

CARATHÉODORY NUMBERS OF THE BARVINOK–NOVIK ORBITOPES, OF ALL FOUR-DIMENSIONAL $SO(2)$ -ORBITOPES, AND OF A FURTHER FAMILY

PAATA IVANISVILI

This proof was generated on October 27, 2026, by Grok Bot using Cursor's agents, guided by several prompts from Paata Ivanisvili

ABSTRACT. For a trigonometric moment curve $U_A(t) = (e^{ia_1 t}, \dots, e^{ia_d t}) \in \mathbb{C}^d = \mathbb{R}^{2d}$, let $\mathcal{C}_A = \text{conv } U_A(\mathbb{R})$ be the corresponding $SO(2)$ -orbitope (a Carathéodory orbitope in the terminology of Sanyal, Sottile and Sturmfels). They asked for the Carathéodory numbers of orbitopes (Orbitopes, Question 3). We prove: (A) the Barvinok–Novik orbitope $B_k = \mathcal{C}_{(1,3,\dots,2k-1)} \subset \mathbb{R}^{2k}$ has Carathéodory number $2k - 1$ for $k \geq 2$; (B) $\mathcal{C}_{(a,b)}$ has Carathéodory number 3 for all co-prime $1 \leq a < b$, so every four-dimensional $SO(2)$ -orbitope has Carathéodory number 3; (C) $\mathcal{C}_{(1,2,\dots,d-1,2d-1)}$ has Carathéodory number $2d - 1$ for $d \geq 2$. In all three cases Fenchel's bound $(2k, 4, 2d)$ is not attained. More generally, for $d \geq 2$ the Carathéodory number is $2d - 1$ whenever $a_d = 2d - 1$, $\{0, \pm a_1, \dots, \pm a_{d-1}\}$ is a complete residue system modulo a_d , and the contact points of every face with a_d contact points are equally spaced. We verify the last condition for all such A with $2 \leq d \leq 5$. The verification is computer-assisted for 3 of the 8 sets with $d = 4$ and 13 of the 16 sets with $d = 5$. In (A), for $k \geq 3$, the value is far above the dimension count $k + 1$, and it is attained on the boundary. The lower bound in (A) is elementary and also follows from known results on real ranks of binary forms; the new content is the upper bound. The upper bounds come from a ray-and-chord argument: rays from curve points through an interior point are followed into the faces of the orbitope, and averaging over a regular polygon of starting points is combined with an elementary inequality for chords of the unit disk.

1. STATEMENTS

For integers $0 < a_1 < \dots < a_d$ let $U(t) = U_A(t) = (e^{ia_1 t}, \dots, e^{ia_d t})$, $t \in S := \mathbb{R}/2\pi\mathbb{Z}$, where $\mathbb{C}^d$ is identified with $\mathbb{R}^{2d}$ via $x_m = x_{\cos m} + i x_{\sin m}$. So U_A is the curve $(\cos a_1 t, \sin a_1 t, \dots, \cos a_d t, \sin a_d t)$. Write $z_m(x) \in \mathbb{C}$ for the coordinate of frequency $m \in A$, let $X = U(S)$ and $K = \mathcal{C}_A = \text{conv } X$. For $p \in K$ let d_p be the least number of extreme points of K whose convex hull contains p , and $\mathfrak{c}(K) = \sup_p d_p$. This is the Carathéodory number of [11, §2.1], where Question 3 asks: *What are the Carathéodory numbers of orbitopes?*

Standing facts. (i) The functions $\cos mt, \sin mt$ ($m \in A$) are linearly independent, so X spans $\mathbb{R}^{2d}$. For any integer $n > \max A$, $0 = \frac{1}{n} \sum_{j < n} U(2\pi j/n) \in K$, so the affine hull of K is $\mathbb{R}^{2d}$ and K has nonempty interior. (ii) $|U(t)|^2 = d$ is constant, and U is injective if $\gcd(A) = 1$. Then each $U(s)$ is exposed by $\langle U(s), \cdot \rangle$, and the extreme points of K are exactly the points of X (every point of $\text{conv } X$ is a finite convex combination of points of X , and $\text{conv } X$ is compact). So d_p is the least number of curve points needed to represent p . (iii) $|z_m| \leq 1$ on K .

Theorem 1. *Let $k \geq 2$ and $B_k = \mathcal{C}_{(1,3,\dots,2k-1)} \subset \mathbb{R}^{2k}$ (the Barvinok–Novik orbitope [3]). Then $\mathfrak{c}(B_k) = 2k - 1$. The value $2k - 1$ is attained at every point of the relative interior of each $(2k - 2)$ -simplex face $B_k \cap \{z_{2k-1} = e^{i\varphi}\}$, and at all points of B_k near such a point (including interior points).*

Theorem 2. *Let $1 \leq a < b$ be coprime integers. Then $\mathfrak{c}(\mathcal{C}_{(a,b)}) = 3$. Consequently, every four-dimensional $SO(2)$ -orbitope has Carathéodory number 3.*

Theorem 3. *Let $d \geq 2$ and $A = (1, 2, \dots, d-1, 2d-1)$. Then $\mathfrak{c}(\mathcal{C}_A) = 2d-1$. The value $2d-1$ is attained on the relative interiors of the $(2d-2)$ -simplex faces $\mathcal{C}_A \cap \{z_{2d-1} = e^{i\varphi}\}$ and near them.*

For $d = 2$, Theorem 3 is the case $B_2 = \mathcal{C}_{(1,3)}$ of Theorems 1 and 2. For $d \geq 3$ it gives, besides B_k , a second family of unbounded dimension on which the Carathéodory number is exactly one below Fenchel's bound. Section 6 also settles, among the sets satisfying condition (R) of Proposition 13 (which gives a simplex face at the top frequency): all four triples with $a_3 = 5$ (Proposition 16), all eight quadruples with $a_4 = 7$ (Proposition 17; partly computer-assisted), and all sixteen quintuples with $a_5 = 9$ (Proposition 18; computer-assisted). In all these cases the value is $2d-1$.

For the consequence (cf. [11, Example 2.1, Lemma 5.1]), let $SO(2)$ act linearly on V and $v \in V$. Decompose $V = V_0 \oplus \bigoplus_{m \geq 1} V_m$ into isotypic components, where rotation by t acts trivially on V_0 and as e^{imt} on V_m for a complex structure J_m . Write $v = \sum_m v_m$. The orbit is $t \mapsto v_0 + \sum_{m \geq 1} (\cos(mt)v_m + \sin(mt)J_m v_m)$. With $A = \{m \geq 1 : v_m \neq 0\}$, the real-affine map $(w_m)_{m \in A} \mapsto v_0 + \sum_{m \in A} (\operatorname{Re} w_m v_m + \operatorname{Im} w_m J_m v_m)$ is injective (since $v_m, J_m v_m$ are independent and the V_m are independent), and it maps $U_A(t)$ to the orbit point. So the orbitope is affinely isomorphic to $\mathcal{C}_A$ and has dimension $2|A|$. Dimension 4 forces $A = \{a, b\}$ with $a < b$. Finally $\mathcal{C}_{(a,b)} = \mathcal{C}_{(a/g, b/g)}$ as sets, where $g = \gcd(a, b)$, and the Carathéodory number is an affine invariant.

