let $q \in [q_L, q_3]$, i.e. $u \in [u_3, U_+] \subset [U_-, U_+]$. Reduce α as in Section 4.7.

(1) $a_1 = 1$: $\alpha = e_1$ and $\mathbb{E}|L| = 2\tau < T$.
(2) $a_1 \le \frac{2}{5}$: (u, a_1) lies in a cell, and Lemma 4.15 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 7.2 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, not small. If it is lp, Lemma 4.23 gives $\mathbb{E}|L| < T$. If it is ncA or ncB, Lemma 4.35 gives $\mathbb{E}|L| < T$ (here $u \ge u_3$). If it is ms, Lemma 4.39 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 (Theorem 4.2, $q < \frac{1}{3}$). Hence $R(q) = T(q)$. For $q \in [1 - q_3, 1 - q_L]$ use Lemma 4.1: $R(q) = R(1 - q) = 2\sqrt{3}\, q^2\tau$.

(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 4.39 gives $\alpha = a_1e_1 + sa_2e_2 + be_{i_0}$ with $G_3(a_1, sa_2, b) = T$ and $a_1, b > 0$, $a_2 \ge b > 0$. By Lemma 7.3, (a_1, sa_2, b) is a positive multiple of $\pm(1, 1, 1)$ (the alternative $\pm(e_i + e_j)$ has a zero entry), so $s = 1$ and $a_1 = a_2 = b$, i.e. $\alpha = (e_1 + e_2 + e_{i_0})/\sqrt{3}$. Undoing the reduction gives the list in (b). Conversely, each listed vector attains T at the stated q (Theorem 4.2; at q_3, $T_2 = T$). For $q \ge \frac{1}{2}$ use Lemma 4.1.

(c) For $q \in (q_3, \frac{1}{2}]$, $R(q) \ge T_2(q) > T(q)$ by (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 (iii). □

8. The regime $k = 3$, lower part: $R(q) = 2\sqrt{3}\,(1 - q)^2\sqrt{q(1 - q)}$ for $q_4 \le q \le q_L$

Theorem 8.1 (the regime $k = 3$, lower part)**.** [computer-assisted, see Sec. 16] *Let $T = T_3 = 2\sqrt{3}\,(1 - q)^2\tau$.*

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

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

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 $q \in (0, q_4)$, $R(q) \geq T_4(q) > T(q)$.

Corollary 8.2 (the whole $k=3$ regime)**.** [computer-assisted, see Sec. 16] *$R(q) = T_3(q)$ for every $q \in [q_4, q_3]$, and $\{q \in (0, \frac{1}{2}] : R(q) = T_3(q)\} = [q_4, q_3]$. 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 7.1(a),(b); on $[q_4, q_L]$ it is Theorem 8.1(a),(b). For $q \in (q_3, \frac{1}{2}]$, $R(q) \geq T_2(q) > T_3(q)$ (Theorem 7.1(c)), and for $q < q_4$, $R(q) \geq T_4(q) > T_3(q)$ (Theorem 8.1(c)). □

Parameters. The range $q \in [q_4, q_L]$ corresponds to $u \in [\frac{12}{5}, u_4]$. We fix

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

(indeed $U_+^2 > 3$ and $(U_+^2-3)^2 \geq 12$, so $U_+^2 \geq 3+2\sqrt{3}$), and put $q_U = 1/(1+U_+^2) \leq q_4$. Since $u_3 < U_-$, every q in the range satisfies $q < q_3$. We put $A_S = \frac{7}{20}$. The computations cover $u \in [U_-, U_+]$; the theorem uses only $u \in [U_-, u_4]$. In (4.3) the verifier uses a rational lower bound S_3 of $\sqrt{3}$ ($N = 10^{15}$) in exact arithmetic and an outward-rounded enclosure of $\sqrt{3}$ in its interval parts; rational bounds of square roots in the patch enclosures use $N = 10^{12}$. By (4.4): for $q \leq q_3$, $2\tau < T_2 \leq T$; and for $q < \frac{1}{4}$, $T_4 \geq T$ iff $q \leq q_4$, with equality iff $q = q_4$. Lemma 7.2 applies on the whole range ($q < q_3$): $\mathbb{E}|c\chi_1 + sd\chi_2| < T\sqrt{c^2+d^2}$ for $(c,d) \neq 0$.

Lemma 8.3 (three- and four-bit lemmas, $k=3$ lower part)**.** [computer-assisted, see Sec. 16] *Let $c \neq 0$.*

(a) If $q \in [q_U, q_L]$ and $c \in \mathbb{R}^3$, then $G_3(c) \leq T|c|$, with equality iff c is a positive multiple of $\pm(e_1+e_2+e_3)$.

(b) If $q \in [q_4, q_L]$ and $c \in \mathbb{R}^4$, then $G_4(c) \leq T|c|$, with equality iff 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. For $f : \{0,1\}^n \to \{-1,1\}$ put $H_f(q) = 12(1-q)^4 - \sum_{i=1}^n \Delta_i(f)^2$. *Claims* (finite exact computations):

(C1) ($n=3$, all 2^8 functions) $H_f \geq 0$ 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) $H_f \geq 0$ 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, Lemma 4.17 with $B^2 = 12(1-q)^4$ gives $G_n(c) \leq T|c|$ on the stated ranges. If equality holds, $H_{f^*}(q) = 0$ and c is a positive multiple of $\Delta(f^*)$; by the claims and (4.8): for $n=3$, $f^* = \pm\mathrm{OR}_{\{1,2,3\}}$ and $\Delta(f^*) = \pm 2(1-q)^2(1,1,1)$; for $n=4$, either $f^* = \pm\mathrm{OR}_S$ with $|S|=3$ and $\Delta(f^*) = \pm 2(1-q)^2\sum_{i\in S} e_i$, or $q = q_4$, $f^* = \pm\mathrm{OR}_{\{1,2,3,4\}}$ and $\Delta(f^*) = \pm 2(1-q)^3(1,1,1,1)$. Conversely these vectors attain $T|c|$ by Theorem 4.2 (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 (Section 4.7). 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 $n=4$, with $g_4(q) = 4q^2 - 8q + 1$ and rationals $q_4^- < q_4 < q_4^+$, $g_4(q_4^-) > 0 > g_4(q_4^+)$, $q_U < q_4^-$, $q_4^+ < q_L$: 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 $H_f(q_4^-) > 0$. As a check of (4.8): $H_{\mathrm{OR}_{\{1,2,3,4\}}} = 12(1-q)^4 - 16(1-q)^6 = -4(1-q)^4 g_4(q)$. □

Lemma 8.3(b) 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 enters the proof. In this regime the two-coordinate route uses vertex certificates (Section 4.9) with patches p_2 and p_3, and the m-split below.

8.1. **Pieces of type TC, SG and TCS.** The following definitions are used in this section and in Section 9, with the target T of the regime. Let B be a box with $b^- > 0$, sign s, and $[m_1, m_2] \subset (0, 1]$.

Definition 8.4 (pieces of type TC and SG)**.**

- A TC piece with sign $s_3 \in \{1, -1\}$ is a rational cap $\kappa \in (0, 1]$ with $\kappa \geq \kappa(m_2) = \min(1, m_2/\sqrt{1 - m_2^2})$ (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 8.5 (TC and SG piece lemma)**.** [computer-assisted, see Sec. 16] *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 4.25 ($j = 1$) gives $\mathbb{E}|L| = \mathbb{E}F_{p_3(t,r,m)}(M')$, $M' = M^{(1)}$, with $\mu(M') \leq \kappa(m) \leq \kappa(m_2) \leq \kappa$, so $M' \in \mathcal{Z}$ and Lemma 4.32 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 4.25(ii)); 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 4.32. (ii) By Lemma 4.8 with $m_c = m_1$, $p_3(M) \leq \varphi(m_1) \leq p^*$. Also $m \leq m_2$ and $m \leq \bar{m}(B)$, so $m \leq \kappa$. Thus $M \in \mathcal{Z}$, and Lemmas 4.25 ($j = 0$) and 4.32 give $\mathbb{E}|L| < T$. □

Definition 8.6 (pieces of type TCS)**.** A TCS piece on $[m_1, m_2]$ is: a rational cap $\kappa \in (0, 1]$ with $\kappa \geq \kappa(m_2)$; 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 ($A_4$) or ($B_4$) on $B \times [m_1, m_2] \times [n_1, n_2]$, whose union contains $[m_c', \kappa]$.

Lemma 8.7 (TCS piece lemma)**.** [computer-assisted, see Sec. 16] *Let $[m_1, m_2]$ carry a TCS piece for B, and suppose that $G_4(c) \leq T|c|$ for all $c \in \mathbb{R}^4$ at the values of q considered. At every point of B with $r < 1$ 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 $m < 1$, $\mu(M') = 1$, $\alpha = a_1 e_1 + s a_2 e_2 + a_3 e_{i_0} + a_4 e_{i_1}$ for some $i_1 \notin \{1, 2, i_0\}$, and $G_4(a_1, s a_2, a_3, a_4) = T$, where all four entries are nonzero.*

Proof. If $m = 1$: $\mathbb{E}|L| = F_{p_3(t,r,1)}(y)$ for every y (Lemma 4.25(ii)); 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 4.32 gives $\mathbb{E}|L| = \mathbb{E}F_{p_3(t,r,1)}(Z) < T$.

Now let $m < 1$ and $M' = M^{(1)}$. By Lemma 4.25, $\mathbb{E}|L| = \mathbb{E}F_{p_3(t,r,m)}(M')$ and $m' := \mu(M') \leq \kappa(m) \leq \kappa$.

- If $m' \leq m_c'$: M' is in the class of $\mathcal{C}'$, and Lemma 4.32 gives $\mathbb{E}|L| < T$.
- If $m' \geq m_c'$ and M' has the coefficient $-m'$ at some χ_{i_1}: by Lemma 4.8, $p_3(M') \leq \varphi(m_c') \leq p'^*$, and $m' \leq \kappa$, so M' is in the class of $\mathcal{C}''$, and $\mathbb{E}|L| < T$.
- Otherwise 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 the point is positively peeled through $[m_1, m_2], [n_1, n_2]$. If the sub-piece passes (B_4), Lemma 4.37 gives $\mathbb{E}|L| < T$. If it passes (A_4), Lemma 4.37 (with the main-term bound $G_4 \leq T|\cdot|$) gives $\mathbb{E}|L| < T$ when $b_2 > 0$, and $\mathbb{E}|L| = G_4(c) \leq T$ with $c = (a_1, s a_2, a_3, a_4)$, $|c| = 1$, when $b_2 = 0$.

In the last case with $b_2 = 0$ we have $m' = 1$ and $a_4 = b_1 > 0$ (as $m < 1$); all entries of c are nonzero ($a_1 > 0$, $a_2 \geq |\alpha_{i_0}| = a_3 = bm > 0$, $a_4 > 0$), and $L = a_1\chi_1 + sa_2\chi_2 + a_3\chi_{i_0} + a_4\chi_{i_1}$. □

Definition 8.8 (m-split box of kind ms5, level one)**.** An m-split box of 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 (A_3), (B_3), 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 8.9 (m-split lemma, $k = 3$ lower part)**.** [computer-assisted, see Sec. 16] *Let B be an m-split box of kind ms5. 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 4.25 and 4.32, $\mathbb{E}|L| < T$. Let $m \geq m_c$. If $\beta_{i_0} = +m$ for some i_0, then m lies in a plus piece. A piece (B_3) or TC gives $\mathbb{E}|L| < T$ (Lemmas 4.37 and 8.5(i)). A piece (A_3) gives $\mathbb{E}|L| < T$ if $b_1 > 0$, and $\mathbb{E}|L| = G_3(a_1, sa_2, b) \leq T$ if $b_1 = 0$ (i.e. $m = 1$), by Lemma 4.37 with the main-term bound of Lemma 8.3(a) ($q \in [q_4, q_L] \subset [q_U, q_L]$); in the latter case equality forces (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 $\mathbb{E}|L| \leq T$ by Lemma 8.7 (with Lemma 8.3(b)); in case of equality, $G_4(a_1, sa_2, a_3, a_4) = T$ with all entries nonzero, so by Lemma 8.3(b) $q = q_4$ and the vector is a positive multiple of $\pm(1, 1, 1, 1)$; since $a_1, a_3, a_4 > 0$, $s = 1$ and $a_1 = a_2 = a_3 = a_4 = \frac{1}{2}$. Otherwise the maximum m is attained only by negative coefficients, $\beta_{i_0} = -m$, and m lies in a minus piece; Lemma 8.5 gives $\mathbb{E}|L| < T$. □

8.2. **Certified data and proof.**

Proposition 8.10 (certified data for Theorem 8.1)**.** [computer-assisted, see Sec. 16]

(i) The rectangle $[U_-, U_+] \times [0, \frac{7}{20}]$ is tiled by 288 cells (98, 126 and 64 cells for $u \in [\frac{12}{5}, \frac{247}{100}]$, $[\frac{247}{100}, \frac{127}{50}]$, $[\frac{127}{50}, U_+]$; widths $6.2 \cdot 10^{-4}$ to 0.0175 in u and 0.022 to 0.044 in a), each with a cell certificate of degree 10 ($k = 3$, ten-moment objective bound) and $\Theta_1 > 0$.

(ii) For each sign s, the box $[U_-, U_+] \times [0, T_8] \times [\frac{7}{20}, 1]$ is tiled by boxes of kind lpv (Section 4.9), ncA (test (A) or (B) of Lemma 4.35) or ms5 (Definition 8.8); the counts are in Table 6. (There are no small boxes.)

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

TABLE 6. Two-coordinate boxes for Theorem 8.1. 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 (A_3), 689 TC, 210 TCS (all with $m_c' = \frac{17}{20}$, with 301 sub-pieces, all of type (A_4)); 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.

How it is verified. Coverage (exact): $\sqrt{5} < U_- \leq \frac{12}{5}$; $U_+ \geq u_4$; $T_8 \geq \sqrt{2} - 1$; the cells and, for each sign, the boxes tile their regions (they lie in the region, have pairwise disjoint interiors and total volume equal to that of the region). Cells: (V1)–(V3) by Sturm sequences; $\Theta_1 > 0$ (indeed $S_3(\frac{u_1^2}{1+u_1^2})^2 \geq S_3(\frac{144}{169})^2 > 1.25 > \frac{7}{20} \geq \bar{a}$); (V4) strictly (the polynomials μ_n from the recursion, the

monomial bounds of Definition 4.11, and a Sturm count of the roots of h on $[0,\bar{m}]$ together with $h(0)>0$). Vertex certificates (all lpv records and all certificates inside ms5 records): (P1) and (P2) exactly; (P3) by exact Gaussian elimination (rank 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), succeeding when every sub-box has a nonnegative lower bound for each facet value, and failing if some 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, 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. Near-circle boxes: interval arithmetic (120 bits), strict. 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 (A_3)/(B_3) piece passes its test (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 (A_4) or (B_4) (strict). □

Proof of Theorem 8.1. *(a)* By Lemma 4.1 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 4.7.

(1) $a_1=1$: $\alpha=e_1$ and $\mathbb{E}|L|=2\tau<T$.
(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 7.2 ($q<q_3$) 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, since $t\in[0,\sqrt{2}-1]\subseteq[0,T_8]$ and $r\ge a_1>\frac{7}{20}$. If it is lpv, Lemma 4.33 gives $\mathbb{E}|L|<T$. If it is ncA, Lemma 4.35 gives $\mathbb{E}|L|<T$ ($q<q_3$, Lemma 7.2). If it is ms5, Lemma 8.9 gives $\mathbb{E}|L|\le T$.

So $\mathbb{E}|L|\le T$ always, and $(e_1+e_2+e_3)/\sqrt{3}$ attains T (Theorem 4.2, $q<\frac{1}{3}$). Hence $R(q)=T(q)$. For $q\in[1-q_L,1-q_4]$ use Lemma 4.1.

(b) Equality can occur only in the ms5 case of (4). By Lemma 8.9, 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 gives the list in (b). Conversely, $(e_i+e_j+e_k)/\sqrt{3}$ gives T for $q<\frac{1}{3}$, and $(e_i+e_j+e_k+e_l)/2$ gives $T_4=T$ at q_4 (Theorem 4.2). For $q\ge\frac{1}{2}$ use Lemma 4.1.

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

9. The regime $k=4$: $R(q)=4(1-q)^3\sqrt{q(1-q)}$ exactly for $q_5\le q\le q_4$

Theorem 9.1 (the regime $k=4$)**.** [computer-assisted, see Sec. 16] *Let $T=T_4=4(1-q)^3\tau$.*

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

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

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.) $R(q) > T(q)$ *for* $q \in (0, q_5) \cup (q_4, \frac{1}{2}]$. *More precisely,* $R(q) \geq T_5(q) > T(q)$ *for* $q < q_5$, $R(q) \geq T_3(q) > T(q)$ *for* $q_4 < q < \frac{1}{3}$, *and* $R(q) \geq 2\tau > T(q)$ *for* $\frac{1}{3} \leq q \leq \frac{1}{2}$. *Hence* $\{q \in (0, \frac{1}{2}] : \ R(q) = T(q)\} = [q_5, q_4]$.