Context. Fenchel's theorem [10] gives $\mathfrak{c}(K) \leq \dim K$ because X is connected (see [11, §2.1]). Counting dimensions gives the lower bound $\mathfrak{c}(\mathcal{C}_A) \geq d+1$, since m curve points with weights form a $(2m-1)$ -dimensional family (cf. [11, Prop. 2.3]). The known exact value is $\mathfrak{c}(\mathcal{C}_{(1,\dots,d)}) = d+1$ for the universal orbitope, from the Carathéodory–Toeplitz theorem [5, 11]; the case $d = 2$ is $\mathfrak{c}(\mathcal{C}_{(1,2)}) = 3$ [11, Example 1.1]. For B_k the lower bound $2k-1$ is elementary (Corollary 10). It also follows from real-rank results, see Remark 20. So the new content of Theorem 1 is the upper bound. Before this note the best general upper bound was Fenchel's $2k$. For $\mathcal{C}_{(a,b)}$ with $(a,b) \neq (1,2)$ the known bounds were $3 \leq \mathfrak{c} \leq 4$. Theorem 1 also shows that the secant lower bound of [11, Prop. 2.3], about $k+1$, is not tight for B_k when $k \geq 3$. This bears on [11, Question 7].

2. CHORDS OF THE UNIT DISK

Fix $\zeta \in \mathbb{C}$ with $|\zeta| < 1$ and put $P := 1 - |\zeta|^2$. For $|v| = 1$, the line through v and ζ meets the unit circle in exactly one further point v' . We call v the *start* and v' the *exit* of the chord, and define $\theta \in (0, 1)$ by $\zeta = (1 - \theta)v + \theta v'$. We write $\theta = \theta_\zeta^{\text{st}}(v)$ when the chord is given by its start, and $\theta = \theta_\zeta^{\text{ex}}(v')$ when it is given by its exit.

Lemma 4. $\theta_\zeta^{\text{st}}(v) = \frac{|v - \zeta|^2}{|v - \zeta|^2 + P}$ and $\theta_\zeta^{\text{ex}}(w) = \frac{P}{P + |w - \zeta|^2}$. In particular θ_ζ^{st} is continuous, and $\theta_\zeta^{\text{ex}}(w) + \theta_\zeta^{\text{ex}}(-w) \leq 1$ for every $|w| = 1$.

Proof. Let $\mathbf{a} = |v - \zeta|$ and $\mathbf{b} = |v' - \zeta|$. By the intersecting chords theorem, $\mathbf{a}\mathbf{b} = P$, and $\theta = \mathbf{a}/(\mathbf{a} + \mathbf{b})$. Substituting $\mathbf{b} = P/\mathbf{a}$, respectively $\mathbf{a} = P/\mathbf{b}$, gives the two formulas. For the inequality write $\mathbf{b}_\pm = |\pm w - \zeta|$. Clearing denominators, $\frac{P}{P + \mathbf{b}_+^2} + \frac{P}{P + \mathbf{b}_-^2} \leq 1$ is equivalent to $P^2 \leq \mathbf{b}_+^2 \mathbf{b}_-^2$. This holds because $\mathbf{b}_+ \mathbf{b}_- = |w^2 - \zeta^2| \geq |w|^2 - |\zeta|^2 = P$. $\square$

Lemma 5. *Let $n \geq 2$, let $v_0, \dots, v_{n-1}$ be the vertices of a regular n -gon inscribed in the unit circle, $\xi \in \mathbb{C}$ and $\theta \in (0, 1)$. If $|\xi - (1 - \theta)v_l| < \theta$ for all l , then $\theta > 1/2$.*

Proof. Since $\sum_l v_l = 0$ and $|v_l| = 1$, we have $\frac{1}{n} \sum_l |\xi - (1 - \theta)v_l|^2 = |\xi|^2 + (1 - \theta)^2$. Hence $\theta^2 > (1 - \theta)^2$. $\square$

3. RAYS FROM CURVE POINTS

Let $K = \mathcal{C}_A$ with $\gcd(A) = 1$ and fix $x \in \text{int } K$. For $s \in S$ let $r_s(\rho) = U(s) + \rho(x - U(s))$ and $\rho^*(s) = \max\{\rho \geq 0 : r_s(\rho) \in K\}$. Since x is interior, $\rho^* > 1$; since $x \neq U(s)$ and K is bounded, $\rho^* < \infty$. The point $y_s := r_s(\rho^*(s))$ lies in ∂K , and

$$(1) \quad x = (1 - \theta_s)U(s) + \theta_s y_s, \quad \theta_s = 1/\rho^*(s) \in (0, 1), \quad \text{hence} \quad d_x \leq 1 + d_{y_s}.$$

For $m \in A$, the interior point x has $|z_m(x)| < 1$. Otherwise $z_m(x) = e^{imt_0}$, and by strict convexity of the disk every representation of x uses only points with $e^{ims} = e^{imt_0}$; then the functional $\text{Re}(e^{-imt_0} z_m) \leq 1$ exposes a proper face containing x . Along the ray, $z_m(r_s(\rho)) = e^{ims} + \rho(z_m(x) - e^{ims})$ is unimodular exactly for $\rho = 0$ and $\rho = 1/\theta^m(s)$, where

$$\theta^m(s) := \theta_{z_m(x)}^{\text{st}}(e^{ims}),$$

and $|z_m(r_s(\rho))| > 1$ for $\rho > 1/\theta^m(s)$. Since $|z_m| \leq 1$ on K , we get $\rho^*(s) \leq 1/\theta^m(s)$. Moreover, $|z_m(y_s)| = 1$ if and only if $\rho^*(s) = 1/\theta^m(s)$, and in that case $z_m(y_s)$ is the exit of the chord starting at e^{ims} .

Lemma 6 (fiber lemma). *Let $m, a \in A$ with $m \geq 2$ and $\gcd(a, m) = 1$, put $\zeta = z_m(x)$, and fix $|v| = 1$, $v = e^{i\vartheta}$. Let $s_l = (\vartheta + 2\pi l)/m$ for $l \in \mathbb{Z}/m$. If $|z_m(y_{s_l})| = 1$ and $|z_a(y_{s_l})| < 1$ for every l , then $\theta_\zeta^{\text{st}}(v) > 1/2$.*

Proof. Since $e^{ims_l} = v$ for all l , we have $\theta^m(s_l) = \theta := \theta_\zeta^{\text{st}}(v)$. By hypothesis $\rho^*(s_l) = 1/\theta$, so $\theta_{s_l} = \theta$, and by (1), $z_a(y_{s_l}) = (\xi - (1 - \theta)e^{ias_l})/\theta$ with $\xi = z_a(x)$. Now $e^{ias_l} = e^{ia\vartheta/m} e^{2\pi i al/m}$, and al runs over $\mathbb{Z}/m$ as l does. So these are the vertices of a regular m -gon inscribed in the unit circle. The hypothesis $|z_a(y_{s_l})| < 1$ reads $|\xi - (1 - \theta)e^{ias_l}| < \theta$, and Lemma 5 gives $\theta > 1/2$. $\square$

Corollary 7. *In the setting of Lemma 6, the hypothesis cannot hold for every unimodular v .*

Proof. Otherwise $\theta_\zeta^{\text{st}}(v) > 1/2$ for every start v . Every unimodular w is the exit of exactly one chord, so $\theta_\zeta^{\text{ex}}(w) > 1/2$ for all w . This contradicts $\theta_\zeta^{\text{ex}}(w) + \theta_\zeta^{\text{ex}}(-w) \leq 1$ (Lemma 4). $\square$

4. THE BARVINOK–NOVIK ORBITOPE: PROOF OF THEOREM 1

Let $A = (1, 3, \dots, N)$ with $N = 2k - 1 \geq 3$, $K = B_k$, $z := z_N$, and $M' := \{1, 3, \dots, N - 2\}$. A linear functional ℓ gives the real trigonometric polynomial $g_\ell(t) = \ell(U(t))$, with frequencies in $\{\pm 1, \pm 3, \dots, \pm N\}$, and $g_\ell(t + \pi) = -g_\ell(t)$. The map $\ell \mapsto g_\ell$ is injective.

Lemma 8. *A real trigonometric polynomial $g \not\equiv 0$ of degree $\leq n$ has at most $2n$ zeros on S counted with multiplicity. If $g \geq 0$ its zeros have even multiplicity.*

Proof. $g(t) = e^{-int} P(e^{it})$ with P a nonzero polynomial of degree $\leq 2n$. Orders of vanishing match root multiplicities. A zero of odd order of a nonnegative function would be a sign change. $\square$

Lemma 9. *Let $\ell \neq 0$, $c = \max_K \ell$, $Z = \{t : g_\ell(t) = c\}$. Then $c > 0$ and $|Z| \leq N$. If $|Z| = N$, then $Z = t_0 + \frac{2\pi}{N}\mathbb{Z}$ for some t_0 , and $\ell = c \text{Re}(e^{-iNt_0} z)$.*

Proof. Write $g = g_\ell$. Then $g \not\equiv 0$ has no constant term, and $\min g = -\max g = -c$ by oddness, so $c > 0$. Apply Lemma 8 to $c - g \geq 0$: $|Z| \leq N$. Let $Z = \{t_1, \dots, t_N\}$ and $G = c^2 - g^2 \geq 0$, of degree $\leq 2N$. Then G vanishes on the $2N$ distinct points $Z \cup (Z + \pi)$ (where $g = \pm c$), and $G \not\equiv 0$, since otherwise $g \equiv \pm c$, which contradicts $\int g = 0$. Each of these $2N$ distinct zeros has even multiplicity because $G \geq 0$, so G has at least $4N$ zeros counted with multiplicity. Lemma 8 allows at most $4N$. Hence each zero is exactly double, there are no other zeros, and $w^{2N}G$ is a polynomial of degree $4N$ with double roots exactly at $\pm e^{it_i}$. The same holds for $w^{2N}S_0^2$, where $S_0 = \prod_i \sin(t - t_i)$ and $w^N S_0 = (2i)^{-N} \prod_i (w^2 e^{-it_i} - e^{it_i})$. Hence $G = CS_0^2$ for a constant C . Here $C > 0$ because G and S_0^2 are nonnegative and neither vanishes identically. So $g^2 + h^2 = c^2$ for the real trigonometric

polynomial $h = \sqrt{C} S_0$. In $\mathbb{C}[w, w^{-1}]$ ($w = e^{it}$) this reads $(g + ih)(g - ih) = c^2$. The units are the monomials, so $g + ih = \kappa w^M$ for some $\kappa \neq 0$, and $2g = \kappa w^M + (c^2/\kappa)w^{-M}$. Moreover $M \neq 0$, since g is not constant. As g is real, $2g = 2\bar{g} = \bar{\kappa}w^{-M} + (c^2/\bar{\kappa})w^M$ on $|w| = 1$. Comparing the coefficients of w^M gives $\kappa = c^2/\bar{\kappa}$, i.e. $|\kappa| = c$, so $g = c \cos(Mt + \varphi)$. The frequencies of g are odd and at most N , and $\{g = c\}$ has $|M|$ points, so $|M| = N$. Thus $g = c \cos(N(t - t_0))$ and $Z = t_0 + \frac{2\pi}{N}\mathbb{Z}$. Finally ℓ and $c \operatorname{Re}(e^{-iNt_0}z)$ agree on X , which spans $\mathbb{R}^{2k}$. $\square$

For $t_0 \in \mathbb{R}$ let $\tau_j = t_0 + 2\pi j/N$ and $F_{t_0} = \operatorname{conv}\{U(\tau_j) : j \in \mathbb{Z}/N\}$.

Corollary 10. (a) $K \cap \{z = e^{iNt_0}\} = F_{t_0}$ is an exposed face and an $(N-1)$ -simplex. (b) If $y \in \partial K$, then $d_y \leq N$. If moreover $|z(y)| < 1$, then $d_y \leq N-1$.

Proof. (a) As in §3, every representation of a point with $z = e^{iNt_0}$ uses only the points $U(\tau_j)$. Conversely $F_{t_0} \subset \{z = e^{iNt_0}\}$, and $\operatorname{Re}(e^{-iNt_0}z) \leq 1$ exposes it. For affine independence, let $\sum c_j = 0$ and $\sum c_j U(\tau_j) = 0$ with $c_j \in \mathbb{R}$. Then $\sum_j c_j \omega^{mj} = 0$, $\omega = e^{2\pi i/N}$, for $m \in \{0\} \cup M' \cup (-M')$. Since $-M' \equiv \{2, 4, \dots, N-1\} \pmod{N}$, this is a complete residue system, so the discrete Fourier transform of (c_j) vanishes and $c = 0$. (b) Take a supporting functional ℓ at y . Every representation of y uses only points $U(t)$ with $t \in Z$, and $|Z| \leq N$. If $|Z| = N$, then $\operatorname{Re}(e^{-iNt_0}z(y)) = 1$ by Lemma 9, so $|z(y)| = 1$. $\square$

Proof of Theorem 1. Lower bound. Let p be in the relative interior of some F_{t_0} , for instance the barycenter $b = \frac{1}{N} \sum_j U(2\pi j/N)$ of F_0 . Every representation of p uses only vertices of the simplex F_{t_0} (Corollary 10(a)), and the barycentric coordinates of p are all positive. So $d_p = N$. If $p_n \rightarrow p$ with $d_{p_n} \leq N-1$, a compactness argument (convergent subsequences of the $N-1$ points and weights) represents p with $N-1$ points, which is impossible. So $d = N$ on a neighbourhood of p in K .

Upper bound. Boundary points have $d_y \leq N$ by Corollary 10(b). Let $x \in \operatorname{int} K$ and suppose $d_x > N$. By (1), $d_{y_s} \geq N$ for every s . By Corollary 10, $|z(y_s)| = 1$ and y_s lies in a simplex F_t . Since $d_{y_s} = N$, all its barycentric coordinates are positive. So $z_1(y_s)$ is a convex combination with positive weights of the $N \geq 3$ distinct unimodular numbers $e^{i\tau_j}$, and $|z_1(y_s)| < 1$. Thus the hypothesis of Lemma 6 holds for $m = N$, $a = 1$ and every unimodular v , contradicting Corollary 7. $\square$

5. FOUR-DIMENSIONAL ORBITOPES: PROOF OF THEOREM 2

Let $1 \leq a < b$ be coprime, $K = \mathcal{C}_{(a,b)}$, $U(t) = (e^{iat}, e^{ibt})$. The map $t \mapsto (at, bt) \in (\mathbb{R}/2\pi\mathbb{Z})^2$ is injective. Indeed, if $a(t - t') = 2\pi\mu$ and $b(t - t') = 2\pi\nu$ with $\mu, \nu \in \mathbb{Z}$, then $b\mu = a\nu$, so $a \mid \mu$ and $t - t' \in 2\pi\mathbb{Z}$.