Parameters. The range $q \in [q_5, q_4]$ corresponds to $u \in [u_4, u_5]$. We fix

$$U_- = \frac{1589}{625} = 2.5424 \ \leq u_4, \qquad U_+ = \frac{29107}{10000} = 2.9107 \ \geq u_5,$$

since $U_-^2 > 3$ and $(U_-^2 - 3)^2 \leq 12$, and $U_+^2 > 4$ and $(U_+^2 - 4)^2 \geq 20$; and $A_S = \frac{33}{100}$. The computations cover $u \in [U_-, U_+]$; the theorem uses only $u \in [u_4, u_5]$. Here $S_4 = 2$, so $T^-(u_1, u_2) = \min\{T(u_1), T(u_2)\}$ is rational. Also $U_- \geq 2$, and $\hat{q}_- = U_-^2/(1 + U_-^2)$ (the value of $1 - q$ at $u = U_-$) satisfies

$$\hat{q}_-^4 \geq \tfrac{1}{2}, \qquad 2\hat{q}_-^3 \geq 1 \tag{9.1}$$

(exact check; $\hat{q}_- \approx 0.866020$). Since $\hat{q}_-$ 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 $u \geq U_-$. By (4.4) and (9.1): (i) $T_3 \leq T$ iff $q \leq q_4$, with equality iff $q = q_4$; (ii) $T_5 \leq T$ iff $q \geq q_5$, with equality iff $q = q_5$; (iii) for $u \geq U_-$: $2\tau < T$ (as $2(1-q)^3 > 1$) and $T_2 < T$ (as $(1-q)^4 > \frac{1}{2}$). Hence, by Lemma 4.16, $\mathbb{E}|c\chi_1 + sd\chi_2| \leq \max(2\tau, T_2)\sqrt{c^2 + d^2} < T\sqrt{c^2 + d^2}$ for $u \geq U_-$ and $(c, d) \neq 0$. By Lemma 4.18 and (ii): if $q \geq q_5$, $c \in \mathbb{R}^5$ has $c_i > 0$ and $c_i > q \sum_l c_l$ for all i, then $G_5(c) \leq T_5|c| \leq T|c|$, and $G_5(c) = T|c|$ iff $q = q_5$ and $c_1 = \cdots = c_5$.

Lemma 9.2 (three- and four-bit lemmas, $k = 4$)**.** [computer-assisted, see Sec. 16] *Let* $q \in [q_5, q_4]$ *and* $c \neq 0$.

(a) If $c \in \mathbb{R}^3$, *then* $G_3(c) \leq T|c|$, *with equality iff* $q = q_4$ *and* c *is a positive multiple of* $\pm(e_1 + e_2 + e_3)$.

(b) If $c \in \mathbb{R}^4$, *then* $G_4(c) \leq T|c|$, *with equality iff* 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. For $f : \{0,1\}^n \to \{-1, 1\}$ put $H_f(q) = 16(1-q)^6 - \sum_{i=1}^n \Delta_i(f)^2$. *Claims*:

(C1) ($n = 3$, all 2^8 functions) $H_f \geq 0$ 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) $H_f \geq 0$ 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, Lemma 4.17 with $B^2 = 16(1-q)^6$ gives $G_n(c) \leq 4(1-q)^3\tau|c| = T|c|$ on $[q_5, q_4]$. If equality holds, then $H_{f^*}(q) = 0$ and c is a positive multiple of $\Delta(f^*)$; by the claims and (4.8): 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 $T|c|$ by Theorem 4.2: $(1,1,1,1)$ gives T_4 for $q < \frac{1}{4}$, and at q_4, $e_i + e_j + e_k$ gives $T_3 = T_4$.

How the claims are checked. The distinct polynomials H_f are tested (39 for $n = 3$, 1 630 for $n = 4$). With $g_4(q) = 4q^2 - 8q + 1$ and $g_5(q) = 5q^2 - 10q + 1$, 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 $g_4(q_4^+) < 0$. 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 $H_f = g_4 Q \geq 0$ 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 $[q_5, q_4]$. As a check of (4.8): 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 $n = 4$, $H_{\mathrm{OR}_{\{1,2,3,4\}}} = 16(1-q)^6 - 4 \cdot 4(1-q)^6 = 0$. □

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 $G_5 \le T|c|$ in the OR region 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 enter the proof; the box computations cover $u \in [U_-, U_+]$, and their conclusions are used only for $u \in [u_4, u_5]$.

9.1. **The m-split for $k = 4$.** In the coordinates of Section 4.7 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 use the pieces of Section 8.1 (with $T = T_4$) and, inside some pieces, peel off the largest coefficient again, up to five split coordinates. We write $M' = M^{(1)}$, $m' = \mu(M')$, $M'' = M^{(2)}$, $m'' = \mu(M'')$ (Lemma 4.25), and $a_3 = bm$, $b' = b\sqrt{1-m^2}$, $a_4 = b'm'$, $b'' = b'\sqrt{1-m'^2}$, $a_5 = b''m''$, $b''' = b''\sqrt{1-m''^2}$ (so $b' = b_1$, $b'' = b_2$, $b''' = b_3$).

Definition 9.3 (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 $\kappa_4 \ge \kappa(n_2)$ 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 $\kappa_4 \ge \kappa(n_2)$; a rational m''_c and a rational p''^* with $2m''^2_c > 1$, $\varphi(m''_c) \le p''^* < 0$ 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 $(\mathrm{A}_5^{\mathrm{OR}})$ or (B_5) 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 $\varphi(n_1) \le p'^* < 0$, a rational cap $\kappa_3 \in (0, 1]$ with $\kappa_3 \ge n_2$ or $\kappa_3 \ge \kappa(m_2)$, and a vertex certificate for $(X_3, (1, s, 1), [u_1, u_2], \kappa_3, p'^*)$.

Definition 9.4 (pieces of type TCN)**.** A TCN piece on $[m_1, m_2]$ is: a rational cap $\kappa \in (0, 1]$ with $\kappa \ge \kappa(m_2)$; 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 (A_4) or (B_4) 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 9.5 (TCN piece lemma)**.** [computer-assisted, see Sec. 16] *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 $\mathbb{E}|L| \le T$. 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 8.7, $\mathbb{E}|L| = F_{p_3(t,r,1)}(y)$ 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 $\mathbb{E}|L| < T$.

Let $m < 1$. By Lemma 4.25 ($j = 1$), $\mathbb{E}|L| = \mathbb{E}F_{p_3(t,r,m)}(M')$ and $m' = \mu(M') \le \kappa(m) \le \kappa$.

(1) $m' \le m'_c$: M' is in the class of $\mathcal{C}'$, and $\mathbb{E}|L| < T$ (Lemma 4.32).
(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 4.8 (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 $m' \le \kappa(m_2)$. So M' is in the class of the SG3 certificate (patch p_3, $\sigma = (1, s, 1)$), and $\mathbb{E}|L| < T$.

- TC4 with $s_4 = -1$: if $m' < 1$, Lemma 4.25 ($j = 2$, $\varsigma_2 = -1$) gives $\mathbb{E}|L| = \mathbb{E}F_{p_4(t,r,m,m')}(M'')$ with $\mu(M'') \le \kappa(n_2) \le \kappa_4$, so $\mathbb{E}|L| < T$ by Lemma 4.32. 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 4.25(ii)), and $Z = \chi'$ gives $\mathbb{E}|L| < T$.

(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 the point is positively peeled through $[m_1, m_2], [n_1, n_2]$.

- (A_4) or (B_4): Lemma 4.37 (with the main-term bound of Lemma 9.2(b)) gives $\mathbb{E}|L| < T$, except in case (A_4) with $b'' = 0$, where $\mathbb{E}|L| = G_4(a_1, sa_2, a_3, a_4) \le T$; as in Lemma 8.7 all four entries are nonzero, so by Lemma 9.2(b) equality forces $s = 1$ and $a_1 = \cdots = a_4 = \frac{1}{2}$, i.e. $\alpha = \frac{1}{2}(e_1 + e_2 + e_{i_0} + e_{i_1})$.
- TC4 with $s_4 = 1$: as for $s_4 = -1$ above (now $\varsigma_2 = +1$), $\mathbb{E}|L| < T$.
- 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 $\mathbb{E}|L| < T$. If $m' < 1$, then $\mathbb{E}|L| = \mathbb{E}F_{p_4(t,r,m,m')}(M'')$ with $m'' = \mu(M'') \le \kappa(n_2) \le \kappa_4$, 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 4.8) and M'' is in the class of $\mathcal{D}''$; in both cases $\mathbb{E}|L| < T$. 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 the point is positively peeled through $[m_1, m_2], [n_1, n_2], [o_1, o_2]$. By Lemma 4.37 (via ($A_5^{\mathrm{OR}}$), whose main-term bound is $G_5 \le T_5|\cdot| \le T|\cdot|$ for $q \ge q_5$, or via (B_5)), $\mathbb{E}|L| < T$, except in case (A_5^{OR}) with $b''' = 0$, where $\mathbb{E}|L| = G_5(a_1, \dots, a_5) \le T$ with equality only if $q = q_5$ and $a_1 = \cdots = a_5 = \frac{1}{\sqrt{5}}$ (and $s = 1$, which (A_5^{OR}) 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. □

Definition 9.6 (m-split box, $k = 4$)**.** An m-split box of kind ms5 for $k = 4$ is as in Definition 8.8, except that the plus pieces may also be of type TCN.

Lemma 9.7 (m-split lemma, $k = 4$)**.** [computer-assisted, see Sec. 16] *Let B be an m-split box (Definition 9.6). At every point of B with $r < 1$ and $q \in [q_5, q_4]$ we have $\mathbb{E}|L| \le T$. 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 4.25 ($j = 0$) and 4.32, $\mathbb{E}|L| < T$. Let $m \ge m_c$. If $\beta_{i_0} = +m$ for some i_0, then m lies in a plus piece. A piece (B_3) or TC gives $\mathbb{E}|L| < T$ (Lemmas 4.37 and 8.5(i)). A piece (A_3) gives $\mathbb{E}|L| < T$ if $b' > 0$, and $\mathbb{E}|L| = G_3(a_1, sa_2, b) \le T$ if $b' = 0$ (i.e. $m = 1$); in the latter case equality forces, by Lemma 9.2(a), $q = q_4$ 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 $\mathbb{E}|L| \le T$ by Lemma 8.7 (with Lemma 9.2(b)), and equality forces $G_4(a_1, sa_2, a_3, a_4) = T$ with all entries nonzero, hence (Lemma 9.2(b)) $s = 1$ and $\alpha = \frac{1}{2}(e_1 + e_2 + e_{i_0} + e_{i_1})$. A piece TCN gives $\mathbb{E}|L| \le T$ with equality only as in Lemma 9.5. Otherwise the maximum m is attained only by negative coefficients, $\beta_{i_0} = -m$, and m lies in a minus piece; Lemma 8.5 gives $\mathbb{E}|L| < T$. □

9.2. **Certified data and proof.**

Proposition 9.8 (certified data for Theorem 9.1)**.** [computer-assisted, see Sec. 16]

(i) The rectangle $[U_-, U_+] \times [0, \frac{33}{100}]$ is tiled by 1 268 cells (256, 257, 300 and 455 for $u \in [U_-, \frac{66}{25}]$, $[\frac{66}{25}, \frac{273}{100}]$, $[\frac{273}{100}, \frac{141}{50}]$, $[\frac{141}{50}, U_+]$), each with a cell certificate of degree ten ($k = 4$, ten-moment objective bound) and $\Theta_1 > 0$.

(ii) For each sign s, the box $[U_-, U_+] \times [0, T_8] \times [\frac{33}{100}, 1]$ is tiled by boxes of the kinds small, lpv, ncA, ncB and ms5 (Definition 9.6); only lpv and ms5 occur, and the counts are in Table 7.

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 7. Two-coordinate boxes for Theorem 9.1. 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 (A_3), 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 (A_4). 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 (A_4), 2 479 TC4 and 216 TC4S (all with $m_c''=\frac{17}{20}$; 383 sub-pieces, all of type (A_5^{OR})), 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.

How it is verified. As for Proposition 8.10, with the following changes. Coverage: $2\le U_-\le u_4$ (checked as $U_-^2\le3$ or $(U_-^2-3)^2\le12$), $U_+\ge u_5$ (checked as $U_+^2\ge4$ and $(U_+^2-4)^2\ge20$), (9.1); every box has the sign of its file and one of the kinds small, lpv, ncA, ncB, ms5. 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): (P4) is checked by the recursion of Lemma 4.28 as described after it, with exact sign decisions and integer square-root bounds. The sign vector, caps and p^* values are taken from the structure: $\bar m(B)$ for lpv, m_c for $\mathcal{C}^{(1)}$, m_c' for $\mathcal{C}'$, m_c'' for $\mathcal{D}'$, and the recorded cap and p^* for the others. m-split structure, in addition to the checks of Proposition 8.10: the cap conditions of TCS and TCN (with m_2) and of TC4 and TC4S (with n_2); the φ conditions of SG, TCS, SG3 and TC4S; the cap conditions of SG and SG3; $0<m_c'<\kappa\le1$ for TCN and $m_c''<\kappa_4$ for TC4S; all nested covers; and each (A_4)/(B_4) and (A_5^{OR})/(B_5) piece passes its test (interval arithmetic, strict). Cells: $\Theta_1>0$, indeed $2(\frac{u_1^2}{1+u_1^2})^3\ge2\hat q_-^3\ge1>\frac{33}{100}\ge\overline{a}$ by (9.1). □

Proof of Theorem 9.1. *(a)* By Lemma 4.1 let $q\in[q_5,q_4]$, i.e. $u\in[u_4,u_5]\subseteq[U_-,U_+]$. Reduce α as in Section 4.7.

(1) $a_1=1$: $\alpha=e_1$ and $\mathbb{E}|L|=2\tau<T$ by (iii).
(2) $a_1\le\frac{33}{100}$: (u,a_1) lies in a cell, and Lemma 4.15 gives $\mathbb{E}|L|<T$.
(3) $a_1>\frac{33}{100}$ and $r=1$: $L=a_1\chi_1+sa_2\chi_2$, and $\mathbb{E}|L|<T$ by the two-coordinate bound above.
(4) $a_1>\frac{33}{100}$ and $r<1$: (u,t,r) lies in a box of the cover for the sign s, and it is not a small box, since $a_1>A_S$. If it is lpv, Lemma 4.33 gives $\mathbb{E}|L|<T$. If it is ncA or ncB, Lemma 4.35 gives $\mathbb{E}|L|<T$. If it is ms5, Lemma 9.7 gives $\mathbb{E}|L|\le T$.

So $\mathbb{E}|L|\le T$ always, and $(e_1+e_2+e_3+e_4)/2$ attains T (Theorem 4.2, $q<\frac14$). Hence $R(q)=T(q)$. For $q\in[1-q_4,1-q_5]$ use Lemma 4.1: $R(q)=R(1-q)=4q^3\tau$.

(b) Equality can occur only in the ms5 case of (4). By Lemma 9.7, after the reduction, $\alpha=\frac12(e_1+e_2+e_{i_0}+e_{i_1})$, or $q=q_4$ and $\alpha=\frac{1}{\sqrt3}(e_1+e_2+e_{i_0})$, or $q=q_5$ and $\alpha=\frac{1}{\sqrt5}(e_1+e_2+e_{i_0}+e_{i_1}+e_{i_2})$. Undoing the reduction gives the list in (b). Conversely, each listed vector attains T at the stated q (Theorem 4.2): $T_3=T_4$ at q_4 and $T_5=T_4$ at q_5. For $q\ge\frac12$ use Lemma 4.1.

(c) For $q<q_5<\frac15$, $R(q)\ge T_5(q)>T(q)$ by (ii). For $q_4<q<\frac13$, $R(q)\ge T_3(q)>T(q)$ by (i). For $\frac13\le q\le\frac12$, $R(q)\ge\mathbb{E}|\chi_1|=2\tau$, and $2\tau>4(1-q)^3\tau$ because $(1-q)^3\le(\frac23)^3<\frac12$. □

10. The regime $k=5$: $R(q)=2\sqrt{5}\,(1-q)^4\sqrt{q(1-q)}$ exactly for $q_6\le q\le q_5$

Theorem 10.1 (the regime $k=5$)**.** [computer-assisted, see Sec. 16] *Let $T=T_5=2\sqrt{5}\,(1-q)^4\tau$.*

(a) For every $q\in[q_6,q_5]$, every $n\ge 1$ and every $\alpha\in\mathbb{R}^n$ with $|\alpha|=1$,

$$\mathbb{E}\Big|\sum_{i=1}^n \alpha_i\chi_i\Big| \le 2\sqrt{5}\,(1-q)^4\sqrt{q(1-q)}.$$

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 $\alpha=\pm\frac12(e_i+e_j+e_k+e_l)$ 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.) $R(q)>T(q)$ for $q\in(0,q_6)\cup(q_5,\frac12]$. More precisely, $R(q)\ge T_6(q)>T(q)$ for $q<q_6$, $R(q)\ge T_4(q)>T(q)$ for $q_5<q<\frac14$, and $R(q)\ge 2\tau>T(q)$ for $\frac14\le q\le\frac12$. Hence $\{q\in(0,\frac12]:\ R(q)=T(q)\}=[q_6,q_5]$.

Parameters. The range $q\in[q_6,q_5]$ corresponds to $u\in[u_5,u_6]$. We fix

$$U_-=\frac{29106}{10000}=2.9106\ \le u_5,\qquad U_+=\frac{3236855}{1000000}=3.236855\ \ge u_6,$$

since $U_-^2>4$ and $(U_-^2-4)^2\le 20$, and $U_+^2>5$ and $(U_+^2-5)^2\ge 30$; and $A_S=\frac14$. The computations cover $u\in[U_-,U_+]$; the theorem uses only $u\in[u_5,u_6]$. In (4.3), $S_5=\lfloor\sqrt{5}\rfloor_{15}$. The value $\hat q_-=U_-^2/(1+U_-^2)$ of $1-q$ at $u=U_-$ satisfies

$$5\hat q_-^8>1,\qquad 5\hat q_-^6>2 \tag{10.1}$$

(exact check; $\hat q_-\approx 0.894421$, $5\hat q_-^8\approx 2.05$, $5\hat q_-^6\approx 2.56$). Since $1-q$ increases with u, $5(1-q)^8>1$ and $5(1-q)^6>2$ for all $u\ge U_-$. By (4.4) and (10.1): (i) $T_4\le T$ iff $q\le q_5$, with equality iff $q=q_5$; (ii) $T_6\le T$ iff $q\ge q_6$, with equality iff $q=q_6$; and $T_{j+1}\le T_j$ for every $j\ge 6$ and $q\ge q_6$ (as $1-q\le\sqrt{5/6}\le\sqrt{j/(j+1)}$); (iii) for $u\ge U_-$: $2\tau<T$ and $T_2<T$. Hence $\mathbb{E}|c\chi_1+sd\chi_2|<T\sqrt{c^2+d^2}$ for $u\ge U_-$ and $(c,d)\ne 0$ (Lemma 4.16). In the OR region of Lemma 4.18: $G_5(c)\le T|c|$, with equality iff $c_1=\cdots=c_5$; and for $q\ge q_6$ and $n\ge 6$, $G_n(c)\le T_n|c|\le T|c|$, where $G_n(c)=T|c|$ holds iff $n=6$, $q=q_6$ and $c_1=\cdots=c_6$ (for $n\ge 7$, $T_n\le T_7<T_6\le T$, since $T_7<T_6$ iff $1-q<\sqrt{6/7}$).

The ranges $[G_j^-,G_j^+]$ of the ten-moment cumulant enclosures are computed in this regime as the hull of exact end values on subintervals of $[w^-,w^+]$ on which G_j' has no root (Sturm) and interval Horner enclosures on subintervals that still contain one after a fixed number of bisections (30 in the verifier, i.e. of length 2^{-30} times the range; 24 in the generator): G_9' vanishes at $w\approx 8.68$, i.e. $u\approx 2.926$, inside the range.

Lemma 10.2 (three- and four-bit lemmas, $k=5$)**.** [computer-assisted, see Sec. 16] *Let $q\in[q_6,q_5]$ and $c\ne 0$.*

(a) If $c\in\mathbb{R}^3$, then $G_3(c)<T|c|$.

(b) If $c\in\mathbb{R}^4$, then $G_4(c)\le T|c|$, with equality iff $q=q_5$ and c is a positive multiple of $\pm(e_1+e_2+e_3+e_4)$.

Proof. For $f:\{0,1\}^n\to\{-1,1\}$ put $H_f(q)=20(1-q)^8-\sum_{i=1}^n\Delta_i(f)^2$. *Claims*:

(C1) ($n=3$, all 2^8 functions) $H_f>0$ on $[q_6,q_5]$.

(C2) ($n=4$, all 2^{16} functions) $H_f\ge 0$ 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 Lemma 4.17 gives $G_n(c) \le T|c|$ on $[q_6, q_5]$. If equality holds with $c \neq 0$, then $H_{f^*}(q) = 0$ and c is a positive multiple of $\Delta(f^*)$. 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 (4.8). In particular equality never holds for $n = 3$. Conversely, at q_5 the vector $c = \pm(1,1,1,1)$ gives $G_4(c) = T_4|c| = T|c|$ by Theorem 4.2 ($q_5 < \frac{1}{4}$).

How the claims are checked. The distinct polynomials H_f are tested (39 for $n = 3$, 1 630 for $n = 4$). With $g_5(q) = 5q^2 - 10q + 1$ and $g_6(q) = 6q^2 - 12q + 1$, 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 $g_5(q_5^+) < 0$. 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 $[q_6, q_5]$. 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 (4.8): $H_{\mathrm{OR}_{\{1,2,3\}}} = 20(1-q)^8 - 12(1-q)^4 = 4(1-q)^4\big(5(1-q)^4 - 3\big) > 0$ (as $(1-q)^2 \ge \frac{4}{5}$ for $q \le q_5$), and $H_{\mathrm{OR}_{\{1,2,3,4\}}} = 20(1-q)^8 - 16(1-q)^6 = 4(1-q)^6 g_5(q)$. □

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 $G_6 \le T|c|$ in the OR region 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 $G_n \le T_n|c| \le T|c|$ for $n \ge 6$ in the OR region ($q \ge q_6$; Lemma 4.18 and (ii) above), both used in the near-sphere bounds of the m-split below; the box computations cover $u \in [U_-, U_+]$, and their conclusions are used only for $u \in [u_5, u_6]$.

10.1. **The m-split for $k = 5$: split nodes.** In the coordinates of Section 4.7 the extremisers are the following points (all with $s = 1$ and $t = \sqrt{2} - 1$; $\mu_1, \mu_2, \dots$ are the successive maxima of Lemma 4.25): $(e_1 + \cdots + e_5)/\sqrt{5}$, 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. 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*. The points above are reached at the leaves, where the remainder is used up ($b_j = 0$) and the near-sphere bound is exact. Throughout, (A_n^*) denotes the test (A_n) if $n \le 4$ and $(\mathrm{A}_n^{\mathrm{OR}})$ if $n \ge 5$ (Section 4.10).

Lemma 10.3 (main terms for $k = 5$)**.** [computer-assisted, see Sec. 16] *Let $q \in [q_6, q_5]$, $n \ge 3$, and $c = (a_1, sa_2, a_3, \dots, a_n)$ with all $a_i > 0$; if $n \ge 5$ suppose moreover $s = 1$ and $a_i > q\sum_{i'} a_{i'}$ for all i. Then $G_n(c) \le T|c|$, with equality only if $s = 1$, $a_1 = \cdots = a_n$, and either $n = 5$, or $n = 4$ and $q = q_5$, or $n = 6$ and $q = q_6$.*

Proof. For $n = 3$ this is Lemma 10.2(a), with strict inequality. For $n = 4$ it is Lemma 10.2(b): 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 $n \ge 5$, Lemma 4.18 and the comparisons above give $G_n(c) = 2\tau(1-q)^{n-1}\sum_i a_i \le T_n|c| \le T|c|$, with equality iff all a_i are equal and $T_n = T$, i.e. $n = 5$, or $n = 6$ and $q = q_6$. □

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 $\sigma_l = (1, s, 1, \dots, 1) \in \{1, -1\}^{2+l}$.

Definition 10.4 (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 $(X_l \times [n_1,n_2]$, $(\sigma_l,1)$, $[u_1,u_2]$, κ', $-)$;
- 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 $(X_l \times [n_1,n_2]$, $(\sigma_l,-1)$, $[u_1,u_2]$, κ', $-)$.

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 Section 9, $\mathsf{TC4}$, $\mathsf{TC4S}$ and $\mathsf{SG3}$ are the pieces $\mathsf{TC}^\pm$, TCS and SG of a node of level one.

Lemma 10.5 (split node lemma)**.** [computer-assisted, see Sec. 16] *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 $\mathbb{E}|L| \le T$. 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 4.25(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 4.32 gives $\mathbb{E}|L| < T$.

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 Lemmas 4.37 and 10.3 (with $j=l+1$, $n=l+3$; all $a_i>0$, and for $n\ge5$ the test $(\mathrm{A}^{\mathrm{OR}}_n)$ gives $s=1$ and the OR-region condition), $\mathbb{E}|L| < T$, except for (A^*_{l+3}) with $b_{l+1}=0$, where $\mathbb{E}|L| \le T$. 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 4.25(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 4.32 gives $\mathbb{E}|L| < T$. 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 4.25(ii)); with $Z = \chi'$ (in the class, cap 1), $\mathbb{E}|L| = \mathbb{E}F_{p_{3+l}(\xi,1)}(Z) < T$.
- 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 $\mathbb{E}|L| = \mathbb{E}F_{p_{3+l}(\xi,1)}(Z) < T$. 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 $\mathbb{E}|L| \le T$, with equality only as stated.

Case $\mu \geq m_c$, 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 4.8 (applied to $M^{(l)}$ with $n_1 \leq \mu$ in place of m_c), $p_3(M^{(l)}) \leq \varphi(n_1) \leq p^*$; and $\mu \leq \min(n_2, \hat{\kappa}) \leq \kappa'$. So $M^{(l)}$ is in the class of the certificate, and Lemma 4.32 gives $\mathbb{E}|L| < T$.
- TC$^-$: exactly as for TC$^+$, peeling the coefficient $-\mu$ ($\varsigma_{l+1} = -1$, sign vector $(\sigma_l, -1)$): $\mathbb{E}|L| < T$.

□

Definition 10.6 (m-split box, $k = 5$)**.** 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 10.7 (m-split lemma, $k = 5$)**.** [computer-assisted, see Sec. 16] *Let B be an m-split box. At every point of B with $r < 1$ and $q \in [q_6, q_5]$ we have $\mathbb{E}|L| \leq T$. Equality forces $s = 1$ and $\alpha = n^{-1/2}(e_1 + e_2 + e_{l_1} + \cdots + e_{l_{n-2}})$ for distinct $l_1, \ldots, l_{n-2} \geq 3$, 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 $\mu_1 = m \leq \min(1, a_2/b) \leq \min(1, \bar{m}(B))$. Apply Lemma 10.5 with $l = 0$. □

10.2. **Certified data and proof.**

Proposition 10.8 (certified data for Theorem 10.1)**.** [computer-assisted, see Sec. 16]

(i) The rectangle $[U_-, U_+] \times [0, \frac{1}{4}]$ is tiled by 861 cells (234, 232, 245 and 150 for $u \in [U_-, 3]$, $[3, \frac{31}{10}]$, $[\frac{31}{10}, \frac{16}{5}]$, $[\frac{16}{5}, U_+]$), each with a cell certificate of degree ten ($k = 5$, ten-moment objective bound) and $\Theta_1 > 0$.

(ii) For each sign s, the box $[U_-, U_+] \times [0, T_8] \times [\frac{1}{4}, 1]$ is tiled by boxes of the kinds small, lpv, ncA, ncB and ms (Definition 10.6); only lpv and ms occur, and the counts are in Table 8.

sign	lpv	ncA/ncB	ms	small	total
$s = +1$	3804	0	4303	0	8107
$s = -1$	1059	0	0	0	1059

TABLE 8. Two-coordinate boxes for Theorem 10.1. 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 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 (A_4), 5768 TC, 3958 TCN, 1400 TCS; level 2: minus 3958 TC; plus 1431 (A_5^{OR}), 6240 TC, 396 TCS. Every TCS piece has $m_c' = \frac{17}{20}$; the sub-pieces are 58 (A_4) at level 0, 1769 (A_5^{OR}) at level 1, 644 (A_6^{OR}) 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.

How it is verified. As for Proposition 9.8, with the following changes. Coverage: $U_- \leq u_5$ (checked as $U_-^2 \leq 4$ or $(U_-^2 - 4)^2 \leq 20$), $U_+ \geq u_6$ (checked as $U_+^2 \geq 5$ and $(U_+^2 - 5)^2 \geq 30$), (10.1). Vertex

certificates of every node of every split tree are checked as before, with the patch parameters, sign vector, cap and p^* value of each certificate taken from its position in the tree. Split trees: for every ms box $r_2 < 1$ and a recorded root cap $\geq \min(1, \bar{m}(B))$; recursively, for every node: $0 < m_c < \kappa \leq 1$ 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 $\kappa \geq \kappa(n_2)$ is checked); 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 its test (strict; $(\mathrm{A}^{\mathrm{OR}}_n)$ includes $s = 1$ and the OR-region condition); the cap condition $\kappa' \geq \kappa(n_2)$ 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^*) and $\kappa' \geq \min(n_2, \hat{\kappa})$. Cells: $\Theta_1 > 0$, indeed $\hat{q}^4_- \geq 5^{-1/2} > \frac{2}{5}$ and $S_5 \geq 2$, so $S_5(\frac{u_1^2}{1+u_1^2})^4 \geq S_5 \hat{q}^4_- > \frac{4}{5} > \frac{1}{4} \geq \overline{a}$. □

Proof of Theorem 10.1. *(a)* By Lemma 4.1 let $q \in [q_6, q_5]$, i.e. $u \in [u_5, u_6] \subseteq [U_-, U_+]$. Reduce α as in Section 4.7.

(1) $a_1 = 1$: $\alpha = e_1$ and $\mathbb{E}|L| = 2\tau < T$ by (iii).
(2) $a_1 \leq \frac{1}{4}$: (u, a_1) lies in a cell, and Lemma 4.15 gives $\mathbb{E}|L| < T$.
(3) $a_1 > \frac{1}{4}$ and $r = 1$: $L = a_1\chi_1 + sa_2\chi_2$, and $\mathbb{E}|L| < T$ by the two-coordinate bound above.
(4) $a_1 > \frac{1}{4}$ and $r < 1$: (u, t, r) lies in a box of the cover for the sign s, not small since $a_1 > A_S$. If it is lpv, Lemma 4.33 gives $\mathbb{E}|L| < T$. If it is ncA or ncB, Lemma 4.35 gives $\mathbb{E}|L| < T$. If it is ms, Lemma 10.7 gives $\mathbb{E}|L| \leq T$.

So $\mathbb{E}|L| \leq T$ always, and $(e_1 + \cdots + e_5)/\sqrt{5}$ attains T (Theorem 4.2, $q < \frac{1}{5}$). Hence $R(q) = T(q)$. For $q \in [1 - q_5, 1 - q_6]$ use Lemma 4.1: $R(q) = R(1 - q) = 2\sqrt{5}\, q^4\tau$.

(b) Equality can occur only in the ms case of (4). By Lemma 10.7, after the reduction, $\alpha = n^{-1/2}(e_1 + e_2 + e_{l_1} + \cdots + e_{l_{n-2}})$ with distinct $l_i \geq 3$, where $n = 5$, or $n = 4$ and $q = q_5$, or $n = 6$ and $q = q_6$. Undoing the reduction gives the list in (b). Conversely, each listed vector attains T at the stated q (Theorem 4.2): $(e_{i_1} + \cdots + e_{i_5})/\sqrt{5}$ 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 $q \geq \frac{1}{2}$ use Lemma 4.1.

(c) For $q < q_6 < \frac{1}{6}$, $R(q) \geq T_6(q) > T(q)$ by (ii). For $q_5 < q < \frac{1}{4}$, $R(q) \geq T_4(q) > T(q)$ by (i). For $\frac{1}{4} \leq q \leq \frac{1}{2}$, $R(q) \geq \mathbb{E}|\chi_1| = 2\tau$, and $2\tau > 2\sqrt{5}(1 - q)^4\tau$ because $5(1 - q)^8 \leq 5(\frac{3}{4})^8 < 1$. □

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

11.1. **Setting.** By $\chi \mapsto -\chi$, $R(q) = R(1 - q)$; in this section $q \in (0, \frac{1}{2}]$. Recall $\tau = \sqrt{q(1 - q)}$, $u = \sqrt{(1 - q)/q}$, $v = \sqrt{q/(1 - q)}$ (so $\chi \in \{u, -v\}$, $qu = (1 - q)v = \tau$), and $\chi = (X - q)/\tau$ with $X \sim \mathrm{Bernoulli}(q)$. Put

$$s = s(q) = \ln \tfrac{1}{1-q}, \qquad M(q) = \max_{k \geq 1} 2\sqrt{kq}\,(1 - q)^{k-1/2},$$

$$B(q) = \sqrt{\frac{2q}{e(1 - q)s}}, \qquad q^*_k = 1 - e^{-1/(2k)} \quad (k \geq 1).$$

Definition 11.1 (Kolmogorov measures and R_{ID})**.** 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

$$Z_K = \sigma G + \sum_{j=1}^m a_j\Big(N_j - \frac{w_j}{a_j^2}\Big), \qquad G \sim N(0, 1),\ N_j \sim \mathrm{Poisson}(w_j/a_j^2),$$

all independent; $\mathbb{E}Z_K = 0$ and $\mathbb{E}Z_K^2 = K(\mathbb{R}) = 1$. Let $R_{\mathrm{ID}} = \sup_K \mathbb{E}|Z_K|$.

For $K \geq 2$ let $q_K = 1 - \sqrt{(K-1)/K}$, let $g(x) = 2\sqrt{x}\, e^{-x}$ $(x \geq 0)$ and $C(q) = \max_{k \geq 1} g(ks)$. Since $(1-q)^k = e^{-ks}$,

$$M(q) = 2\sqrt{\tfrac{q}{1-q}} \max_{k \geq 1} \sqrt{k}\, e^{-ks} = \sqrt{\tfrac{q}{(1-q)s}}\, C(q). \tag{11.1}$$

11.2. **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 11.2 (level-one form)**.** *$R(q)^2 = 4q(1-q) \sup_{n,f} D(f)$.*

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 $f = \mathbf{1}\{L > 0\}$; 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 $L = \sum \alpha_i \chi_i$: $\tau D(f) = \mathbb{E}[fL] \leq \mathbb{E}L_+ = \mathbb{E}|L|/2 \leq R(q)\sqrt{D(f)}/2$. □

11.3. **Poissonisation.**

Theorem 11.3 (Poissonisation)**.** *For every $q \in (0, \frac{1}{2}]$, 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 $x_i = \mathbf{1}\{N_i \geq 1\}$; 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 h, $\mathbb{E}[(N-s)h(N)] = s\mathbb{E}[h(N+1) - h(N)]$; 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 11.2 gives $R(q)^2 \leq 4q(1-q)R_{\mathrm{ID}}^2/(4s(1-q)^2)$. □

The proof only tests F against sums of i.i.d. Poisson(s) variables; applied to one configuration at a time, it gives the following q-free condition, uniform in k.

Theorem 11.4 (configuration-wise Poissonisation)**.** *Let $q \in (0, \frac{1}{2}]$, $s = s(q)$, and g, $C(q)$ as in* (11.1)*. For $f : \{0,1\}^n \to [0,1]$ with $D(f) > 0$ let $\beta = \Delta(f)/\sqrt{D(f)}$ (a unit vector) and*

$$K_f = \sum_{i:\, \beta_i \neq 0} \beta_i^2 \, \delta_{\beta_i/\sqrt{s}},$$

a probability measure on $\mathbb{R} \setminus \{0\}$. For $\theta > 0$ and a measure K put $\lambda_+(K) = \lambda_\theta^+(K) = \int_{[\theta,\infty)} x^{-2} K(dx)$ and $\lambda_-(K) = \lambda_\theta^-(K) = \int_{(-\infty,-\theta]} x^{-2} K(dx)$ (the expected numbers of jumps of Z_K of size $\geq \theta$, resp. $\leq -\theta$).

(a) $2\tau\sqrt{D(f)} \leq \sqrt{q/((1-q)s)}\, \mathbb{E}|Z_{K_f}|$.

(b) $\lambda_\pm(K_f) = s\, k_\pm$ *with the integers* $k_\pm = \#\{i : \pm\beta_i \geq \theta\sqrt{s}\}$, *and for every integer* $k \geq 1$, $\sqrt{q/((1-q)s)}\, g(ks) = T_k(q) = 2\sqrt{kq}(1-q)^{k-1/2}$ *(and* $g(0) = 0$*).*

(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

$$\mathbb{E}|Z_{K_f}| \leq \max\big(g(\lambda_+(K_f)),\, g(\lambda_-(K_f)),\, C(q)\big) \tag{11.2}$$

($\lambda_\pm$ taken at $\theta(f)$), then $R(q) = M(q)$.