Lemma 11 (mixed functionals). *Let $g(t) = \operatorname{Re}(\alpha e^{iat} + \beta e^{ibt})$ with $\alpha \neq 0 \neq \beta$, and $c = \max g$. Then $\{t \in S : g(t) = c\}$ has at most two elements.*

Proof. At a point t with $g(t) = c$ write $\alpha e^{iat} = X_1 + iY_1$ and $\beta e^{ibt} = X_2 + iY_2$. Then

$$g = X_1 + X_2 = c, \quad g' = -aY_1 - bY_2 = 0, \quad g'' = -a^2X_1 - b^2X_2 \leq 0,$$

and $X_1^2 + Y_1^2 = |\alpha|^2$, $X_2^2 + Y_2^2 = |\beta|^2$. Substituting $X_2 = c - X_1$, $Y_2 = -\frac{a}{b}Y_1$ and $Y_1^2 = |\alpha|^2 - X_1^2$ gives

$$q(X_1) := (b^2 - a^2)X_1^2 - 2b^2cX_1 + b^2c^2 + a^2|\alpha|^2 - b^2|\beta|^2 = 0.$$

The leading coefficient of q is positive and its vertex is at $X_v = b^2c/(b^2 - a^2)$. The condition $g'' \leq 0$ reads $(b^2 - a^2)X_1 \leq b^2c$, i.e. $X_1 \leq X_v$. So X_1 is the smaller root of q (if the two roots coincide, then $X_1 = X_v$), the same value at every maximum point. Then $X_2 = c - X_1$ is determined, $Y_1 = \pm\sqrt{|\alpha|^2 - X_1^2}$, and $Y_2 = -\frac{a}{b}Y_1$. So the pair $(\alpha e^{iat}, \beta e^{ibt})$ takes at most two values, i.e. (at, bt) modulo 2π takes at most two values. By injectivity, t takes at most two values. $\square$

For $t_0 \in \mathbb{R}$ let $Q_{t_0} = \text{conv}\{U(t_0 + 2\pi j/b) : j \in \mathbb{Z}/b\}$ and $P_{t_0} = \text{conv}\{U(t_0 + 2\pi j/a) : j \in \mathbb{Z}/a\}$. The z_a -coordinates of the vertices of Q_{t_0} are $e^{iat_0} e^{2\pi i aj/b}$, so Q_{t_0} is a regular b -gon in the plane $\{z_b = e^{ibt_0}\}$ (a segment if $b = 2$). Likewise P_{t_0} is a regular a -gon in $\{z_a = e^{iat_0}\}$ (a point if $a = 1$, a segment if $a = 2$).

Lemma 12. (a) $K \cap \{z_b = e^{ibt_0}\} = Q_{t_0}$ and $K \cap \{z_a = e^{iat_0}\} = P_{t_0}$. If $|z_a(y)| = |z_b(y)| = 1$ for $y \in K$, then $y \in X$. (b) Every $y \in \partial K$ has $d_y \leq 3$. If $d_y = 3$, then y lies in some Q_{t_0} with $b \geq 3$ and $|z_a(y)| < 1$, or in some P_{t_0} with $a \geq 3$ and $|z_b(y)| < 1$.

Proof. (a) By strict convexity of the disk, a representation of a point with $z_b = e^{ibt_0}$ uses only t with $e^{ibt} = e^{ibt_0}$. If both coordinates are unimodular, all points used share (e^{iat}, e^{ibt}) , hence coincide by injectivity. (b) Let ℓ be a supporting functional at y , $g_\ell = \text{Re}(\alpha e^{iat} + \beta e^{ibt})$. If $\alpha\beta \neq 0$, then y is a combination of the ≤ 2 contact points (Lemma 11). If $\beta = 0$, the contact set is $t_0 + \frac{2\pi}{a}\mathbb{Z}$ and the exposed face is P_{t_0} , a convex polygon in a plane (or a point or segment). So $d_y \leq 3$, and $d_y = 3$ forces $a \geq 3$; moreover $|z_b(y)| < 1$, since otherwise $y \in X$ by (a). The case $\alpha = 0$ is symmetric. $\square$

Proof of Theorem 2. Lower bound. The points with $d_p \leq 2$ form the image of the smooth map $S \times S \times [0, 1] \rightarrow \mathbb{R}^4$, $(s, t, \lambda) \mapsto \lambda U(s) + (1 - \lambda)U(t)$, from a 3-dimensional manifold with boundary. This image has Lebesgue measure zero, while K has nonempty interior. So $\mathfrak{c}(K) \geq 3$.

Upper bound. Boundary points are handled by Lemma 12(b). Let $x \in \text{int } K$ and suppose $d_x \geq 4$ (in fact $d_x \leq 4$ by Fenchel's theorem). By (1), $d_{y_s} \geq 3$ for every s . By Lemma 12, for each s exactly one of $|z_a(y_s)|$, $|z_b(y_s)|$ equals 1. By §3, if $|z_b(y_s)| = 1$ then $\rho^*(s) = 1/\theta^b(s) \leq 1/\theta^a(s)$, with equality impossible since $|z_a(y_s)| < 1$. So $\theta^b(s) > \theta^a(s)$. Symmetrically, $|z_a(y_s)| = 1$ forces $\theta^a(s) > \theta^b(s)$. Thus the continuous function $\theta^a - \theta^b$ (Lemma 4) has no zero on the connected circle S , so it has constant sign.

If $\theta^b > \theta^a$ on S , then $|z_b(y_s)| = 1$ and $|z_a(y_s)| < 1$ for all s . This is the hypothesis of Lemma 6 with $m = b \geq 2$ and the frequency a , for every v , which contradicts Corollary 7. If $\theta^a > \theta^b$ on S , then $|z_a(y_s)| = 1$ and $|z_b(y_s)| < 1$ for all s . By Lemma 12(b) this is already a contradiction if $a \leq 2$. If $a \geq 3$, Lemma 6 with $m = a$ and the frequency b gives the same contradiction as before. Hence $d_x \leq 3$. $\square$

6. A SIMPLEX FACE AT THE TOP FREQUENCY: PROOF OF THEOREM 3

The proof of Theorem 1 uses only two properties of A . We isolate them.

Proposition 13. Let $A = (a_1 < \dots < a_{d-1} < N)$ with $\gcd(A) = 1$ and $N \geq 3$, and put $A' = \{a_1, \dots, a_{d-1}\}$. Assume:

- (R) $\{0\} \cup A' \cup (-A')$ is a complete residue system mod N (so $N = 2d - 1$);
- (F) every supporting functional ℓ of $\mathcal{C}_A$ whose maximum is attained at N points of S is a positive multiple of $\text{Re}(e^{-iNt_0} z_N)$ for some t_0 .

Then $\mathfrak{c}(\mathcal{C}_A) = N = 2d - 1$. The value N is attained on the relative interiors of the $(N - 1)$ -simplex faces $\mathcal{C}_A \cap \{z_N = e^{iNt_0}\}$ and near them.

Proof. Let $K = \mathcal{C}_A$ and $z = z_N$. For a supporting functional ℓ , the function $c - \ell \circ U \geq 0$ is a nonzero trigonometric polynomial of degree $\leq N$, so it has at most N zeros (Lemma 8). By (F), the faces with N contact points are the sets $F_{t_0} = K \cap \{z = e^{iNt_0}\} = \text{conv}\{U(t_0 + 2\pi j/N)\}$ (strict convexity of the disk). By (R), the argument of Corollary 10(a) shows that F_{t_0} is an $(N - 1)$ -simplex. The proof of Corollary 10(b) applies unchanged: boundary points have $d_y \leq N$, and $d_y \leq N - 1$ if $|z(y)| < 1$. The lower bound is proved as in Theorem 1. For the upper bound, (R) gives some $a \in A'$ with $a \equiv \pm 1 \pmod{N}$. Then $\gcd(a, N) = 1$, so the numbers $e^{ia\tau_j}$ ($\tau_j = t_0 + 2\pi j/N$) are $N \geq 3$ distinct unimodular numbers. The proof of Theorem 1 then goes through with the fiber lemma for $m = N$ and the auxiliary frequency a . $\square$

For B_k , (R) and (F) are Corollary 10(a) and Lemma 9; so Theorem 1 is a special case. Condition (F) for other A comes from the next lemma.

Lemma 14 (equally spaced contact points). *Let $N \geq 2$, $1 \leq r \leq N - 1$ with $r \geq \frac{N-1}{2}$, and let $f \geq 0$, $f \not\equiv 0$, be a real trigonometric polynomial of degree $\leq N$ whose Fourier coefficients $\hat{f}_k$ vanish for $N - r \leq k \leq N - 1$. If f has N distinct zeros $t_1, \dots, t_N$ in S , then they are equally spaced, $\{t_j\} = t_0 + \frac{2\pi}{N}\mathbb{Z}$, and $f = C(1 - \cos(N(t - t_0)))$ for some $C > 0$.*

Proof. Each zero has even order (Lemma 8), so these are all the zeros, each double, and $w^N f$ is a polynomial of degree $2N$ with double roots at $w_j = e^{it_j}$. Let $P(w) = \prod_j (w - w_j) = \sum_{m=0}^N c_m w^m$ ($c_N = 1$). The polynomials $w^N f$ and P^2 have degree $2N$ and the same roots, so $w^N f = \kappa P^2$. On $|w| = 1$ we have $|P(w)|^2 = \lambda w^{-N} P(w)^2$ with $\lambda = \prod_j (-\bar{w}_j)$, because $1 - \bar{w}_j w = -\bar{w}_j(w - w_j)$. Hence $f = (\kappa/\lambda)|P|^2 =: C_1|P|^2$, with $C_1 > 0$ because $f \geq 0$ and $f \not\equiv 0$. Since all roots of P are unimodular, P is self-inversive: $w^N \overline{P(1/\bar{w})} = \prod_j (1 - \bar{w}_j w) = \lambda P(w)$, i.e. $\bar{c}_m = \lambda c_{N-m}$ for all m . The coefficient of w^k in $|P|^2 = P \cdot \sum_m \bar{c}_m w^{-m}$ is $\sum_{m=0}^{N-k} c_{m+k} \bar{c}_m$. We show by induction on $j = 1, \dots, r$ that $c_{N-j} = 0$; by self-inversiveness this also gives $\bar{c}_j = \lambda c_{N-j} = 0$. For $k = N - j$ the sum is $c_{N-j} \bar{c}_0 + \sum_{m=1}^{j-1} c_{N-j+m} \bar{c}_m + c_N \bar{c}_j$. The middle terms vanish by induction, and $c_{N-j} \bar{c}_0 + \bar{c}_j = 2\lambda c_{N-j}$. So $\hat{f}_{N-j} = 0$ forces $c_{N-j} = 0$. Since $r \geq \frac{N-1}{2}$, the sets $\{1, \dots, r\}$ and $\{N - r, \dots, N - 1\}$ cover $\{1, \dots, N - 1\}$. Hence $P = w^N + c_0$ with $|c_0| = 1$, and the roots are equally spaced. Writing $c_0 = -e^{iNt_0}$ gives $f = C_1|w^N - e^{iNt_0}|^2 = 2C_1(1 - \cos(N(t - t_0)))$. $\square$

Proof of Theorem 3. Let $N = 2d - 1$. Condition (R) holds because $\{0, \pm 1, \dots, \pm(d - 1)\}$ consists of N consecutive integers. For (F), let ℓ attain its maximum c at N points and put $g = \ell \circ U$ and $f = c - g$. Then $f \geq 0$ has mean $c > 0$. Its coefficients $\hat{f}_k$ vanish for $d \leq k \leq N - 1$, since these frequencies are not in A ; this is the range $N - r \leq k \leq N - 1$ with $r = d - 1 = \frac{N-1}{2}$. By Lemma 14, $g = (c - C) + C \cos(N(t - t_0))$, and since g has no constant term, $C = c$. Thus $\ell = c \operatorname{Re}(e^{-iNt_0} z_N)$. Proposition 13 applies. $\square$

Proposition 15 (an algebraic criterion for (F)). *Let A satisfy (R) with $N = 2d - 1$. Define $Z \subset \{1, \dots, N - 1\}$ as the smallest set with the following property: if $a \in A'$ and for every $1 \leq i \leq a - 1$ at least one of $i, a - i$ lies in Z , then $a \in Z$ and $N - a \in Z$. If $Z = \{1, \dots, N - 1\}$, then (F) holds, and hence $\mathfrak{c}(\mathcal{C}_A) = 2d - 1$.*

Proof. Let ℓ attain its maximum c at N points and $f = c - \ell \circ U$. As in Lemma 14, $w^N f = \kappa P^2$ with $P = \sum_{m=0}^N c_m w^m$ monic, all roots unimodular, $|c_0| = 1$ and $\bar{c}_m = \lambda c_{N-m}$. Also $\hat{f}_k = 0$ for $k \in \{1, \dots, N - 1\} \setminus A' = N - A'$. The coefficient of w^{N-k} in $w^N f$ is $\hat{f}_{-k} = \bar{\hat{f}}_k$, so $[w^a]P^2 = 0$ for all $a \in A'$. That is, $2c_0 c_a + \sum_{i=1}^{a-1} c_i c_{a-i} = 0$. Build Z step by step. Whenever every product $c_i c_{a-i}$ contains a factor already known to vanish, we get $c_a = 0$, and $c_{N-a} = \bar{\lambda} \bar{c}_a = 0$. If $Z = \{1, \dots, N - 1\}$, then $P = w^N + c_0$, the contact points are equally spaced, and (F) follows as in the proof of Theorem 3. $\square$

The criterion requires $1 \in A'$. It holds for B_k (odd a : one of $i, a - i$ is a smaller odd number), for $(1, \dots, d - 1, 2d - 1)$, and for instance for $(1, 2, 4, 7)$. It fails for $(2, 4, 5)$, $(3, 4, 5)$ and $(1, 4, 5, 7)$. For these, and for the four sets with $d = 4$ and $1 \notin A'$, (F) is proved below using that the roots are unimodular (Propositions 16 and 17). A numerical search over root configurations (`numerics/caratheodory_RF_check.py`, output `caratheodory_RF.txt`) covers every A satisfying (R) with $d \leq 5$: 4, 8 and 16 sets for $d = 3, 4, 5$. From 1200–1500 random starts per set, it found no configuration of N distinct unimodular roots with $[w^a]P^2 = 0$ for all $a \in A'$ other than the equally spaced one. Propositions 16, 17 and 18 below turn this into a proof for $d \leq 5$. We expect (R) $\Rightarrow$ (F) in general, which would give $\mathfrak{c}(\mathcal{C}_A) = 2d - 1$ for every A satisfying (R).

Proposition 16. $\mathfrak{c}(\mathcal{C}_{(2,4,5)}) = \mathfrak{c}(\mathcal{C}_{(3,4,5)}) = 5$. Hence $\mathfrak{c}(C_A) = 5$ for each of the four triples $A = (1, 2, 5), (1, 3, 5), (2, 4, 5), (3, 4, 5)$, which are exactly the triples with $a_3 = 5$ satisfying (R).