(d) 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

$$\mathbb{E}|Z_K| \le \max\big(g(\lambda_+(K)),\, g(\lambda_-(K)),\, C\big) \qquad (\lambda_\pm \text{ taken at } \theta(K)).$$

If $\mathrm{ID}^*(C)$ holds, then $R(q) = M(q)$ for every $q \in (0, \frac12]$ with $C(q) \ge C$. For $K \ge 2$, $\min_{0<q\le q_K} C(q) = C_K := \sqrt{2/e}/(1 + E_{K-1})$ (E_k as in Proposition 11.5), attained at q_K; so $\mathrm{ID}^*(C_K)$ gives $R = M$ on $(0, q_K]$. Numerically, $C_4 = 0.85334356\ldots$, $C_5 = 0.85510045\ldots$, $C_6 = 0.85598448\ldots$, i.e. $\sqrt{2/e} - C_K = 0.0044203$, 0.0026634, 0.0017794. A decimal C may replace C_K only if $C \le C_K$ (e.g. 0.8533435, 0.855100, 0.855984). In closed form $C_5 = g(2\ln\frac54) = 1.28\sqrt{2\ln 1.25}$.

Proof. (a) This is the proof of Theorem 11.3 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 (11.2), $2\tau\sqrt{D(f)} \le \max(T_{k_+}(q), T_{k_-}(q), M(q)) = M(q)$, with $T_0 := 0$ and $T_k \le M$ by the definition of M. By Lemma 11.2, $R(q) = 2\tau\sup_f\sqrt{D(f)} \le M(q)$, and $R \ge M$ by Theorem 4.2. 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 (11.2) 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 (11.1) and the definition of B; by Proposition 11.5, 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. At q_5, $1 - q_5 = 2/\sqrt{5}$, so $s(q_5) = \frac12\ln\frac54$, the tie $g(4s(q_5)) = g(5s(q_5))$ holds, and $C_5 = C(q_5) = g(4\cdot\frac12\ln\frac54) = g(2\ln\frac54)$. The decimal values are evaluations of these closed forms. □

11.4. **Size of the window.**

Proposition 11.5 (size of the window)**.** *$B(q)/M(q) = 1/\max_{k\ge1}\tilde g(ks)$ with $\tilde g(x) = \sqrt{2ex}\,e^{-x} = g(x)/\sqrt{2/e}$. On the band $q \in [1 - \sqrt{k/(k+1)},\, 1 - \sqrt{(k-1)/k}]$ where k is the maximiser of Theorem 4.2, $B/M - 1$ 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 $\sup_{0<q\le 1-1/\sqrt2}(B/M - 1) = E_1 = \sqrt{2/(e\ln 2)} - 1 = 0.030279$, attained at $q = 1 - 1/\sqrt2$; 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. By definition $B(q) = 2\sqrt{q/(1-q)}\max_{\kappa>0}\sqrt{\kappa}e^{-\kappa s}$, since $\max_{\kappa>0}\sqrt{\kappa}e^{-\kappa s} = (2es)^{-1/2}$ (proof of Theorem 4.2), and $M(q) = 2\sqrt{q/(1-q)}\max_{k\in\mathbb{N}}\sqrt{k}e^{-ks}$ by (11.1). So $B/M = (2es)^{-1/2}/\max_k\sqrt{k}e^{-ks} = 1/\max_k\tilde g(ks)$. By Theorem 4.2, k maximises $\sqrt{j}e^{-js}$ exactly for $s \in [s_k, s_{k-1}]$ with $s_k = \frac12\ln(1+1/k)$ ($s_0 = \infty$). On that band $B/M = 1/\tilde g(ks)$, and $\log\tilde g(ks) = \frac12\log(2eks) - ks$ 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 $\tilde{g}(x_k)$, $x_k = ks_k = \frac{k}{2}\ln(1+1/k)$, which gives E_k. Since $k\ln(1+1/k)$ increases to 1, x_k increases to $1/2$, and $\tilde{g}$ increases on $(0,1/2]$, so E_k decreases. The bands meeting $(0, 1-1/\sqrt{2}]$ are those with $k \geq 2$ (and the endpoint $s = s_1$), whose end values are E_j, $j \geq 1$. 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. □

Remark 11.6 (the Dirac family). For $N \sim \text{Poisson}(\lambda)$ and $m = \lfloor\lambda\rfloor$, $\mathbb{E}(\lambda - N)_+ = \lambda\mathbb{P}(N \leq m) - \lambda\mathbb{P}(N \leq m-1) = \lambda\mathbb{P}(N = m)$; for $\lambda < 1$ this is $\lambda e^{-\lambda}$. Hence for $a \geq 1$, $\mathbb{E}|Z_{\delta_a}| = a\,\mathbb{E}|N_{1/a^2} - a^{-2}| = 2a^{-1}e^{-1/a^2} = g(1/a^2) = g(\lambda_\theta^+(\delta_a))$ when $a \geq \theta$. So $\mathrm{ID}^*(C)$ is tight along the Dirac family and must be proved exactly near every δ_a with $g(1/a^2)$ close to C; away from the Dirac family it is the bound $\mathbb{E}|Z_K| \leq C$, with the margin $\sqrt{2/e} - C$. This is why the proof of $\mathrm{ID}^*(C_5)$ (Sections 13–15) treats a band around the Dirac laws separately from the far region.

12. Localisation of maximisers at finite q

In this section χ_i are i.i.d., $\chi_i = u$ with probability q and $-v$ with probability $1-q$, $u = \sqrt{(1-q)/q}$, $v = 1/u$, $\tau = \sqrt{q(1-q)} = qu = (1-q)v$, and $s = \ln(1/(1-q))$. 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 $0 < R \leq 1$. Here $L^+ = \max(L,0)$, $L^- = \max(-L,0)$ and P denotes probability.

Theorem 12.1 (localisation)**.** *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) Let $q \leq \frac{1}{2}$, 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 $\tilde{K} = \sum_i \alpha_i^{*2}\delta_{\alpha_i^*/\sqrt{s}}$ (that is, K_{f^*} of Theorem 11.4) 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 finitely supported probability measure K on $[-A,A]$ has some $\theta = \theta(K) > 0$ with $\mathbb{E}|Z_K| \leq \max(g(\lambda_\theta^+(K)), g(\lambda_\theta^-(K)), C)$, then $R(q) = M(q)$. *The proof uses the hypothesis only at $K = \tilde{K}$ for one n, and this $\tilde{K}$ is a finitely supported probability measure 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 $A'(0.05) = 1.46976$, $A'(q_6) = 1.51455$, $A'(0.1) = 1.53085$, $A'(q_5) = 1.53804$, $A'(q_4) = 1.57599$. In closed form $1 - q_5 = 2/\sqrt{5}$ and $s(q_5) = \frac{1}{2}\ln\frac{5}{4}$, so $A'(q_5) = \sqrt{5q_5/\ln\frac{5}{4}} = 1.538044391650755\ldots < \frac{77}{50}$. The bound is nearly attained: OR_k *at $q = q_{k+1}$ (where $\mathbf{1}_k/\sqrt{k}$ attains $M(q)$, tied with $\mathbf{1}_{k+1}/\sqrt{k+1}$; Theorem 4.2) 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 $\sqrt{2}$.*

Proof. (a) For $|t|$ small, $\varphi(t) := \mathbb{E}|L + t\chi_i| \leq R_n|\alpha + te_i| = R_n(1 + 2t\alpha_i + t^2)^{1/2} =: \gamma(t)$, by maximality and homogeneity, with equality at $t = 0$. Comparing difference quotients (division by $t < 0$ reverses the inequality) gives $\varphi'_+(0) \leq \gamma'(0) \leq \varphi'_-(0)$, while $\varphi'_-(0) \leq \varphi'_+(0)$ by convexity of φ. So $\varphi'_+(0) = \varphi'_-(0) = \gamma'(0) = R_n\alpha_i$. 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: $\{L = 0\} \supseteq \{\chi_i = u, L' = -\alpha_i u\} \cup \{\chi_i = -v, L' = \alpha_i v\}$, 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 $p_- \geq (1-q)P(-\alpha_i u < L' < \alpha_i v)$. 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 $p_+ \geq (1-q)P(-bv < L' < bu)$.

(c) Append an independent bit χ with coefficient β: $\mathbb{E}|L + \beta\chi| \leq R_{n+1}\sqrt{1+\beta^2} \leq R(1 + \beta^2/2)$. For $a, b > 0$ and real x, $|x + a| - |x| = a(1 - 2 \cdot \mathbf{1}\{x < 0\}) + 2(x + a)^+\mathbf{1}\{x < 0\}$ and $|x - b| - |x| = b(1 - 2 \cdot \mathbf{1}\{x > 0\}) + 2(b - x)^+\mathbf{1}\{x > 0\}$. 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 $H^-(b) \geq 0$: $2qH(a) \leq \delta + R\beta^2/2 = \delta + Rqa^2/(2(1 - q))$, 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 $\mathbb{E}[L^-] = \mathbb{E}[L^+] = R_n/2$. Since $(L + a)^+ \geq L + a$, $H(a) \geq ap_- - R_n/2$, so by (c) $ap_- - Ra^2/(4(1 - q)) \leq R_n/2 + \delta/(2q)$ for every $a > 0$; at $a = 2(1 - q)p_-/R$ this reads $(1 - q)p_-^2/R \leq (R_n + \delta/q)/2$. The bound for p_+ is the same with $H^-(a) \geq ap_+ - R_n/2$. Finally $R_n/2 = \mathbb{E}[L(\mathbf{1}\{L > 0\} - p_+)] \leq (\mathbb{E}L^2)^{1/2}(p_+(1-p_+))^{1/2}$ by Cauchy–Schwarz, with $\mathbb{E}L^2 = 1$.

(e) Combine (b) and (d): $u|\alpha_i| \leq 2\max(p_+, p_-)/R_n \leq \Lambda_n$. 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', the level-one identity $\mathbb{E}[f\chi_i] = \tau\Delta_i(f)$ and $\mathbb{E}[\alpha'\cdot\chi] = 0$ give $\mathbb{E}|\alpha'\cdot\chi| = 2\mathbb{E}[(\alpha'\cdot\chi)^+] \geq 2\mathbb{E}[f\,\alpha'\cdot\chi] = 2\tau\,\alpha'\cdot\Delta(f)$, with equality for $f = \mathbf{1}\{\alpha'\cdot\chi > 0\}$. Hence $R_n = \max_{\alpha'} \mathbb{E}|\alpha'\cdot\chi| \leq 2\tau \max_f |\Delta(f)| = 2\tau|\Delta(f^*)| = 2\tau\,\alpha^*\cdot\Delta(f^*) \leq \mathbb{E}|\alpha^*\cdot\chi| \leq R_n$. The atoms of $\tilde{K}$ are $\alpha_i^*/\sqrt{s}$ with $|\alpha_i^*| \leq \Lambda_n/u$ 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 $\operatorname{supp}\tilde{K} \subset [-A, A]$. By Theorem 11.4(a) at $f = f^*$ (for which $2\tau\sqrt{D(f^*)} = 2\tau|\Delta(f^*)| = R_n$) and the hypothesis at $K = \tilde{K}$ with $\theta = \theta(\tilde{K})$, $R_n \leq \mathbb{E}|Z_{\tilde{K}}|\sqrt{q/((1-q)s)} \leq \max(g(\lambda_+), g(\lambda_-), C)\sqrt{q/((1-q)s)} \leq M(q)$, since $\lambda_\pm(\tilde{K}) = s \cdot \#\{i : \pm\alpha_i^* \geq \theta\sqrt{s}\}$ and $g(ks)\sqrt{q/((1-q)s)} = T_k(q) \leq M(q)$ (Theorem 11.4(b)). This contradicts $R_n > M(q)$. Hence $R(q) \leq M(q)$, and $R(q) \geq M(q)$ by Theorem 4.2.

(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. □

13. The band around the Dirac laws

13.1. **Setting.** 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 $x \geq 1$ (Remark 11.6), and $\max g = g(1/2) = \sqrt{2/e}$. Sections 13.2–13.4 are written for a general threshold θ and support bound A.

13.2. **Exact identities.**

Lemma 13.1 (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 $\varsigma = \operatorname{sgn}(y)$, so $y + w = \varsigma(|y| + \varsigma w)$. If $|y| + \varsigma w \geq 0$ then $|y+w| = |y| + \varsigma w$ and $(-\varsigma w - |y|)_+ = 0$. If $|y| + \varsigma w < 0$ then $|y+w| = -|y| - \varsigma w = |y| + \varsigma w + 2(-\varsigma w - |y|)$. Take expectations; $\mathbb{E}[\operatorname{sgn}(Y)W] = \mathbb{E}\operatorname{sgn}(Y)\,\mathbb{E}W = 0$. □

Lemma 13.2 (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*

$$\ell(y) = y + 2\mathbb{E}(-W - y)_+ = -y + 2\mathbb{E}(W + y)_+, \qquad |y| \leq \ell(y) \leq \sqrt{y^2 + \rho^2}.$$

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 $\ell(y) \geq |y|$ and Cauchy–Schwarz $\ell(y) \leq (\mathbb{E}(y+W)^2)^{1/2}$. □

Lemma 13.3 (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 $N_S \sim \text{Poisson}(\Lambda)$ 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 13.1 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 $x = \sqrt{2V}$. □

13.3. **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 13.4 (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 13.5 (smoothed stop-loss test functions). 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 $\frac{1}{2}g(1/4) = \frac{1}{2}e^{-1/4}$.

Lemma 13.6 (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) $2\mathbb{E}(W-t)_+ \le 2\mathbb{E}\psi_{t,h}(W)$. Apply Lemma 13.4 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 $2\mathbb{E}(W-t)_+ = \mathbb{E}|W-t| - t \le (t^2+\rho^2)^{1/2} - t$; 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 13.4 again (moving the atom $a\delta_\theta$ to $a\delta_{\theta'}$, $\theta' > \theta$). □

13.4. **The jump law and the band bound.**

Lemma 13.7 (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 13.3 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 13.8 (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 $x \in [\theta, A]$: $A^{-2} \le x^{-2} \le \theta^{-2}$, $A^{-1} \le x^{-1} \le \theta^{-1}$, $\theta x^{-2} \le x^{-1} \le A x^{-2}$, and $(x^{-1} - A^{-1})(\theta^{-1} - x^{-1}) \ge 0$; (F4) is Cauchy–Schwarz. □

Proposition 13.9 (band bound)**.** *Let $0 < \theta \le A$ and let K be a finitely supported probability Kolmogorov measure on $[-A, A]$ with $K_S = K|_{[\theta,A]} \neq 0$; let V, Λ, m be as in Lemma 13.3, $K_R = K - K_S$ with $a, b, \rho^2 = 1 - V$ as in Lemma 13.6, $W = Z_{K_R}$, $\ell(y) = \mathbb{E}|y + W|$ 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*

$$\mathbb{E}|Z_K| \le e^{-\Lambda}(m + c_B) + \Lambda e^{-\Lambda}\, O + m\Lambda e^{-\Lambda} + P_2(\Lambda)\, c_C. \tag{13.1}$$

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 (13.1) *equals $2me^{-\Lambda} + e^{-\Lambda}c_B + \Lambda e^{-\Lambda}O' + P_2(\Lambda)c_C$.*

Proof. By Lemmas 13.2 and 13.3, $\mathbb{E}|Z_K| = \sum_{n\ge0} \mathbb{P}(N_S = n)\, \mathbb{E}\,\ell(S_n - m)$. For $n = 0$, $\ell(-m) = m + 2\mathbb{E}(W-m)_+$ (Lemma 13.2). For $n = 1$ the term is $\Lambda e^{-\Lambda}\mathbb{E}\ell(J-m)$. For $n \ge 2$, $y = S_n - m \ge 2\theta - m$ 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 13.2), 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. By Lemmas 13.2, 13.6 and 13.7: $c_B = \min(\chi_h^B(m), \sqrt{m^2+\rho^2} - m)$, $c_C = \min(\chi_h^C(2\theta - m), \sqrt{(2\theta-m)^2+\rho^2} - (2\theta - m))$, any $h > 0$. 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 13.2 and 13.6

$$\varphi(y) \le \chi_h^C(y), \quad \varphi(y) \le \sqrt{y^2+\rho^2} - y, \quad \varphi(y) = -2y + 2\mathbb{E}(W+y)_+ \le -2y + \chi_h^B(-y)$$

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 13.7(a)), with the endpoint values $\varphi(\theta - m)$, $\varphi(A - m)$ replaced by any of the upper bounds above;
(O2) Lemma 13.7(b) with $\Gamma(y) = -2y + \chi_h^B(-y)$, $\kappa = 1/h$ (Lemma 13.6(iii));
(O3) Lemma 13.7(c) with $j_0 = \theta - m$ and $\psi = \chi_h^C$, whose second derivative $\mathbb{P}(W_C > y - h)/h$ is nonincreasing (Lemma 13.6(iii)), ψ being convex and nonincreasing;
(O4) if $\theta \ge m$: Lemma 13.7(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: since $J \in [\theta, A]$, $\mathbb{E}[(J-\theta)(A-J)] \ge 0$, that is, $\mathbb{E}J^2 \le (A+\theta)\mu_1 - A\theta$).