Proof. For both triples (R) holds: $\{0, \pm 2, \pm 4\}$ and $\{0, \pm 3, \pm 4\}$ are complete mod 5. We check (F). As in Lemma 14, a supporting functional with five contact points gives $f = C_1|P|^2$, where P has degree 5 and unimodular roots, and the coefficients of $|P|^2$ vanish at the frequencies not in A . A rotation multiplies λ by a fifth power of a unimodular number, so we may assume $\lambda = 1$. Then $\bar{c}_m = c_{5-m}$, and $P = w^5 + aw^4 + bw^3 + \bar{b}w^2 + \bar{a}w + 1$ with $a = c_4$, $b = c_3$. The coefficients of $|P|^2$ are

$$s_4 = 2a, \quad s_3 = 2b + a^2, \quad s_2 = 2\bar{b} + 2ab, \quad s_1 = 2\bar{a} + 2a\bar{b} + b^2.$$

$A = (2, 4, 5)$: $s_1 = s_3 = 0$. Then $b = -a^2/2$ and $\bar{a}(2 - |a|^2) + a^4/4 = 0$. Writing $a = \rho e^{i\varphi}$ with $\rho > 0$ gives $\rho^3 e^{5i\varphi} = 4(\rho^2 - 2)$. So $e^{5i\varphi} = \pm 1$, and $\rho \in \{2, 1 + \sqrt{5}\}$ (sign $+$) or $\rho = \sqrt{5} - 1$ (sign $-$). Rotations by $2\pi/5$ preserve $\lambda = 1$ and multiply a by fifth roots of unity, so each branch is one rotation orbit. It has the real representative $a \in \{2, 1 + \sqrt{5}, 1 - \sqrt{5}\}$, $b = -a^2/2$. $A = (3, 4, 5)$: $s_1 = s_2 = 0$. Then $\bar{b} = -ab$. Either $b = 0$, and then $s_1 = 2\bar{a} = 0$; or $|a| = 1$. In the second case write $a = e^{i\psi}$ and $b = \beta e^{i\chi}$ with $\beta > 0$. Then $e^{2i\chi} = -e^{-i\psi}$, so $e^{i\chi} = \varepsilon i e^{-i\psi/2}$ with $\varepsilon = \pm 1$, and $s_1 = e^{-i\psi}(2 - \beta^2 - 2\beta\varepsilon i e^{5i\psi/2})$. So $s_1 = 0$ forces $i e^{5i\psi/2} = \pm 1$, i.e. $e^{5i\psi} = -1$, and $\beta^2 \pm 2\beta - 2 = 0$, i.e. $\beta \in \{\sqrt{3} - 1, \sqrt{3} + 1\}$. For each ψ and each β the sign ε is determined. So each branch consists of five solutions, one rotation orbit. The representative $\psi = \pi$ gives $a = -1$ and b real with $b^2 - 2b - 2 = 0$, i.e. $b = 1 \pm \sqrt{3}$. *Exclusion of the nonzero branches.* For real a, b , P is palindromic of odd degree. Hence $P = (w + 1)w^2h(w + 1/w)$ with $h(u) = u^2 + (a - 1)u + (b - a - 1)$. All roots of P are unimodular exactly when both roots of h are real and lie in $[-2, 2]$. The roots of h for the five representatives are $\frac{-1 \pm \sqrt{21}}{2}$ (one is ≈ -2.79); $\approx 2.16, -4.39$; $\approx 2.45, -0.22$; $1 \pm i3^{1/4}$; and $1 \pm 3^{1/4}$ (one is ≈ 2.32). In each case some root fails. So $a = b = 0$, $P = w^5 + 1$, the contact points are equally spaced, and (F) follows as in the proof of Theorem 3. Proposition 13 applies. The last statement combines this with Theorems 1 and 3. Among the triples with $a_3 = 5$ and $\gcd = 1$, (R) fails exactly for $(1, 4, 5)$ and $(2, 3, 5)$. $\square$

Proposition 17. Condition (F) holds for each of the eight sets $A = (a_1, a_2, a_3, 7)$ satisfying (R), namely $A' = \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 5\}, \{1, 4, 5\}, \{2, 3, 6\}, \{2, 4, 6\}, \{3, 5, 6\}, \{4, 5, 6\}$. Hence $\mathfrak{c}(C_A) = 7$ for each of them. Together with Theorem 2 and Proposition 16, $\mathfrak{c}(C_A) = 2d - 1$ for every A satisfying (R) with $2 \leq d \leq 4$. For three of the eight sets the proof is computer-assisted.

Proof. As in the proof of Proposition 15, a supporting functional with seven contact points gives a monic $P = \sum_{m=0}^7 c_m w^m$ with distinct unimodular roots $\zeta_1, \dots, \zeta_7$, with $\bar{c}_m = \lambda c_{7-m}$, and with $[w^a]P^2 = \sum_{i+j=a} c_i c_j = 0$ for $a \in A'$. A rotation $t \mapsto t + s$ replaces c_m by $e^{-i(7-m)s} c_m$ and λ by $e^{7is} \lambda$. It multiplies each $[w^a]P^2$ by a unimodular factor and preserves the conclusion $P = w^7 + c_0$. So, as in Proposition 16, we may assume $\lambda = 1$, i.e. $c_0 = c_7 = 1$ and $c_{7-m} = \bar{c}_m$. We show $c_1 = c_2 = c_3 = 0$, i.e. $P = w^7 + 1$; then (F) follows as in the proof of Theorem 3, and Proposition 13 applies. We use the power sums $p_k = \sum_j \zeta_j^k$, which satisfy $|p_k| \leq 7$. Newton's identities express them through $e_j = (-1)^j c_{7-j}$; here $e_1 = -\bar{c}_1$, $e_2 = \bar{c}_2$, $e_3 = -\bar{c}_3$, $e_4 = c_3$, and $p_1 = e_1$, $p_2 = e_1 p_1 - 2e_2$, $p_3 = e_1 p_2 - e_2 p_1 + 3e_3$, $p_4 = e_1 p_3 - e_2 p_2 + e_3 p_1 - 4e_4$.

$A' = \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 5\}$. Proposition 15 applies.

$A' = \{1, 4, 5\}$. First $[w^1]P^2 = 2c_1 = 0$. Then $[w^4]P^2 = 2\bar{c}_3 + c_2^2 = 0$ and $[w^5]P^2 = 2\bar{c}_2 + 2c_2 c_3 = 0$, so $c_3 = -\bar{c}_2^2/2$ and $\bar{c}_2(2 - |c_2|^2) = 0$. If $c_2 \neq 0$, then $|c_2|^2 = 2$. Since $e_1 = p_1 = 0$, we get $p_4 = 2e_2^2 - 4e_4 = 4c_2^2$, so $|p_4| = 8 > 7$, a contradiction. Hence $c_2 = c_3 = 0$.

$A' = \{2, 3, 6\}$. The equations $[w^2]P^2 = 2c_2 + c_1^2 = 0$ and $[w^3]P^2 = 2c_3 + 2c_1 c_2 = 0$ give $c_2 = -c_1^2/2$ and $c_3 = c_1^3/2$. Suppose $c_1 = \rho e^{i\alpha}$ with $\rho > 0$. Then $[w^6]P^2 = 2\bar{c}_1 + 2c_1 \bar{c}_2 + 2c_2 \bar{c}_3 + c_3^2 = e^{-i\alpha}(2\rho - \rho^3 - \frac{1}{2}\rho^5 + \frac{1}{4}\rho^6 e^{7i\alpha})$. So $\varepsilon := e^{7i\alpha} = \pm 1$ and $g_\varepsilon(\rho) := 2 - \rho^2 - \frac{1}{2}\rho^4 + \frac{\varepsilon}{4}\rho^5 = 0$. With $x = \bar{c}_1$, Newton's identities give $p_3 = -4x^3$ and $p_4 = \frac{11}{2}x^4 - 2\bar{x}^3$. Hence $|p_3| = 4\rho^3$ and $|p_4| = \rho^3|\frac{11}{2}\rho - 2\varepsilon|$.