13.5. **The band lemma at $\theta = \frac{17}{20}$, $A = \frac{77}{50}$.** By Theorems 11.4(d) and 12.1(f),(g), Theorem 1.1 for $q \le q_5$ follows from $\mathrm{ID}^*(C_5)$ for finitely supported probability measures K on $[-1.54, 1.54]$, where $C_5 = g(2\ln\frac{5}{4}) = 0.8551004\ldots$. We prove it with $\theta = 0.85$ on a band. Near the Dirac laws with $g(\Lambda) > C_5$ the bound of Proposition 13.9 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 13.7(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 13.10 (absorption)**.** *Let $K_S \neq 0$ 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 13.11 (band lemma, $\theta = 0.85$, $A = 1.54$)**.** [computer-assisted, see Sec. 16] *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 $K_S = K|_{[\theta,A]} \neq 0$, $V = K_S(\mathbb{R}) \ge 4/5$, $\Lambda = \lambda^+_\theta(K)$, 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 13.9 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 13.6 and O' any of (O1)–(O5). 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

$$\mathcal{D}^* = \{a, b \ge 0,\ a + b \le \tfrac{1}{5},\ (\Lambda, m) \text{ satisfy (F1)–(F5) with } V = 1 - a - b\}.$$

By Proposition 13.12, $\mathcal{D}^*$ is covered by boxes in (a, b, Λ, m) on each of which $F \le \max(g(\Lambda), C_5)$: 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 13.10 when (O5) is used) and one of the tests (T1)–(T3) below. □

13.6. **The certified band computation.** All inequalities are decided in ball arithmetic (`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. Grid points are rounded by exact comparisons with dyadic rationals.

Evaluation of χ. For $J > 0$, $\lambda \ge 0$, $s \ge 0$, $c \in \mathbb{R}$: $\mathbb{E}(J(N_\lambda - \lambda) - c + sG)_+^2 = \sum_{n\ge 0} p_n(\lambda)\,Q(J(n-\lambda) - c, s)$ with $p_n(\lambda) = e^{-\lambda}\lambda^n/n!$ and $Q(d, s) = \mathbb{E}(d + sG)_+^2 = (d^2 + s^2)\Phi(d/s) + ds\,\phi(d/s)$ ($Q(d, 0) = d_+^2$; Φ, ϕ the standard normal distribution function and density). The sum is taken over $n \le 14$; the tail is bounded by $\sum_{n>14} \frac{\lambda^n}{n!}((Jn + C)^2 + s^2) \le t_{15}/(1 - \varrho)$ with $C = J\lambda + |c|$, t_{15} its first term and $\varrho = 16\lambda/15^2 < 1$ (ratio of consecutive terms), using $Q(d, s) \le d^2 + s^2$ and $e^{-\lambda} \le 1$. The values χ_h^B, χ_h^C are enclosed in this way, with jump θ resp. A.

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 13.6(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 (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 $V \in [V_{\mathrm{lo}}, V_{\mathrm{hi}}]$; 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: $e^{-\Lambda} \le e^{-\Lambda_1}$, $\Lambda e^{-\Lambda} \le \max_{[\Lambda_1,\Lambda_2]} te^{-t}$, $P_2(\Lambda) \le P_2(\Lambda_2)$ ($P_2'(t) = te^{-t} \ge 0$); 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 $m \le m_2$, $V \le V_{\mathrm{hi}}$, computed exactly from the unimodality of g; $\mu_1 = m/\Lambda \in [\mu_{\mathrm{lo}}, \mu_{\mathrm{hi}}]$ with $\mu_{\mathrm{lo}} = \max(\theta, m_1/\Lambda_2)$, $\mu_{\mathrm{hi}} = \min(A, m_2/\Lambda_1)$; $d = \mu_1 - \theta \ge d_{\mathrm{lo}} = \mu_{\mathrm{lo}} - \theta$; $\sigma_J^2 \le s^2 = \min((\Lambda_2 V_{\mathrm{hi}} - m_1^2)/\Lambda_1^2,\ d_{\mathrm{hi}}(A - \theta - d_{\mathrm{lo}}))$ (exact formula and Bhatia–Davis); in the box version of Lemma 13.7(c), $j_0' = \theta - m_2$, $w' = d_{\mathrm{lo}}^2/(d_{\mathrm{lo}}^2 + s^2)$ and $u' = \min_{d\in[d_{\mathrm{lo}},d_{\mathrm{hi}}]}(d + s^2/d)$, the far point $j_0' + u'$ being rounded down to the m-grid. The functions $t \mapsto 2\mathbb{E}(W - t)_+$ 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). The chord of (O1) has nonnegative weights, so it is at most the chord through upper values $\bar\varphi_1 \ge \varphi(\theta - m)$, $\bar\varphi_2 \ge \varphi(A - m)$; replacing $\bar\varphi_1$ by $\max(\bar\varphi_1, \bar\varphi_2)$ (still an upper bound, as $\varphi(\theta - m) \ge \varphi(A - m)$) makes this chord nonincreasing in μ_1, so its value at μ_{lo} bounds it on the box.
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 μ_{lo}; (O3) in the box version with three float-chosen h; (O4) in the box version if $\theta - m_2 \ge 0$; (O2) with $\Gamma(\mu) \le -2(\mu_{\mathrm{lo}} - m_2) + \chi_h^B(t)$, $t \le -(\mu_{\mathrm{hi}} - m_1)$ 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 $[r_1, r_2]$: $V \le 1 - r_1$ is used for s^2, and all costs are replaced by linear bounds valid for $a, b \ge 0$, $a + b \le r$, with $r = \min(\lceil 4096 r_2 \rceil/4096, \frac{1}{50}) \ge r_2$. For $c = t - h > 0$ with $r/\theta \le 2(\theta - c)$, and with $\Psi(x) = \mathbb{E}(G - x)_+^2$,

$$\chi_h^B(t) \le a\,\frac{1}{2h\theta^2} \sum_{n\ge1} \frac{(r/\theta^2)^{n-1}}{n!}\big((\theta n - c)^2 + r\big) + b\,\frac{\Psi(c/\sqrt{r})}{2h},$$

because the term $n = 0$ of the lattice sum is $\mathbb{E}(\sqrt{b}G - a/\theta - c)_+^2 \le b\,\Psi(c/\sqrt{b}) \le b\,\Psi(c/\sqrt{r})$, and for $n \ge 1$, $\mathbb{P}(N_{a/\theta^2} = n) \le \frac{a}{\theta^2}\frac{(r/\theta^2)^{n-1}}{n!}$ 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 $0 \le a/\theta \le 2(\theta n - c)$); symmetrically, for $c = y - h > 0$ with $r/A \le 2(A - c)$, $\chi_h^C(y) \le a\,\frac{\Psi(c/\sqrt{r})}{2h} + b\,\frac{1}{2hA^2}\sum_{n\ge1}\frac{(r/A^2)^{n-1}}{n!}((An - c)^2 + r)$. 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 $\kappa \le d_{\mathrm{lo}}^2\sqrt{\Lambda_1/(1 - r_1)}$, $(1 - w)\rho^2/(2h) \le (1 - w')\rho^2/(2h)$, and $\chi_h^C(\mu_1 - m) \le \chi_h^C(\theta - m_2 + d_{\mathrm{lo}})$ (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

$$F \le \sqrt{1 - \rho^2}\, g(\Lambda) + \rho^2 M_x \le \big(1 - \tfrac{\rho^2}{2}\big) g(\Lambda) + \rho^2 M_x,$$

by (F4) for (O1), (O3), (O4), and by Lemma 13.10 (with $D = d_{\mathrm{lo}}$, as $\Lambda \ge \Lambda_1$, $V \le 1 - r_1$) for (O5). The piece is certified by one of: (T1) $M_x \le \frac{1}{2}\min(g(\Lambda_1), g(\Lambda_2))$; then $F \le g(\Lambda) \le \max(g(\Lambda), C_5)$;

(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 $F \le \hat g+\rho^2(M_x-\hat g/2) < T$; (T3) $M_0 + r_2 M_x < T$, where M_0 bounds $2me^{-\Lambda}$ (with $V \le 1-r_1$), 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 13.10 ($e^{-\Lambda}Q(m) \le e^{-\Lambda}Q(m_2)$ if $m_2 < \sqrt{\Lambda V}$, and $\le \sqrt{V}g(\Lambda) \le M$ 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 $0.44628\ldots < \Lambda < 0.55785\ldots$ 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.

Proposition 13.12 (certified band data)**.** [computer-assisted, see Sec. 16] *The procedure above certifies every square of the triangle* $\{a, b \ge 0,\ a+b \le \frac{1}{5}\}$*:*

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 1 339 certified squares cover the triangle. The 7 874 211 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.

14. The heavy part of the far region

Throughout this section $\theta = 17/20$ and $A = 77/50$. For a probability Kolmogorov measure K on $[-A, A]$ put $V_+ = K([\theta, A])$ and $V_- = K([-A, -\theta])$. By Theorem 13.11, the region left is the far region $\{V_+ < \frac{4}{5},\ V_- < \frac{4}{5}\}$; we split it into the *light* part $\{V_+ < \frac{1}{2},\ V_- < \frac{1}{2}\}$ (Section 15) and the *heavy* part, where $V_+ \ge \frac{1}{2}$ or $V_- \ge \frac{1}{2}$.

Theorem 14.1 (heavy far region)**.** [computer-assisted, see Sec. 16] *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 $\mathbb{E}|Z_K| < C_5$.*

The proof is a moment argument for everything except the positive edge $[\theta, A]$, which is handled exactly. Lemma 14.2 replaces the jumps in $[\theta, A]$ by jumps at θ 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 $[-A, \theta] \cup \{A\}$. It enters only through its cumulants, which are bounded by a degree-16 polynomial majorant and a Lagrangian relaxation, both checked in ball arithmetic.

14.1. Chord reduction of the positive edge.

For $a, b \ge 0$ put $M(a,b) = a\theta^2 + bA^2$ and $Q(a,b) = (a\theta + bA)^2/(a+b)$, with $Q(0,0) = 0$.

Lemma 14.2 (chord reduction)**.** *Let K_+ be a finite measure on $[\theta, A]$, $\nu(dx) = x^{-2}K_+(dx)$, and*

$$a_+ = \int \frac{A-x}{A-\theta}\,\nu(dx), \qquad b_+ = \int \frac{x-\theta}{A-\theta}\,\nu(dx), \qquad K_+^{\#} = a_+\theta^2\delta_\theta + b_+A^2\delta_A.$$

(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 $\Lambda = \nu(\mathbb{R}) \le \theta^{-2}K_+(\mathbb{R})$ and $m = \int x\,\nu(dx)$. Since $\theta(A-x)+A(x-\theta) = (A-\theta)x$, we have $a_+ + b_+ = \Lambda$ and $a_+\theta + b_+A = m$. 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, $x^2 \le \frac{A-x}{A-\theta}\theta^2 + \frac{x-\theta}{A-\theta}A^2$ on $[\theta, A]$; integrating against ν gives $K_+(\mathbb{R}) \le M(a_+,b_+)$.

(ii) As in the proof of Lemma 13.3, $Z_{K_+} \overset{d}{=} S_N - m$, 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 $\pi = (a_+\delta_\theta + b_+\delta_A)/\Lambda$, with partial sums $S_n^{\#}$, independent of N. For convex φ and $x \in [\theta, A]$, $\varphi(x) \le \frac{A-x}{A-\theta}\varphi(\theta) + \frac{x-\theta}{A-\theta}\varphi(A)$, 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, $S_N^{\#} \overset{d}{=} \theta N_{a_+} + AN_{b_+}$ 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 14.3 (the rate functions)**.** *On $[0,\infty)^2$ the functions M, Q and $M - Q$ are continuous and nondecreasing in each variable, $M(a,b) - Q(a,b) = ab(A-\theta)^2/(a+b)$ for $a + b > 0$, and $Q(a,b) \ge \max(a\theta^2, bA^2)$.*

Proof. For $a + b > 0$, $(a\theta^2 + bA^2)(a+b) - (a\theta + bA)^2 = ab(A-\theta)^2$, 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 $\sigma = a\theta + bA$, $\partial_a Q = \sigma\,(a\theta + b(2\theta - A))/(a+b)^2 \ge 0$ because $2\theta = 1.7 > A$, and $\partial_b Q = \sigma\,(a(2A-\theta) + bA)/(a+b)^2 \ge 0$. Hence $Q(a,b) \ge Q(a,0) = a\theta^2$ and $Q(a,b) \ge Q(0,b) = bA^2$. □

14.2. **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

$$\mu_B = 1 - \max\bigl(Q(a_2,b_2), \tfrac{1}{2}\bigr) + M(a_2,b_2) - M(a_1,b_1), \qquad \text{cap}_B = (b_2 - b_1)A^2,$$

$C_B = \theta(N_{a_1} - a_1) + A(N_{b_1} - b_1)$ (independent Poisson counts) and $h_B(r) = \mathbb{E}|C_B + r|$. Let $\mathcal{W}_B$ be the set of measures W on $[-A, \theta] \cup \{A\}$ 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 14.4 (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 $K_+ = K|_{[\theta,A]}$ (Lemma 14.2).* (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 14.2(i) and 14.3, $\max(a_+\theta^2, b_+A^2) \le Q(a_+,b_+) \le V_+ < \frac{4}{5}$. So $a_+ < 0.8/\theta^2 = 1.107\ldots < \frac{28}{25}$ 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 14.3, $Q_1 \le Q_+ \le Q_2$ 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 14.2(i). So B is not empty.

Let $W_0 = K|_{[-A,\theta)}$, of mass $1 - V_+$, and $W_1 = W_0 + (a_+ - a_1)\theta^2\delta_\theta + (b_+ - b_1)A^2\delta_A$. Then $K_+^{\#} + W_0 = K_c + W_1$ with $K_c = a_1\theta^2\delta_\theta + b_1A^2\delta_A$, and $Z_{K_c} \overset{d}{=} C_B$. The measure W_1 is carried by $[-A,\theta] \cup \{A\}$, $W_1(\{A\}) = (b_+ - b_1)A^2 \le \text{cap}_B$, 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 14.2(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 $Z_W \stackrel{d}{=} Z_{W_1} + \sigma G$ with $\sigma^2 = \mu_B - W_1(\mathbb{R})$. Now $\mathbb{E}|Z_K| \le \mathbb{E}|Z_{K_+^\# + W_0}|$ by Lemma 14.2(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. □

14.3. **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 $R_B = [-A\mu_B,\ \theta\mu_B + (A-\theta)\mathrm{cap}_B] \times [0,\ A^2\mu_B]$.

Lemma 14.5 (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 $w = W(\{A\}) \le \mathrm{cap}_B$: $\kappa_3 \le \theta(\mu_B - w) + Aw \le \theta\mu_B + (A-\theta)\mathrm{cap}_B$, $\kappa_3 \ge -A\mu_B$, and $0 \le \kappa_4 \le A^2\mu_B$. □

Lemma 14.6 (linear functionals)**.** *Let $\mathcal{R}$ be a Borel function on $[-A,\theta] \cup \{A\}$, bounded above on $[-A,\theta]$ by S. Then $\int \mathcal{R}\,dW \le \mu_B S + \mathrm{cap}_B\,(\mathcal{R}(A) - S)_+$ for every $W \in \mathcal{W}_B$.*

Proof. With $w = W(\{A\}) \in [0, \mathrm{cap}_B]$ we have $W([-A,\theta]) = \mu_B - w \ge 0$. So $\int \mathcal{R}\,dW \le (\mu_B - w)S + w\mathcal{R}(A) = \mu_B S + w(\mathcal{R}(A) - S) \le \mu_B S + \mathrm{cap}_B(\mathcal{R}(A) - S)_+$. □

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 $j \in \{3, \dots, 16\}$, $s_3, s_4 \in \mathbb{R}$, $\gamma_j(x) = x^{j-2} - s_3x - s_4x^2$ and $S \ge \sup_{[-A,\theta]} \gamma_j$. Then $\kappa_j = \int \gamma_j\,dW + s_3\kappa_3 + s_4\kappa_4$, so Lemma 14.6 gives

$$\kappa_j \le U_j := \mu_B S + \mathrm{cap}_B(\gamma_j(A) - S)_+ + \max(s_3k_3^-, s_3k_3^+) + \max(s_4k_4^-, s_4k_4^+).$$

The lower bound L_j comes in the same way from $-\gamma_j$ (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 $\gamma(x) = -s_3x - s_4x^2$ and $S \ge \sup_{[-A,\theta]} \gamma$. For every $W \in \mathcal{W}_B(\mathcal{C})$ we have $0 = \int \gamma\,dW + s_3\kappa_3 + s_4\kappa_4 \le \Phi := \mu_B S + \mathrm{cap}_B(\gamma(A) - S)_+ + \max(s_3k_3^-, s_3k_3^+) + \max(s_4k_4^-, s_4k_4^+)$. 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 14.5, $\mathbb{E}\varphi(Z_W) = \sum_k c_k P_k$. 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 $\mathcal{W}_B(\mathcal{C})$:

$$w_\alpha - X^-Y - Y^-X + X^-Y^-, \qquad w_\alpha - X^+Y - Y^+X + X^+Y^+,$$
$$-w_\alpha + X^+Y + Y^-X - X^+Y^-, \qquad -w_\alpha + X^-Y + Y^+X - X^-Y^+,$$
$$\mu_B^{t-1}\int |x|^{s_\alpha}\,dW - w_\alpha, \qquad \mu_B^{t-1}\int |x|^{s_\alpha}\,dW + w_\alpha \qquad (s_\alpha = \textstyle\sum_i(\alpha_i - 2)),$$
$$k_3^+ - \kappa_3, \quad \kappa_3 - k_3^-, \quad k_4^+ - \kappa_4, \quad \kappa_4 - k_4^-.$$

The first four are the McCormick inequalities $(X - X^-)(Y - Y^-) \geq 0$, $(X^+ - X)(Y^+ - Y) \geq 0$, $(X^+ - X)(Y - Y^-) \geq 0$, $(X - X^-)(Y^+ - Y) \geq 0$. The next two are Hölder's inequality: for $\mu_B > 0$ and the probability measure W/μ_B, $\prod_i \mathbb{E}|x|^{p_i} \leq \prod_i (\mathbb{E}|x|^s)^{p_i/s} = \mathbb{E}|x|^s$ with $p_i = \alpha_i - 2 \geq 1$ and $s = \sum p_i$ (Lyapunov), so $|\kappa^\alpha| \leq \prod_i \int |x|^{\alpha_i - 2} dW \leq \mu_B^{t-1} \int |x|^{s_\alpha} dW$; 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 $c'' + \int \mathcal{R}\, dW + \sum_\alpha e'_\alpha w_\alpha$ with $\mathcal{R}(x) = \sum_j p'_j x^{j-2} + \sum_s \eta_s |x|^s$. By Lemma 14.6 and $w_\alpha \in [\kappa^{\alpha,-}, \kappa^{\alpha,+}]$,

$$\mathbb{E}\varphi(Z_W) \leq \beta := c'' + \mu_B S_{\mathcal{R}} + \mathrm{cap}_B(\mathcal{R}(A) - S_{\mathcal{R}})_+ + \sum_\alpha \max(e'_\alpha \kappa^{\alpha,-}, e'_\alpha \kappa^{\alpha,+}),$$

for any $S_{\mathcal{R}} \geq \sup_{[-A,\theta]} \mathcal{R}$. On $[-A, 0]$ and on $[0, \theta]$, $\mathcal{R}$ is a polynomial.