- By Descartes' rule, g_{-1} has exactly one positive root, and a sign change places it in $(1.04, 1.05)$. There $|p_4| = \rho^3(\frac{11}{2}\rho + 2) > 1.04^3 \cdot 7.72 > 8.6$.
- The polynomial g_{+1} has at most two positive roots, and sign changes place them in $(1.24, 1.25)$ and $(2, 3)$. There $|p_3| > 4 \cdot 1.24^3 > 7.6$.

Each case contradicts $|p_k| \leq 7$. Hence $c_1 = 0$, and then $c_2 = c_3 = 0$.

$A' = \{2, 4, 6\}, \{3, 5, 6\}, \{4, 5, 6\}$ (*computer-assisted*). Put $u_j = c_j$ and $v_j = \bar{c}_j$ ($j = 1, 2, 3$), regarded as independent unknowns. The three equations $[w^a]P^2 = 0$ ($a \in A'$) and their complex conjugates form a system of six quadratic equations over $\mathbb{Q}$ in $(u_1, u_2, u_3, v_1, v_2, v_3)$. A lexicographic Gröbner basis of this system, computed exactly, is in shape position. It consists of a univariate polynomial $h(v_3)$ and of the polynomials $\gamma_x x - f_x(v_3)$ for $x \in \{u_1, u_2, u_3, v_1, v_2\}$, with rational $\gamma_x \neq 0$. So the complex solutions are exactly the points $(f_x(r)/\gamma_x, r)$ with $h(r) = 0$. Here $\deg h = 64, 36, 36$ respectively, and h is squarefree. The root $r = 0$ gives the trivial solution $c = 0$. The other roots of h were isolated in Arb ball arithmetic, and the coordinates of the corresponding solutions were enclosed in balls. For each of these solutions, the power sums of $w^7 + v_1 w^6 + v_2 w^5 + v_3 w^4 + u_3 w^3 + u_2 w^2 + u_1 w + 1$ (which is P if the solution comes from a functional) satisfy a certified inequality $|p_k| > 7$ for some $k \leq 5$. Hence no nontrivial solution comes from a functional, and $c = 0$. The script is `numerics/caratheodory_F_d4.py`, with output `caratheodory_F_d4.txt`. It also rechecks $A' = \{2, 3, 6\}$; there 14 of the 35 nontrivial solutions are certified not to satisfy $u_j = \bar{v}_j$, and the others have $|p_k| > 7$ with $k \leq 4$. The hand proof for $A' = \{1, 4, 5\}$ is confirmed by the splitting method of Proposition 18 (`numerics/caratheodory_F_d4_split_1457.txt`). The sets $\{2, 3, 6\}, \{2, 4, 6\}, \{3, 5, 6\}, \{4, 5, 6\}$ were rechecked with the Singular pipeline used there (`numerics/caratheodory_F_d4_singular.txt`). $\square$

Proposition 18 (computer-assisted). *Let $A = (a_1, \dots, a_4, 9)$ be one of the sixteen sets satisfying (R). Then condition (F) holds, and hence $\mathfrak{c}(\mathcal{C}_A) = 9$. Consequently $\mathfrak{c}(\mathcal{C}_A) = 2d - 1$ for every A satisfying (R) with $2 \leq d \leq 5$.*

Proof. The set-up is that of Proposition 17 with $N = 9$: $P = w^9 + \sum_{m=1}^8 c_m w^m + 1$ with $c_{9-m} = \bar{c}_m$, unknowns $u_j = c_j$ and $v_j = \bar{c}_j$ ($j \leq 4$) treated as independent, and the ideal $I \subset \mathbb{Q}[u, v]$ generated by the equations $[w^a]P^2 = 0$ ($a \in A'$) and their conjugates. Only zeros with $v = \bar{u}$ come from functionals; call them *real*. For a real zero, $c_j = 0$ iff $u_j = v_j = 0$. Two facts are used.

- The trivial zero $c = 0$ is isolated and simple. Indeed, the linear parts of the eight generators at 0 are $2u_j$ and $2v_j$ in some order, because A' contains exactly one of j and $9 - j$.
- Nine unimodular roots give $|p_k| \leq 9$ for every k .

Exact Gröbner bases and saturations are computed in Singular, and roots are isolated in Arb.

- For eleven sets the ideal I is zero-dimensional, and its lexicographic basis is in shape position. The last coordinate is v_4 , or a linear form $v_4 + \sum r_i x_i$ with small integers r_i . As in Proposition 17, every nontrivial zero is then certified either not to be real, or to have $|p_k| > 9$ for some $k \leq 7$. For three of these sets, $(1, 2, 3, 4, 9)$, $(1, 2, 3, 5, 9)$ and $(1, 3, 5, 7, 9)$, the only zero is $c = 0$, as also follows from Proposition 15.
- For the other five sets the real zeros are split exhaustively, for $j = 1, 2, \dots$, according to whether $c_j = 0$ (add u_j, v_j) or $c_j \neq 0$ (saturate by $u_j v_j$). For $(1, 3, 4, 7, 9)$, $(2, 5, 6, 8, 9)$ and $(3, 5, 7, 8, 9)$ the ideal I is one-dimensional, so the splitting is necessary. For $(2, 4, 6, 8, 9)$ and $(4, 6, 7, 8, 9)$ the ideal is zero-dimensional ($\text{vdim } 256 = 1 + 3 + 252$ and $148 = 1 + 3 + 144$), but no separating coordinate with a lexicographic basis computable in reasonable time was found, so these were split as well. The first split is on c_1 . In the branch $c_1 = 0$ the trivial zero is removed by saturating with the maximal ideal at 0; by (a) this removes exactly that point. In the branch $c_1 \neq 0$ it is removed by the saturation by $u_1 v_1$ itself, since by (a) the origin is an isolated point of $V(I)$ lying in $V(u_1 v_1)$. Every saturation J of an ideal I_0 by f is checked independently: each generator g of J satisfies $f^k g \in I_0$ for some

$k \leq 10$. For the maximal ideal, f runs over the variables. This proves $J \subseteq (I_0 : f^\infty)$, hence $V(J) \supseteq V(I_0) \setminus V(f)$, which is the inclusion the exhaustiveness of the splitting needs. Each zero-dimensional piece is treated as in (i). The positive-dimensional pieces are as follows.

- For $(1, 3, 4, 7, 9)$ there is one piece, on which $|p_6|^2 = p_6(u, v)p_6(v, u)$ has constant normal form $200 > 81$.
- For $(2, 5, 6, 8, 9)$ there is one piece, on which $|p_4|^2 = 196$.
- For $(3, 5, 7, 8, 9)$ there is the piece $c_2 = c_3 = 0$, $|c_1| = 1$, $c_4^2 = -2\bar{c}_1$. A normal form computation gives $p_5 = -\bar{c}_1^5 - 10c_4$ there, so $|p_5| \geq 10|c_4| - |c_1|^5 = 10\sqrt{2} - 1 > 9$.

Hence $P = w^9 + 1$ in all cases, and Proposition 13 applies. The scripts are in `numerics/`:

- certification: `caratheodory_F_general.py` and `caratheodory_F_split.py`;
- power sums: `caratheodory_F_posdim.py`;
- the normal form for the last piece: `caratheodory_F_d5_hand.py`;
- driver `caratheodory_F_d5_all.sh`, with output `caratheodory_F_d5.txt`.