Lemma 14.7 (majorant test)**.** *Let $L \geq \theta a_1 + A b_1$ and $n_a, n_b \geq 0$. For $n \leq n_a$, $m \leq n_b$ put $\pi_{nm} = \mathbb{P}(N_{a_1} = n)\mathbb{P}(N_{b_1} = m)$ and $c_{nm} = \theta(n - a_1) + A(m - b_1)$. Let $T \geq \mathbb{P}(N_{a_1} > n_a) + \mathbb{P}(N_{b_1} > n_b)$ and $e = (T(\theta^2 a_1 + A^2 b_1))^{1/2}$.* (i) *$h_B(r) \leq H(r) := \sum_{n \leq n_a, m \leq n_b} \pi_{nm} |c_{nm} + r| + T|r| + e$ for all r.* (ii) *$h_B(r) = r$ for $r \geq L$, and $h_B(r) \leq -r + \delta$ for $r \leq -L$, where $\delta = 2\sum_{n \leq n_a, m \leq n_b} \pi_{nm}(c_{nm} - L)_+ + 2e$.* (iii) *Let φ be a polynomial and $\varepsilon \geq 0$. 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 $\varphi + \varepsilon \geq H$ on $[-L, L]$. Then $\varphi + \varepsilon \geq h_B$ on $\mathbb{R}$.*

Proof. Let $E = \{N_{a_1} \leq n_a,\ N_{b_1} \leq n_b\}$, so $\mathbb{P}(E^c) \leq T$, and recall $\mathbb{E}C_B = 0$, $\mathbb{E}C_B^2 = \theta^2 a_1 + A^2 b_1$. (i) $\mathbb{E}[|C_B + r|; E]$ is the sum, and $\mathbb{E}[|C_B + r|; E^c] \leq |r|\mathbb{P}(E^c) + \mathbb{E}[|C_B|; E^c] \leq T|r| + (\mathbb{P}(E^c)\mathbb{E}C_B^2)^{1/2}$ (Cauchy–Schwarz). (ii) $C_B \geq -\theta a_1 - A b_1 \geq -L$, so $C_B + r \geq 0$ and $h_B(r) = r$ for $r \geq L$. For $r \leq -L$, $|C_B + r| = |r| - C_B + 2(C_B - |r|)_+$, so $h_B(r) = -r + 2\mathbb{E}(C_B - |r|)_+ \leq -r + 2\mathbb{E}(C_B - L)_+$. On E this is the sum, and on E^c use $(C_B - L)_+ \leq |C_B|$ and Cauchy–Schwarz as in (i). (iii) For $t \geq 0$, $\varphi(L + t) \geq L + t = h_B(L + t)$ and $\varphi(-L - t) \geq L + t + \delta \geq h_B(-L - t)$ by (ii); on $[-L, L]$ use (i). □

On $[-L, L]$, H is piecewise linear, with kinks at 0 and at the points $-c_{nm}$, which are exact rationals. The test $\varphi + \varepsilon \geq H$ is therefore one polynomial upper bound per piece, $\sup(H - \varphi) \leq \varepsilon$.

Lemma 14.8 (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 14.5. □

14.4. **The certified heavy-region data and the proof.**

Proposition 14.9 (certified heavy-region data)**.** [computer-assisted, see Sec. 16] *The rate rectangle $[0, \frac{28}{25}] \times [0, \frac{17}{50}]$ is tiled by dyadic leaf boxes B (from a 16×16 grid, each box split into four up to four times; the box with indices (i_a, i_b) at level d is $[i_a, i_a + 1] \cdot \frac{28}{25} 2^{-4-d} \times [i_b, i_b + 1] \cdot \frac{17}{50} 2^{-4-d}$). Every leaf box is either empty ($Q(a_1, b_1) \geq \frac{4}{5}$ or $M(a_2, b_2) < \frac{1}{2}$, in exact arithmetic), or carries a tiling of R_B by cells $\mathcal{C}$ (dyadic quadtree leaves), each with a certificate that is either an emptiness certificate ((a) with $L_j > U_j$ for some j, or (b) with $\Phi < 0$), or a polynomial φ of degree ≤ 16 with L, the multipliers of (a) and (c), such that the tail test of Lemma 14.7(iii) holds at L, $\varphi + \varepsilon \geq H$ on $[-L, L]$, and $\beta + \varepsilon < C_5$. In the recorded data there are 436 leaves (certified at levels 0–4: 96,*

71, 66, 44, 3; empty: 134, 12, 6, 3, 1) and 1 237 cell certificates (1 236 polynomial, 1 Farkas; cells of depth 0, 1, 2: 109, 536, 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* $\frac{1}{2}$*).*

How it is verified. All decisions use exact rationals and ball arithmetic 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. θ, 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, and $p \le q_0 + \sum_{k \text{ odd}} |q_k| d^k + \sum_{k\ge 2 \text{ even}} \max(q_k, 0) d^k$ on the piece; pieces are bisected while this bound exceeds the best value found by more than a tolerance, and 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 $S_{\mathcal{R}}$ in (c) (separately on $[-A, 0]$ and $[0, \theta]$), and for each piece of $H - \varphi$ in Lemma 14.7. *Majorant data.* 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 $(1 - \sum_{n\le n_a} \mathbb{P}(N_{a_1} = n)) + (1 - \sum_{m \le n_b} \mathbb{P}(N_{b_1} = m))$, clipped at 0. L is the double stored in the certificate (between 7.20 and 14.63), checked to be $\ge \theta a_1 + A b_1$. The returned ε is the upper end of the largest piece bound, and $\varepsilon = 0$ if all are ≤ 0. *Tilings.* Every index lies in its grid ($0 \le i_a, i_b < 2^{4+d}$), so every leaf lies in exactly one initial box, and each of the 256 initial boxes contains at least one leaf; for each initial box its leaves are pairwise non-nested dyadic sub-squares whose areas add up to its area. Distinct non-nested dyadic squares have disjoint interiors, so their union has full measure and, being closed, is the whole box. The cells of R_B are checked in the same way. *Cells.* A polynomial certificate passes if φ has 17 finite coefficients, the tail test holds at L, and $\beta + \varepsilon < C_5$, where 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) passes whatever its type; a Farkas certificate passes if $\Phi < 0$ in (b). The recorded certificates are not in the code archive. A cover regenerated for this paper with the generator of Section 16 (424 leaves; 281 boxes with 1 244 cell certificates and 143 empty boxes; largest bound $0.854900 < C_5$) is accepted by the same verifier (Section 16.5); any accepted cover proves Theorem 14.1. □

Proof of Theorem 14.1. Reflection $x \mapsto -x$ maps Z_K to $-Z_K$ and exchanges V_+ and V_-, so assume $\frac{1}{2} \le V_+ < \frac{4}{5}$. By Lemma 14.4(i), the chord rates (a_+, b_+) lie in some leaf box B of Proposition 14.9. By Lemma 14.4(ii), B is not empty, so it carries a tiling of R_B by cells with certificates. Also by Lemma 14.4(ii), there is $W \in \mathcal{W}_B$ with $\mathbb{E}|Z_K| \le \mathbb{E} h_B(Z_W)$. By Lemma 14.5, $(\kappa_3(W), \kappa_4(W)) \in R_B$, so it lies in some cell $\mathcal{C}$ of the tiling. Then $\mathcal{W}_B(\mathcal{C}) \ne \emptyset$, so the certificate of $\mathcal{C}$ is not an emptiness certificate ((a) or (b)). It is therefore a polynomial φ with $\varphi + \varepsilon \ge h_B$ (Lemma 14.7) and $\mathbb{E}\varphi(Z_W) \le \beta$ (by (c)), where $\beta + \varepsilon < C_5$. Lemma 14.8 gives $\mathbb{E}|Z_K| \le \beta + \varepsilon < C_5$. □

15. The light part of the far region

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 $V_- = K([-A, -\theta])$, and $F_{\text{light}} = \{V_+ < \frac{1}{2},\ V_- < \frac{1}{2}\}$.

Theorem 15.1 (light far region)**.** [computer-assisted, see Sec. 16] *Every finitely supported probability measure* K *on* $[-A, A]$ *with* $V_+ < \frac{1}{2}$ *and* $V_- < \frac{1}{2}$ *satisfies* $\mathbb{E}|Z_K| \le \frac{171}{200}$.

15.1. **Notation.** For a finitely supported finite measure K, $Z_K = \sigma G + \sum_{x \ne 0} x(N_x - \lambda_x)$ with $\sigma^2 = K(\{0\})$, $\lambda_x = K(\{x\})/x^2$ and independent $G \sim N(0,1)$, $N_x \sim \mathrm{Poisson}(\lambda_x)$. 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. We use: (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 $X+Z \le_{cx} Y+Z$. (All variables are integrable. (CO1) is the conditional Jensen inequality $\mathbb{E}[\varphi(X+M)\mid X]\ge\varphi(X)$ for convex φ; (CO2) follows by integrating $\mathbb{E}\varphi(X+z)\le\mathbb{E}\varphi(Y+z)$, valid for every convex φ and every $z\in\mathbb{R}$, against the law of Z.) $\mathbb{E}|Z_K|$ is invariant under $K\mapsto K(-dx)$.

15.2. **The split chain.**

Lemma 15.2 (two-point spread)**.** *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 $N_a\sim\mathrm{Poisson}(p_a)$, $N_b\sim\mathrm{Poisson}(p_b)$, 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 $\sum_x N_x^a\sim\mathrm{Poisson}(p_a)$, $\sum_x N_x^b\sim\mathrm{Poisson}(p_b)$ 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 15.3 (window mass from the rates)**.** *In Lemma 15.2, $K(W)=a^2p_a+b^2p_b-E_W$ with $E_W=\int(x-a)(b-x)\,d\nu$ and*

$$0\le E_W\le\frac{(b-a)^2p_ap_b}{p_a+p_b}\le\Big(\frac{b-a}{b+a}\Big)^2(a^2p_a+b^2p_b).$$

Hence (i) $K(W)\le a^2p_a+b^2p_b$ and (ii) $a^2p_a+b^2p_b\le K(W)\frac{(a+b)^2}{4ab}$; and (iii) if $(p_a,p_b)\in B=[P_a,q_a]\times[P_b,q_b]$ then $V_{\mathrm{lo}}\le K(W)\le V_{\mathrm{hi}}$, where $\mathrm{exc}=\frac{(b-a)^2q_aq_b}{q_a+q_b}$, $V_{\mathrm{lo}}=a^2P_a+b^2P_b-\mathrm{exc}$, $V_{\mathrm{hi}}=a^2q_a+b^2q_b$.

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. $\frac{p_ap_b}{p_a+p_b}$ is nondecreasing in each rate. □

Lemma 15.4 (lower corner and top-up)**.** *In Lemma 15.2 let $K(\mathbb{R})=1$, $(p_a,p_b)\in B$, $P=(P_a,P_b)$ and $\mu=1-a^2P_a-b^2P_b+\mathrm{exc}$. Then $X''(p)+Z_{K_R}\le_{cx}X''(P)+Z_{K'}$ with $K'=K_R+t_a\delta_a+t_b\delta_b+g\delta_0$, $t_a=a^2(p_a-P_a)\in[0,a^2(q_a-P_a)]$, $t_b=b^2(p_b-P_b)\in[0,b^2(q_b-P_b)]$, $g\ge0$, $K'(\mathbb{R})=\mu$.*

Proof. Poisson splitting gives $X''(p)\overset{d}{=}X''(P)+Z_{t_a\delta_a+t_b\delta_b}$. By Lemma 15.3, $K_R(\mathbb{R})+t_a+t_b=1+E_W-a^2P_a-b^2P_b\le\mu$; the independent $Z_{g\delta_0}=\sqrt{g}\,G$ is added by (CO1). □

Corollary 15.5 (reduction to the lower corner)**.** $\mathbb{E}|Z_K|\le\mathbb{E}h_P(Z_{K'})$, $h_P(r)=\sum_{i,j\ge0}\pi_i(P_a)\pi_j(P_b)\,|r+ai+bj-aP_a-bP_b|$, $\pi_i(\lambda)=e^{-\lambda}\lambda^i/i!$.

Proof. $|\cdot|$ is convex; apply Lemmas 15.2 and 15.4 and condition on $Z_{K'}$. □

Lemma 15.6 (a window straddling θ)**.** *In Lemma 15.2 let $a<\theta<b<2a$, $\varsigma=K_W([\theta,b])$, $\beta=\frac{b^2(\theta-a)}{(b-a)\theta^2}$ and $\rho=\frac{q_a(b-a)\theta^2}{b-\theta}$. If (p_a,p_b) lies in the box B of Lemma 15.3(iii), then $\beta<1$ and*

$$\varsigma\ \ge\ s_{\mathrm{lo}}:=\max\Big(0,\ \frac{b^2P_b-\beta V_{\mathrm{hi}}}{1-\beta},\ b^2P_b-\beta\rho\Big);\qquad\text{hence}\quad K_R([\theta,A])=K([\theta,A])-\varsigma\le V_+-s_{\mathrm{lo}}.$$

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 $b^2p_b\le\beta r+\varsigma$ 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 $r=K(W)-\varsigma\le V_{\mathrm{hi}}-\varsigma$. With $p_b\ge P_b$: $\varsigma\ge b^2P_b-\beta\rho$ and $\varsigma(1-\beta)\ge b^2P_b-\beta V_{\mathrm{hi}}$. Finally $(b-a)\theta^2-b^2(\theta-a)=(b-\theta)(a(b+\theta)-b\theta)>0$ since $a>\frac{b}{2}>\frac{b\theta}{b+\theta}$. □

15.3. **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 15.7 (certificate)**.** *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 $f(x) \le y_0 + \sum_I y_I \mathbf{1}_I(x) + y_3 x + y_4 x^2$ on every closed piece between consecutive breakpoints outside W, $f(p) \le y_0 + y_p + y_3 p + y_4 p^2$ 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'. □

Here $[\mathrm{lo}_\alpha, \mathrm{hi}_\alpha]$ is the interval product of the ranges of the factors of w_α. 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. Only non-strict inequalities are needed in (C1), (C2) and (C4). Any $z \ge 0$ gives a valid bound, the residuals being paid in E_w; the choice of tangent points and the order of the inequality rows are conventions of the certificate format and do not affect soundness.

What the exact verifier checks. Everything is recomputed from the cell definition and the certificate (all entries are doubles, stored in hexadecimal and converted exactly; arithmetic in exact rationals). (V1) $\hat{h}$: upper bounds for $\pi_i(P_a)$, $\pi_j(P_b)$, $i \le I = P + 14\sqrt{P} + 25$, from ball arithmetic (160 bits), and the tail $\sum_{(i,j)\ \mathrm{outside}} \pi_i\pi_j|r + c_{ij}| \le \pi_T|r| + E_T$ with $\mathbb{P}(N > I) \le \pi_I\varrho/(1-\varrho)$, $\varrho = P/(I+1)$, $\mathbb{E}[N\mathbf{1}\{N > I\}] = P(\pi_I + \mathbb{P}(N > I))$ and $|c_{ij}| \le ai + bj + aP_a + bP_b$ (here P stands for P_a or P_b); then $\varphi - \hat{h} \ge 0$ 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; $z \ge 0$; γ, ε, E_w, d, e_0 and f exact. (V4) The x-dual (C4), exact. (V5) The final bound is $\le \frac{171}{200}$. Polynomial checks $P \ge 0$ on $[\mathrm{lo}, \mathrm{hi}]$: Taylor expansion at the midpoint, accepted if $c_0 - \sum_k |c_k|h^k \ge 0$ (h the half-width), rejected if $c_0 < 0$, else bisection (depth ≤ 18) and finally an exact Sturm count of the squarefree part (a root in the closed interval means rejection; with no root, $P \ge 0$ is checked at a point); on half-lines: all coefficients ≥ 0 after the shift, else Sturm.

15.4. **Decomposition and cells.**

Windows. $a_k = 0.3 \cdot 1.03^k$ rounded to 4 decimals, $b_k = \frac{6}{5}a_k$, for $k \ge 0$ while $b_k < A$, plus $[\frac{5}{6}A, A]$; the family consists of these and their mirror images. A window is *near* if its end nearer to 0 is below θ in absolute value ($k \le 35$); the others lie in $[\theta, A]$ or $[-A, -\theta]$.

Lemma 15.8 (three cases)**.** *For $K \in F_{\mathrm{light}}$, after a reflection, at least one of the following holds: (1) some near window carries more than $\frac{1}{4}$, and a heaviest near window $W = [a, b]$ ($K(W) \ge K(W')$ for every near W') is positive, with $K(W) > \frac{1}{4}$; or (2) every near window carries $\le \frac{1}{4}$, $V_+ \in [\frac{1}{4}, \frac{1}{2})$ and $V_- \le V_+$; or (3) every window carries $\le \frac{1}{4}$, $V_\pm < \frac{1}{4}$ and $\int x\,dK \ge 0$.*

Proof. If some near window carries more than $\frac{1}{4}$, reflect so that a heaviest one is positive. Otherwise, if $\max(V_+, V_-) \geq \frac{1}{4}$, 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 $\leq \max(V_+, V_-) < \frac{1}{4}$. □

Lemma 15.9 (cells, $\delta = \frac{1}{20}$)**.** *In each case of Lemma 15.8, K' of Lemma 15.4 (cases 1–2), respectively K (case 3), lies in the rest class of a cell that is a root of the following enumeration or a descendant of one under the subdivision rule.*

- *Case 1 (near-split boxes N/k/i, j; 7956 roots): $W = [a, b] = [a_k, b_k]$, (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 15.3(ii) and $K(W) \leq 1$, $i + j \leq \lfloor (a+b)^2/(4ab\delta) \rfloor = \lfloor 20 \cdot \frac{121}{120} \rfloor = 20$. Boxes with $V_{\mathrm{hi}} \leq \frac{1}{4}$ or $V_{\mathrm{lo}} > 1$ contain no admissible rates, by Lemma 15.3(iii). Caps on K_R: $K_R([\theta, A]) \leq \frac{1}{2} - s_{\mathrm{lo}}$ ($V_+ < \frac{1}{2}$ and Lemma 15.6; $s_{\mathrm{lo}} = 0$ unless $b > \theta$, that is, $k \geq 30$), $K_R([-A, -\theta]) \leq \frac{1}{2}$ ($V_- < \frac{1}{2}$), and $K_R(W') \leq V_{\mathrm{hi}}$ for every near $W' \neq W$ (W is heaviest).*
- *Case 2 (chord boxes C/i, j; 60 roots): Lemma 15.2 with $W = [\theta, A]$ (the chord reduction); $V_+ = K(W) < \frac{1}{2}$ gives $i+j \leq \lceil v(a+b)^2/(4ab\delta) \rceil - 1 = 10$ with $v = \frac{1}{2}$ (indeed $\frac{1}{2} \cdot \frac{(\theta+A)^2}{4\theta A} < \frac{11}{20}$); boxes with $V_{\mathrm{hi}} < \frac{1}{4}$ or $V_{\mathrm{lo}} \geq \frac{1}{2}$ are excluded. K_R lives on $[-A, \theta)$; caps: $K_R([-A, -\theta]) \leq \min(\frac{1}{2}, V_{\mathrm{hi}})$ ($V_- \leq V_+ \leq V_{\mathrm{hi}}$), $K_R(W') \leq \frac{1}{4}$ for every near W'.*
- *Case 3 (light cells L/s, t; 537 roots): $m_1 = \int x\, dK \leq AV_+ + \theta(1 - V_+) < \frac{A}{4} + \frac{3\theta}{4} = 1.0225$ and $m_2 = \int x^2 dK \leq A^2(V_+ + V_-) + \theta^2(1 - V_+ - V_-) < \frac{A^2+\theta^2}{2} = 1.547 < \frac{31}{20}$, 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 ($m_2 \geq m_1^2$). Caps: every window $\leq \frac{1}{4}$, $K([\theta, A]) \leq \frac{1}{2}$, $K([-A, -\theta]) \leq \frac{1}{2}$.*
- *Subdivision rule. A failed 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_+ is the cap of K_R on $[\theta, A]$ plus the caps of the atoms at points $\geq \theta$, 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 $\geq \theta$ is $\leq c_+$, at points $\leq -\theta$ it is $\leq c_-$, every other point has $|x| < \theta$, and $K'(\mathbb{R}) = \mu$. A failed 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.*

Proof. In each case the root cells cover all admissible parameters: the bounds on $i+j$, the excluded boxes and the caps are justified in the items (by Lemma 15.3, Lemma 15.6, $V_\pm < \frac{1}{2}$ and the choice of W as a heaviest window), and in case 3 by the stated bounds on m_1 and m_2. Under the subdivision rule the children of a cell cover it: $R(B)$ contains $(\int x\, dK', \int x^2 dK')$ for every K' in the rest class, the subrectangles cover $R(B)$, respectively the rectangle of the cell, and the omitted light children are empty. □

Proposition 15.10 (certified light-region data)**.** [computer-assisted, see Sec. 16] *Every required root of the enumeration of Lemma 15.9 is covered by verified cells (the cell itself or, under the subdivision rule, all its descendants), each with a certificate of Lemma 15.7 whose bound is $\leq \frac{171}{200}$ or which certifies the cell empty:*

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*

The largest bound, 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.

How it is verified. The coverage checker regenerates the required roots and the subdivision rule of Lemma 15.9 from the exact cell definitions, compares the specification of every used certificate with

the expected cell, and re-verifies each certificate with the exact verifier described after Lemma 15.7; every required root is covered and every bound is at most $\frac{171}{200}$ in exact arithmetic. The recorded certificates are not in the code archive; the certificates of windows 30–35 of case 1 were regenerated and verified for this paper (Section 16.5). □

Proof of Theorem 15.1. Let $K \in F_{\text{light}}$ be finitely supported. By Lemma 15.8, after a reflection (which does not change $\mathbb{E}|Z_K|$), one of the cases (1)–(3) holds. In cases (1)–(2), Corollary 15.5 gives $\mathbb{E}|Z_K| \le \mathbb{E}h_P(Z_{K'})$, and in case (3) $\mathbb{E}|Z_K| = \mathbb{E}h(Z_K)$ with $h = |\cdot|$. By Lemma 15.9, K' (resp. K) lies in the rest class of a root cell or of a descendant of it, and by Proposition 15.10 it lies in the rest class of a verified cell. That cell is not certified empty, so Lemma 15.7 bounds $\mathbb{E}h(Z_{K'})$ (resp. $\mathbb{E}|Z_K|$) by a number $U \le \frac{171}{200}$. □

16. Computer-assisted components

16.1. **Conventions.**

- *Decisions.* Every inequality on which a proof rests is decided either in exact rational arithmetic (Sturm sequences, exact comparisons of rationals, exact Gaussian elimination) or in outward-rounded interval or ball arithmetic (the interval arithmetic of mpmath, or the `arb` balls of python-flint), so that each 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 verifiers of Sections 5–10 share no code with their generators, and the later ones reuse only exact helpers of the earlier ones (Sturm sequences, integer square roots, tilings, moment polynomials, cone normals, envelopes). The one exception is the band computation (Proposition 13.12), whose program chooses an option and its parameters for each box in floating point and decides the box in ball arithmetic in the same run.
- *Where the code is.* All programs are in the archive `Rq_proof_code_only.zip`; the paths below are relative to its root directory `Rq_proof_source/`. The verifiers of Sections 5–10 are in `RQ-A/scripts/`, those of Sections 13 and 14 in `RQ-D/scripts/`, and that of Section 15 in `RQ-B/numerics/`. Independent re-implementations of all these computations, written from the mathematical statements without the programs above, are in `RQ-REF1/ref/` (Theorems 5.1, 6.1, 7.1, 8.1), `RQ-REF2/ref/` (Theorems 9.1, 10.1), `RQ-REF3/ref/` (Sections 11–15) and `RQ-AUD/audit/`.
- *Software.* Python 3.12.3, numpy 2.5.4, scipy 1.18.1, sympy 1.14.0, mpmath 1.3.0, python-flint 0.9.0 (`pip install numpy scipy sympy mpmath python-flint`; gmpy2 2.3.2 for some of the independent re-implementations).
- *Certificate data.* The archive contains the programs, logs and small outputs, but none of the certificate data files: the cells and boxes of Theorems 5.1–10.1 (the files listed in `RQ-A/outputs/k2_MD5SUMS.txt`, ..., `k5_MD5SUMS.txt` and `RQ-A/outputs/cover/*.json`, `quartic_cover.json`), the certificates of Theorem 14.1 (`RQ-D/outputs/plus_cert/certs_v1_r*.jsonl`) and of Theorem 15.1 (`RQ-B/numerics/cover_final/*.jsonl.xz`) are referred to by the commands below and by md5 lists in the archive, but are not in it. They can be regenerated by the generators listed in Table 10; the generators are not trusted, and any regenerated data must pass the verifier.
- *Negative tests.* Each regime of Sections 5–10 has a script that corrupts records (lowered coefficients, shrunk polytopes, removed pieces, widened intervals, altered caps and signs) and checks that the verifier rejects them; Sections 13–15 have control runs with lowered targets and mutated certificates.

16.2. **Proof method of every numbered statement.** Table 9 lists every numbered theorem, proposition, lemma, corollary, definition and remark. A statement is *computer-assisted* if its proof uses a finite computation, directly or through another computer-assisted statement. Definitions need no proof and are marked with a dash. The decimal values of explicit constants in Sections 11 and 12 (for example C_5, $A'(q_5) = \sqrt{5q_5/\ln\frac{5}{4}} < \frac{77}{50}$, E_k) are evaluations of closed forms; they are counted as by hand, and they were checked in exact rational enclosures by `RQ-REF3/ref/constants.py` (121 lines, 5.7 KB, with `RQ-REF3/ref/rig.py`, 377 lines, 10.6 KB) and in interval arithmetic by `RQ-B/numerics/uniform_k_constants.py` (95 lines, 2.9 KB); `RQ-B/numerics/constants_check.py` (73 lines, 2.9 KB) evaluates them in floating point on grids.

Table 9: Every numbered statement, proved by hand or computer-assisted.

statement	name	proof
Theorem 1.1	Main Theorem	computer-assisted
Remark 1.2	an equivalent Boolean form	computer-assisted
Remark 1.3	extremisers	computer-assisted
Corollary 3.1	the middle range	computer-assisted
Lemma 4.1	symmetry	by hand
Theorem 4.2	equal coefficients	by hand
Lemma 4.3	one-coordinate identity	by hand
Lemma 4.4	cumulants of order at most six	by hand
Lemma 4.5	cumulants of order seven to ten	computer-assisted
Lemma 4.6	moments from cumulants	by hand
Lemma 4.7	power sums	by hand
Lemma 4.8	sign information	by hand
Definition 4.9	six-moment objective bound	—
Lemma 4.10	six-moment expectation bound	by hand
Definition 4.11	ten-moment objective bound	—
Lemma 4.12	ten-moment expectation bound	computer-assisted
Definition 4.13	cell and cell certificate	—
Lemma 4.14	domination on a cell	by hand
Lemma 4.15	cell lemma	computer-assisted
Lemma 4.16	two-coordinate value	by hand
Lemma 4.17	bit reduction	by hand
Lemma 4.18	OR-region identity	by hand
Lemma 4.19	conditional expectation, box form	by hand
Definition 4.20	box envelope	—
Lemma 4.21	box envelope	by hand
Definition 4.22	box certificate	—
Lemma 4.23	box certificate lemma	by hand
Lemma 4.24	convexity in the coefficients	by hand
Lemma 4.25	conditional expectation	by hand
Definition 4.26	vertex set	—
Lemma 4.27	cone lemma	by hand
Lemma 4.28	facet minima	by hand
Definition 4.29	vertex envelope	—
Lemma 4.30	vertex envelope	by hand
Definition 4.31	vertex certificate	—
Lemma 4.32	vertex certificate lemma	computer-assisted
Lemma 4.33	lpv boxes	computer-assisted
Lemma 4.34	tail bound	by hand
Lemma 4.35	near-circle tests	by hand
Lemma 4.36	near-sphere bound	by hand
Lemma 4.37	piece tests	by hand
Definition 4.38	m-split box, first kind	—

statement	name	proof
Lemma 4.39	m-split lemma, first kind	by hand
Theorem 5.1	the central range	computer-assisted
Lemma 5.2	two-coefficient value	by hand
Lemma 5.3	algebraic identities	by hand
Lemma 5.4	quartic certificate lemma	by hand
Corollary 5.5	quartic bound for $q \geq q_2$	by hand
Lemma 5.6	near-dictator bound	by hand
Proposition 5.7	certified data for Theorem 5.1	computer-assisted
Theorem 6.1	the regime $k = 2$	computer-assisted
Lemma 6.2	two coordinates for $k = 2$	by hand
Lemma 6.3	three-bit lemma, $k = 2$	computer-assisted
Proposition 6.4	certified data for Theorem 6.1	computer-assisted
Theorem 7.1	the regime $k = 3$, upper part	computer-assisted
Lemma 7.2	two coordinates for $k = 3$	by hand
Lemma 7.3	three-bit lemma, $k = 3$	computer-assisted
Proposition 7.4	certified data for Theorem 7.1	computer-assisted
Theorem 8.1	the regime $k = 3$, lower part	computer-assisted
Corollary 8.2	the whole $k = 3$ regime	computer-assisted
Lemma 8.3	three- and four-bit lemmas, $k = 3$ lower part	computer-assisted
Definition 8.4	pieces of type TC and SG	—
Lemma 8.5	TC and SG piece lemma	computer-assisted
Definition 8.6	pieces of type TCS	—
Lemma 8.7	TCS piece lemma	computer-assisted
Definition 8.8	m-split box of kind ms5, level one	—
Lemma 8.9	m-split lemma, $k = 3$ lower part	computer-assisted
Proposition 8.10	certified data for Theorem 8.1	computer-assisted
Theorem 9.1	the regime $k = 4$	computer-assisted
Lemma 9.2	three- and four-bit lemmas, $k = 4$	computer-assisted
Definition 9.3	inner pieces	—
Definition 9.4	pieces of type TCN	—
Lemma 9.5	TCN piece lemma	computer-assisted
Definition 9.6	m-split box, $k = 4$	—
Lemma 9.7	m-split lemma, $k = 4$	computer-assisted
Proposition 9.8	certified data for Theorem 9.1	computer-assisted
Theorem 10.1	the regime $k = 5$	computer-assisted
Lemma 10.2	three- and four-bit lemmas, $k = 5$	computer-assisted
Lemma 10.3	main terms for $k = 5$	computer-assisted
Definition 10.4	split node	—
Lemma 10.5	split node lemma	computer-assisted
Definition 10.6	m-split box, $k = 5$	—
Lemma 10.7	m-split lemma, $k = 5$	computer-assisted
Proposition 10.8	certified data for Theorem 10.1	computer-assisted
Definition 11.1	Kolmogorov measures and R_{ID}	—
Lemma 11.2	level-one form	by hand
Theorem 11.3	Poissonisation	by hand
Theorem 11.4	configuration-wise Poissonisation	by hand
Proposition 11.5	size of the window	by hand
Remark 11.6	the Dirac family	by hand
Theorem 12.1	localisation	by hand
Lemma 13.1	flip formula	by hand
Lemma 13.2	conditional form	by hand
Lemma 13.3	OR-region identity with a residual	by hand
Lemma 13.4	comparison	by hand
Remark 13.5	smoothed stop-loss test functions	by hand
Lemma 13.6	stop-loss bounds	by hand
Lemma 13.7	one jump	by hand
Lemma 13.8	feasible parameters	by hand

statement	name	proof
Proposition 13.9	band bound	by hand
Lemma 13.10	absorption	by hand
Theorem 13.11	band lemma, $\theta = 0.85$, $A = 1.54$	computer-assisted
Proposition 13.12	certified band data	computer-assisted
Theorem 14.1	heavy far region	computer-assisted
Lemma 14.2	chord reduction	by hand
Lemma 14.3	the rate functions	by hand
Lemma 14.4	box reduction	by hand
Lemma 14.5	moments of the rest	by hand
Lemma 14.6	linear functionals	by hand
Lemma 14.7	majorant test	by hand
Lemma 14.8	cell certificate	by hand
Proposition 14.9	certified heavy-region data	computer-assisted
Theorem 15.1	light far region	computer-assisted
Lemma 15.2	two-point spread	by hand
Lemma 15.3	window mass from the rates	by hand
Lemma 15.4	lower corner and top-up	by hand
Corollary 15.5	reduction to the lower corner	by hand
Lemma 15.6	a window straddling θ	by hand
Lemma 15.7	certificate	by hand
Lemma 15.8	three cases	by hand
Lemma 15.9	cells, $\delta = \frac{1}{20}$	by hand
Proposition 15.10	certified light-region data	computer-assisted

16.3. **The computer-assisted statements.** Table 10 gives, for each computer-assisted statement, the method, the programs in the archive that verify it (with their sizes: lines, and KB of 1024 bytes), the certified cases and recorded running times (wall-clock times of the recorded runs, on an 8-core machine unless stated otherwise), and the commands. Statements that are computer-assisted only through others are not listed separately. Theorems 5.1–10.1, Corollaries 8.2 and 3.1, Theorems 13.11, 14.1, 15.1 and 1.1 are listed with the proposition that carries their computation. The others are Remarks 1.2 and 1.3 (through the theorems they restate); Lemmas 4.12, 4.15, 4.32 and 4.33 (through Lemma 4.5); and Lemmas 8.5, 8.7, 8.9, 9.5, 9.7, 10.3, 10.5 and 10.7 (through Lemma 4.32 or the bit lemmas 8.3, 9.2 and 10.2).