Software: Singular 4.3.2, sympy 1.14.0, python-flint 0.9.0 (Arb). □

7. REMARKS

Remark 19 (What the proofs use). For Theorems 1 and 3 the two inputs are isolated in Proposition 13: a simplex face at the top frequency, (R), and the face condition (F). (F) comes from antipodal symmetry for B_k , and from the self-inversive Lemma 14 otherwise. Besides the face structure, the upper bounds use only one auxiliary coordinate. This is the frequency-1 coordinate for B_k , and the other frequency for $\mathcal{C}_{(a,b)}$. That coordinate is coprime to the frequency whose polygonal faces could trap the rays. The trapping is ruled out by averaging over the regular polygon of starting points (Lemma 5) and by the antipodal chord inequality (Lemma 4). Lemma 11 gives an independent elementary proof of the part of Smilansky's classification of the faces of $\mathcal{C}_{(a,b)}$ [13] that is needed here: exposed faces with three or more vertices are the polygons P_{t_0}, Q_{t_0} .

Remark 20 (Binary forms). Let $d = 2k - 1$ and $\ell_t = \cos t X + \sin t Y$. By [11, §5] there is a linear isomorphism from $\mathbb{R}^{2k}$ onto real binary forms of degree d with $U(t) \mapsto \ell_t^d$. It maps B_k onto $\text{conv}\{\ell_t^d\}$. Since $-\ell^d = (-\ell)^d$ for odd d , this is the unit ball of the norm dual to $f \mapsto \max_t |f(\cos t, \sin t)|$ under the apolar pairing $\langle f, \ell_t^d \rangle = f(\cos t, \sin t)$. This is the symmetric nuclear norm. A representation of a point by m curve points is a real Waring decomposition with m terms and positive weights. (i) Theorem 1 says: every real binary form of odd degree $d \geq 3$ whose nuclear norm is at most 1 is a convex combination of at most d powers ℓ_t^d , and d cannot be lowered. For forms of nuclear norm exactly 1, Corollary 10(b) gives nuclear decompositions with at most d terms. (ii) In particular every real binary form of odd degree d has real Waring rank at most d . This is a known fact [7, Prop. 2.1]. (iii) The barycenter b corresponds to $(1/N) \sum_j \ell_{2\pi j/N}^d = 2^{1-d} \text{Re}((X + iY)^d)$, which has d distinct real roots. Such forms have real rank exactly d ([6, Cor. 1], completing [7]), which gives a second proof of $d_b \geq d$.

Remark 21 (General $\mathcal{C}_A$). For the universal orbitope $\mathfrak{c}(\mathcal{C}_{(1,\dots,d)}) = d+1$. For B_k and for $\mathcal{C}_{(1,\dots,d-1,2d-1)}$ the value is $2d - 1$. In all known cases with $d \geq 2$ Fenchel's bound $2d$ is not attained. *Numerical evidence for $d = 3$* (`numerics/caratheodory_6d.py`). Random interior points, and points near the barycenters of the faces $\{|z_m| = 1\}$, were tested.

- $A = (1, 2, 3), (1, 2, 4), (1, 3, 4), (2, 3, 4), (1, 4, 5), (2, 3, 5)$: every point tested is a combination of 4 curve points.
- $A = (1, 3, 5), (1, 2, 5), (1, 3, 7), (1, 5, 7)$: some points need 5.
- No tested point needs 6.

This raises the question whether $\mathfrak{c}(\mathcal{C}_A) \leq 2d - 1$ for every A with $d \geq 2$; the evidence is limited to small cases. For $N = a_d = 2d - 1$ the method of this note gives the bound $2d - 1$ whenever every face with N contact points is of the form $\{z_N = e^{iNt_0}\}$. If moreover $\{0\} \cup \pm\{a_1, \dots, a_{d-1}\}$

is a complete residue system mod N , it gives the value $2d - 1$. Examples are B_k (by antipodal symmetry) and $(1, \dots, d - 1, 2d - 1)$ (by Lemma 14). Every A satisfying (R) with $2 \leq d \leq 5$ has $\mathfrak{c} = 2d - 1$ (Theorem 2 for $d = 2$, and Propositions 16, 17 and 18). Whether (R) implies (F) for all d remains open.

Remark 22 (Literature). We have not found the values $\mathfrak{c}(B_k) = 2k - 1$ ($k \geq 3$) or $\mathfrak{c}(\mathcal{C}_{(a,b)}) = 3$ ($(a, b) \neq (1, 2)$) in the literature on these orbitopes [11, 3, 4, 14, 13, 12, 2, 1]. In [1] a “Carathéodory subset” is a set whose hull contains the origin, which is a different notion. The lower bound in Theorem 1 also follows from [6] (Remark 20). The same quantity appears as the Carathéodory number of a truncated moment problem in [9, 8]. We are not aware of trigonometric cases with gaps treated there. The upper bounds, the ray-and-chord method, Lemma 14 and Theorem 3 appear to be new.

REFERENCES

- [1] H. Adams, J. Bush, F. Frick, *Metric thickenings, Borsuk–Ulam theorems, and orbitopes*, *Mathematika* 66 (2020) 79–102.
- [2] I. Bárány, R. Karasev, *Notes about the Carathéodory number*, *Discrete Comput. Geom.* 48 (2012) 783–792.
- [3] A. Barvinok, I. Novik, *A centrally symmetric version of the cyclic polytope*, *Discrete Comput. Geom.* 39 (2008) 76–99.
- [4] A. Barvinok, S. J. Lee, I. Novik, *Neighborliness of the symmetric moment curve*, *Mathematika* 59 (2013) 223–249.
- [5] C. Carathéodory, *Über den Variabilitätsbereich der Fourier’schen Konstanten von positiven harmonischen Funktionen*, *Rend. Circ. Mat. Palermo* 32 (1911) 193–217; O. Toeplitz, *Über die Fourier’sche Entwicklung positiver Funktionen*, *Rend. Circ. Mat. Palermo* 32 (1911) 191–192.
- [6] A. Causa, R. Re, *On the maximum rank of a real binary form*, *Ann. Mat. Pura Appl.* 190 (2011) 55–59.
- [7] P. Comon, G. Ottaviani, *On the typical rank of real binary forms*, *Linear Multilinear Algebra* 60 (2012) 657–667.
- [8] P. di Dio, M. Kummer, *The multidimensional truncated moment problem: Carathéodory numbers from Hilbert functions*, *Math. Ann.* 380 (2021) 267–291.
- [9] P. di Dio, K. Schmüdgen, *The multidimensional truncated moment problem: Carathéodory numbers*, *J. Math. Anal. Appl.* 461 (2018) 1606–1638.
- [10] W. Fenchel, *Über Krümmung und Windung geschlossener Raumkurven*, *Math. Ann.* 101 (1929) 238–252.
- [11] R. Sanyal, F. Sottile, B. Sturmfels, *Orbitopes*, *Mathematika* 57 (2011) 275–314.
- [12] R. Sinn, *Algebraic boundaries of $SO(2)$ -orbitopes*, *Discrete Comput. Geom.* 50 (2013) 219–235.
- [13] Z. Smilansky, *Convex hulls of generalized moment curves*, *Israel J. Math.* 52 (1985) 115–128.
- [14] C. Vinzant, *Edges of the Barvinok–Novik orbitope*, *Discrete Comput. Geom.* 46 (2011) 479–487.