Table 10: Computer-assisted statements: method, verifying programs (lines, KB), certified cases and recorded runtime, and the commands to reproduce them (run in the directory stated). Generators are listed separately; they are not trusted.

statement	method	verifying programs (lines, KB)	cases; runtime; command
Lemma 4.5	exact symbolic algebra (sympy)	`RQ-A/scripts/verify_k3b.py` part A1 (1006, 37.2); also part A of `verify_k4.py` (737, 30.3) and `verify_k5.py` (639, 26.9)	identities of rational functions; 2 s; in `RQ-A/scripts`: `python3 verify_k3b.py A`

statement	method	verifying programs (lines, KB)	cases; runtime; command
Proposition 5.7; Theorem 5.1	(i) exact rationals, Sturm sequences over Python `Fractions`; (ii) outward-rounded intervals (mpmath, 120 bits), adaptive subdivision; (iii) exact tiling	verifier `RQ-A/scripts/verify_all.py` (449, 17.5), parts A–E; negative tests `break_tests.py` (56, 2.8). Generators: `cover_lp6.py` (137, 4.9), `lp6cert.py` (103, 4.4), `exactcert.py` (164, 5.4), `quartic_verify.py` (329, 10.3), `run_cover.sh` (6, 0.3). Data: `outputs/cover/r1a.json`, . . . , `r3b.json`, `outputs/quartic_cover.json`	379 cells, 641 boxes (20 969 sub-boxes); about 1 min (part C 1 s, part D 13 s); `python3 verify_all.py`; `python3 break_tests.py`; regeneration of one rectangle: `python3 cover_lp6.py 1 776887/500000 0 4/25 ../outputs/cover/r1a.json`; boxes: `python3 quartic_verify.py 611/400 1553774/1000000 9/25 471/1000 ../outputs/quartic_cover.json`
Lemma 6.3	exact Sturm sequences	`RQ-A/scripts/verify_k2.py` part G (716, 28.9)	256 functions; under 1 s; `python3 verify_k2.py G`
Proposition 6.4; Theorem 6.1	cells and (W1), (W2): exact rationals (Sturm); tests (A), (B), (A_3), (B_3): intervals (mpmath, 120 bits); exact tiling	verifier `RQ-A/scripts/verify_k2.py` (716, 28.9) with the exact helpers of `verify_all.py`; negative tests `break_tests_k2.py` (276, 7.8). Generators: `cover2c.py` (141, 6.0), `cert2c.py` (292, 10.3), `nearcircle.py` (66, 2.1), `nsphere3.py` (95, 3.6), `cover_k2.py` (30, 1.1), `run_cover2c.sh` (5, 0.3). Data: `outputs/cover_k2/`, `outputs/cover2c/` (117 entries in `k2_MD5SUMS.txt`)	784 cells; 55 515 boxes (48 810 lp, 4 835 near-circle, 1 189 ms with 1 669 pieces, 681 small); about 5 min (certificates 161 s); `python3 verify_k2.py`; `python3 break_tests_k2.py` (15 s)
Lemma 7.3	exact Sturm sequences	`verify_k2.py` part G with `RQ_K=3`	256 functions; under 1 s; `RQ_K=3 python3 verify_k2.py G`
Proposition 7.4; Theorem 7.1	as for Proposition 6.4	`verify_k2.py` with `RQ_K=3`; `break_tests_k2.py` with `RQ_K=3`. Generators: as for $k = 2$, with `cover_k3.py` (31, 1.1) and `run_k3.sh` (11, 0.5). Data: `outputs/k3/` (98 entries in `k3_MD5SUMS.txt`)	2 704 cells; 81 975 boxes (57 333 lp, 2 534 near-circle, 21 232 ms with 32 932 pieces, 876 small); certificates 317 s; generation 97 jobs, 34 min; `RQ_K=3 python3 verify_k2.py`
Lemma 8.3	exact Sturm sequences, division by g_4	`RQ-A/scripts/verify_k3b.py` part G (1006, 37.2); generator-side check `fourbit.py` (135, 4.6)	2^8 and 2^{16} functions (39 and 1 630 distinct polynomials); 6 s; `python3 verify_k3b.py G`; `python3 fourbit.py`
Proposition 8.10; Theorem 8.1; Corollary 8.2	exact rationals (Sturm, Gaussian elimination); (P4) by interval bisection; tests by intervals (mpmath, 120 bits)	verifier `RQ-A/scripts/verify_k3b.py` (1006, 37.2) with the helpers of `verify_all.py`; negative tests `break_tests_k3b.py` (222, 7.3). Generators: `cover5.py` (290, 10.5), `cert4.py` (258, 8.9), `cert5.py` (324, 10.8), `cover_lp10.py` (154, 5.8), `tenmom.py` (322, 11.4), `run_k3b.sh` (33, 1.4). Data: `outputs/k3b/` (37 entries in `k3b_MD5SUMS.txt`)	288 cells; 1 421 boxes; 2 845 vertex-certificate sets with 16 544 vertices; 93 s; `python3 verify_k3b.py`; regeneration `bash run_k3b.sh` (36 jobs, about 40 min)
Lemma 9.2	exact Sturm sequences	`RQ-A/scripts/verify_k4.py` part G (737, 30.3); generator-side check `bitlemma_k4.py` (99, 3.9)	as above; 6 s; `python3 verify_k4.py G`; `python3 bitlemma_k4.py`

statement	method	verifying programs (lines, KB)	cases; runtime; command
Proposition 9.8; Theorem 9.1	exact rationals; (P4) by the exact recursion of Lemma 4.28; tests by intervals	verifier `RQ-A/scripts/verify_k4.py` (737, 30.3) with the helpers of `verify_k3b.py` and `verify_all.py`; kinds check `k4_kinds_check.py` (38, 1.9); negative tests `break_tests_k4.py` (357, 13.2). Generators: `cover5.py`, `cert5.py`, `cert6.py` (389, 12.9), `sphmin.py` (81, 2.9), `cover_lp10.py`, `run_k4.sh` (66, 2.5). Data: `outputs/k4/` (81 entries in `k4_MD5SUMS.txt`)	1 268 cells; 7 261 boxes; 21 014 vertex-certificate sets with 171 488 vertices; 367 s (46 CPU-minutes); generation 80 jobs, 8.5 job-hours; `python3 verify_k4.py`; `python3 break_tests_k4.py` (10 s)
Lemma 10.2	exact Sturm sequences, division by g_5	`RQ-A/scripts/verify_k5.py` part G (639, 26.9); generator-side check `bitlemma_k5.py` (76, 3.3)	as above; 8 s; `python3 verify_k5.py G`
Proposition 10.8; Theorem 10.1; Corollary 3.1	as for Proposition 9.8; ranges of G_j by Sturm and interval Horner	verifier `RQ-A/scripts/verify_k5.py` (639, 26.9) with the helpers of `verify_k4.py`, `verify_k3b.py`, `verify_all.py`; negative tests `break_tests_k5.py` (418, 13.9). Generators: `cover6.py` (330, 12.2), `cert5.py`, `cert6.py`, `sphmin.py`, `cover_lp10.py`, `run_k5.sh` (73, 3.0), `k5_sched.py` (193, 7.5). Data: `outputs/k5/` (106 entries in `k5_MD5SUMS.txt`)	861 cells; 9 166 boxes; 52 292 vertex-certificate sets with 784 616 vertices; 4 449 s (9.8 CPU-hours); generation 105 jobs, 66 job-hours; `python3 verify_k5.py`; `python3 break_tests_k5.py` (30 s)
Proposition 13.12; Theorem 13.11	ball arithmetic (`arb`, 80 bits), exact dyadic grid comparisons; no stored data needed	verifier `RQ-D/scripts/verify_bandstar.py` (830, 29.5); controls `verify_bandstar_controls.py` (50, 2.2); box-level record and replay (evidence only; no proof depends on them) `bandstar_record.py` (452, 18.2), `bandstar_replay.py` (708, 29.1)	1 339 certified squares; 14 894 034 (Λ, m) boxes, of which 7 874 211 leaves; 793 s with 8 processes; in `RQ-D`: `python3 scripts/verify_bandstar.py all 0.0078125 8 outputs/verify_bandstar_squares.jsonl`; controls `PYTHONPATH=scripts python3 scripts/verify_bandstar_controls.py 8` (60 s)
Proposition 14.9; Theorem 14.1	exact rationals (`fmpq`) and `arb` balls (128 bits); doubles of the data read as exact dyadic rationals	verifier `RQ-D/scripts/verify_plus.py` (187, 7.3) with `plus_verify_lib.py` (488, 17.4); controls `verify_plus_controls.py` (71, 2.8); self-tests `test_plus_verify.py` (283, 12.2). Generators: `plus_cert.py` (352, 14.7), `plus_driver.py` (137, 5.5), `heavy_box_lp.py` (190, 7.8). Data: `outputs/plus_cert/certs_v1_r0.jsonl`, ..., `certs_v1_r4.jsonl`	436 leaf boxes (156 empty, 280 certified), 1 237 cell certificates; 25 s with 8 processes; in `RQ-D/scripts`: `python3 verify_plus.py ../outputs/plus_cert/certs_v1_r[0-4].jsonl --nproc 8`; regeneration `python3 plus_driver.py v1 4 4 2 4` (11 min)

statement	method	verifying programs (lines, KB)	cases; runtime; command
Proposition 15.10; Theorem 15.1	exact rationals (`Fraction`, `fmpq`), `arb` balls (160 bits) for the Poisson weights, Taylor bounds with bisection and exact Sturm counts	coverage checker `RQ-B/numerics/cover_check.py` (253, 11.4) with `cover_common.py` (166, 6.3) and `far_verify.py` (457, 17.5) (and only `cert_from_json` of `far_cert.py`); controls `cover_controls.py` (62, 3.0); script `reproduce_flight.sh` (17, 0.9). Generators: `far_cert.py` (742, 30.6), `cover_driver.py` (345, 15.1). Data: `cover_final/nsplit_D14.jsonl.xz`, `chord_D14.jsonl.xz`, `light_vl025_D18.jsonl.xz`	8 553 roots; 10 966 certificates (231 certify empty cells); about 15 min in all; in `RQ-B/numerics`: `bash reproduce_flight.sh 8`, or `python3 cover_check.py nsplit cover_final/nsplit_D14.jsonl.xz 8` (8 min), `... chord cover_final/chord_D14.jsonl.xz 2` (5 min on 2 cores), `... light cover_final/light_vl025_D18.jsonl.xz 8`
Theorem 1.1	composition of the above	—	—

16.4. **Code and data sizes.** All sizes were measured on the unzipped archive (the script `scripts/ca_inventory.py`, distributed with the LaTeX source of this paper, prints them and checks that every file cited in Table 10 exists; none is missing).

- *All code in the archive:* 636 files (609 Python files and 27 shell scripts), 101 921 lines, 4 045 KB. Of this, 13 828 lines (533.4 KB) are in `RQ-A/`, 14 401 (557.9 KB) in `RQ-B/`, 7 784 (303.0 KB) in `RQ-D/`, 15 229 (616.8 KB) in `RQ-C/` (exploratory and cross-check code), and the independent re-implementations take 4 715 lines (186.4 KB) in `RQ-REF1/`, 3 133 (113.9 KB) in `RQ-REF2/`, 4 107 (148.5 KB) in `RQ-REF3/` and 38 700 (1 583.4 KB) in `RQ-AUD/`; the remaining 24 lines (1.6 KB) are in `tools/`.
- *Programs cited in Table 10* (verifiers, negative tests, controls and self-tests, record and replay tools, driver scripts, generators): 14 937 lines, 571.4 KB; the verifiers alone (`verify_all.py`, `verify_k2.py`, `verify_k3b.py`, `verify_k4.py`, `k4_kinds_check.py`, `verify_k5.py`, `verify_bandstar.py`, `verify_plus.py`, `plus_verify_lib.py`, `cover_check.py`, `cover_common.py`, `far_verify.py`) have 5 966 lines.
- *Stored outputs and logs in the archive* (counting `.txt` files only): 99 files (166.8 KB) in `RQ-A/outputs/`, 3 (0.6 KB) in `RQ-B/numerics/`, 107 (122.0 KB) in `RQ-D/outputs/`, 58 (290.0 KB) in `RQ-C/numerics/out/`, 55 (74.4 KB) in the logs of the independent re-implementations, and 405 (1 238.0 KB) in `RQ-AUD/audit/`. The whole archive has 1 909 files and 27 202 KB (uncompressed).
- *Certificate data* (not in the archive). According to the archive's own description, the data of Theorems 9.1 and 10.1 take about 590 MB and are distributed in a separate outputs archive (together with other large files, 124 files over 1 MB and 696 MB in all). The data regenerated for this paper (Section 16.5) take 179.3 KB for Theorem 5.1 (eight cell files and the 641 quartic boxes), 4 895 KB for a complete heavy-region cover (four certificate files), 7 687 KB (uncompressed) for the 1 653 light-region certificates of windows 30–35 of case 1, and 153.6 KB for the per-square log of the band computation.

16.5. **Verifications re-run for this paper.** The archive was unzipped, all cited files were located and measured, and items (2)–(8) below were re-run twice, each time on a fresh copy of the archive, with the software versions above on an 8-core machine. The two runs gave the same results; where their running times differ, both are given. Since the certificate data are not in the archive, verifiers that read data were run either on data-free parts or on data regenerated by the (untrusted) generators.

(1) *Integrity.* `bash tools/check_pdf_md5.sh`, on the unmodified archive (before the manifests of item (2) were added): of the 122 files whose md5 sums are pinned, 90 match, 2 are log files that were modified after their md5 sums were recorded, and 30 are absent: the nine data files of Proposition 5.7, the data manifests of $k = 2, \dots, 5$, the certificate files of Propositions 14.9 and 15.10, the certificate, result and log files of the recorded run of windows 30–35, and the per-square log and four box-level record files of the band computation.

(2) *Symbolic identities.* Part A of `verify_all.py`, `verify_k2.py` ($k = 2$ and `RQ_K=3`), `verify_k3b.py`, `verify_k4.py` and `verify_k5.py` (Lemmas 4.4 and 4.5, Lemma 4.6, Lemma 5.3, Lemma 4.16 and the target formulas): all pass, 1–2 s each. Part E of `verify_all.py` (Lemma 5.6, the constant 0.940104): passes. (`verify_k2.py` and `verify_k3b.py` read their regime constants $U_\pm$, T_8, A_S from data manifests that are not in the archive; they were supplied from the values stated in Sections 6–8.)

(3) *Bit lemmas.* Part G of `verify_k2.py` ($k = 2$ and `RQ_K=3`), `verify_k3b.py`, `verify_k4.py` and `verify_k5.py`, and the generator-side checks `fourbit.py`, `bitlemma_k4.py`, `bitlemma_k5.py`: Lemmas 6.3, 7.3, 8.3, 9.2 and 10.2 are confirmed, with 39 and 1 630 distinct polynomials and exactly the stated equality cases, in at most 8 s each.

(4) *Proposition 5.7.* The data were regenerated (`cover_lp6.py` for the eight rectangles with the default initial grid of `run_cover.sh`, and `quartic_verify.py`; 30 s in all) and `verify_all.py` (parts A–E) accepted them in 14 s and 13 s: a tiling of the eight rectangles by 348 certified cells (62, 39, 32, 43, 32, 54, 32, 54), and the 641 quartic boxes (20 969 sub-boxes). Both runs regenerated the same files. The regenerated box file `quartic_cover.json` is byte-identical to the recorded one (md5 `f528c4c3a350924d8f878d9375c58af1`), and so is `r1c.json` (md5 `b72637cdb18725601f06acb31fe770f8`); the other cell files differ from the recorded 379-cell cover, whose initial grids are not recorded. `break_tests.py` on the regenerated data: 127 of 160 corrupted certificates rejected, namely 119 of the 120 coefficient decreases and 8 of the 40 increases (an accepted corruption passes every check, so it is again a valid certificate; the recorded run rejected 126 of 160), and the Sturm cross-check against sympy (300 polynomials) and the c_4 scaling test (34 of 34) as recorded.

(5) *Proposition 13.12.* `verify_bandstar.py` was re-run unchanged (518 s and 463 s with 8 processes) and reproduced every count of Proposition 13.12 exactly: 351/837/408/80 squares with 215/102/20/0 not certified, 2 094 045/5 839 031/5 825 480/1 135 478 boxes, 1 339 certified squares, and the leaf dispositions 3 114 781 / 551 105 / 2 876 016 / 128 597 / 1 203 286 / 426. The controls `verify_bandstar_controls.py` (35 s and 32 s) reproduce the recorded statements (the origin squares are certified at target shift 0 and not at 0.0005, first failing box on the Dirac curve; 63 of the 80 last-level squares fail at shift 0.001).

(6) *Proposition 14.9.* The recorded certificates are not in the archive. A complete cover was regenerated in each run with `plus_driver.py v1 4 4 2 4` (544 s and 523 s; four certificate files each, which differ between the runs but have the same counts), and `verify_plus.py` (md5 sums of the verifier and its library equal the recorded ones) accepted each in about 20 s: 424 leaves tile the rate rectangle, 281 boxes certified by 1 244 cell certificates, 143 empty, 0 failures, largest bound $0.854900 < C_5$. (The floating-point generator does not reproduce the recorded cover of 436 leaves exactly; any accepted cover proves Theorem 14.1.) Controls: 0, 0, 3, 45 and 178 of the 281 boxes fail when the target is lowered by 0, 10^{-4}, $3 \cdot 10^{-4}$, 10^{-3}, $3 \cdot 10^{-3}$, and every tiling mutation is rejected.

(7) *Proposition 15.10, partially.* Windows 30–35 of case 1 were regenerated with the documented job (`cover_driver.py nsplit OUT 1/20 1/4 1/2 14 8 30,31,32,33,34,35`, then `refine OUT 8 7`; 373 s and 337 s), which produced the same stage counts as the recorded batch (1 326 and 336 and 16 jobs) and 1 653 certificates. `cover_check.py nsplit` (39 s and 37 s) accepted all 1 653 (5 certify empty cells), covered all 1 326 roots of these windows, and found the largest bound $U = 0.854996980551545$, equal in all printed digits to the largest bound of the whole

light region in Proposition 15.10. The other 6 630 roots of case 1 and cases 2–3 were not regenerated.

(8) *Constants.* `RQ-REF3/ref/constants.py`: all 25 checks pass (among them $\frac{171}{200} < C_5$ with margin $1.005 \cdot 10^{-4}$, $C_4 < C_5 < C_6$, $A'(q_5) = 1.538044391650755 < \frac{77}{50}$, and the numerical facts used in Lemma 15.9 and Section 14), with output identical to the recorded log; the `rig.py` self-test and `RQ-B/numerics/uniform_k_constants.py` (interval arithmetic) pass; `constants_check.py` reproduces the values E_k of Proposition 11.5 in floating point.

Not re-run: the verifiers of Propositions 6.4, 7.4, 8.10, 9.8 and 10.8 on their certificate data (absent from the archive; the recorded regeneration times are about 34 min for $k = 3$, 40 min for the lower part of $k = 3$, 8.5 job-hours for $k = 4$ and 66 job-hours for $k = 5$; none is recorded for $k = 2$), the remaining 85% of the light-region certificates, and the negative tests of Theorems 6.1–10.1, which need the same data.

References

[BF3] BF3, *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*, unpublished report on Open Questions 5–6 of Chase–Filmus–Minzer–Mossel–Saurabh, 22 October 2026, 76 pp.

[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.

Disclosure

This text is an AI-generated proof, prompted by Paata Ivanisvili in Grok Bot from October 21 to October 27, 2026. It was subsequently revised and polished, again by Grok Bots. It is essentially the raw output obtained after a series of prompts.