hexagon:2611.00382v2

A LOWER BOUND OF 0.8366 FOR LEBESGUE'S UNIVERSAL COVERING PROBLEM

TEJASVI SINGH TOMAR

Abstract. A universal cover is a convex set in the plane that contains a congruent copy of every set of diameter at most 1. Lebesgue asked in 1914 for a universal cover of least area; before this work, the infimum Λ of the areas of universal covers was known to satisfy $0.83474 \le \Lambda \le 0.8441$. Lower bounds come from test sets: Λ is bounded below by the least area of a convex hull of congruent copies of given sets of diameter at most 1. The best earlier lower bounds used the disk, the Reuleaux triangle and the Reuleaux pentagon, but these three bodies are known to admit a placement with hull area below 0.83479, so they cannot give a much better bound. Adding the regular Reuleaux heptagon and nonagon of width 1, we improve the lower bound to $\Lambda \ge 0.8366$. Without the nonagon, the other four bodies already give $\Lambda \ge 0.836$. The proof is a computer-assisted branch and bound over the relative placements of the bodies. Its certificates are checked in interval arithmetic, and separate proofs of both bounds in Lean 4, with their own certificates, are checked entirely by Lean's kernel.

1. Introduction

A planar set has diameter at most 1 if any two of its points are at distance at most 1. A *universal cover* is a convex set in the plane that contains a congruent copy of every planar set of diameter at most 1. In a letter of 1914 to Pál, Lebesgue asked for a universal cover of least area [14]. We write Λ for the infimum of the areas of universal covers. Its value is not known [2], and it is listed as constant 13b in the repository *Optimization constants in mathematics* [16].

Upper bounds come from explicit covers. Pál [14] proved that the regular hexagon circumscribed about a disk of diameter 1 is a universal cover. He then cut off two of its corners, which shows $\Lambda \le 2 - 2/\sqrt{3} < 0.8453$. Sprague [15], Hansen [7], and Baez, Bagdasaryan and Gibbs [1] removed further small pieces. The best upper bound, $\Lambda \le 0.8440935944$, is due to Gibbs [6].

Lower bounds come from test sets. Let $T_1, \dots, T_m$ be sets of diameter at most 1. A universal cover contains a congruent copy of each T_i, and since it is convex, it contains the convex hull of these copies. Hence Λ is at least the infimum $M(T_1, \dots, T_m)$ of the areas of such hulls (Lemma 2.2). Pál [14] took a disk and an equilateral triangle of diameter 1 and proved $\Lambda \ge \pi/8 + \sqrt{3}/4 > 0.8257$.[1] Elekes [4] took a disk and regular polygons whose numbers of sides are powers of 3 and proved $\Lambda \ge 0.8271$. Brass and Sharifi [3] took a disk, an equilateral triangle and a regular pentagon. They reduced the placements of these sets to a five-dimensional space, subdivided it, and proved $\Lambda \ge 0.832$. Xie [17] certified 0.833 for the same three sets with interval arithmetic. Gibbs [5] proposed sets of constant width as test sets, among them the regular Reuleaux 3-, 5-, 7- and 9-gons. Hatchett [8], Mishra [12] and Zeng [18] used the disk with the Reuleaux triangle and pentagon of width 1, which contain the triangle and the pentagon. They proved $\Lambda \ge 0.83474$, $\Lambda \ge 0.8344$ and $\Lambda \ge 0.834$, respectively. Mishra also gave a placement

2020 *Mathematics Subject Classification.* 52A10, 52A38; 65G40, 68V05, 68V20.

Key words and phrases. Lebesgue's universal covering problem, Reuleaux polygons, convex hull, branch and bound, interval arithmetic, computer-assisted proof, formal verification, Lean 4.

[1] The repository [16] credits 0.8257 to Elekes [4]; we follow Mishra [12, Section 1] in crediting it to Pál.

of these three bodies and proved, with a circumscribed polygon, that its hull has area at most 0.834781191, so no lower bound obtained from them exceeds this value [12, Section 3].

Let D be the disk of diameter 1, and let B_n be the regular Reuleaux n-gon of width 1 (Definition 2.1).

Theorem 1.1. *We have*

$$M(D, B_3, B_5, B_7) \geq 0.836 \qquad \text{and} \qquad M(D, B_3, B_5, B_7, B_9) \geq 0.8366.$$

Consequently $\Lambda \geq 0.8366$.

The sets D and B_n are convex, have diameter 1 and have an axis of symmetry. Therefore the bound $\Lambda \geq 0.8366$ holds whether or not congruent copies may be reflected, and whether a universal cover must contain copies of all sets of diameter at most 1 or only of the convex sets of diameter 1. Lemma 2.2 does use the convexity of universal covers, which is part of their definition.

As a test of the method on the five-dimensional space of placements of D, B_3 and B_5, we also prove $M(D, B_3, B_5) \geq 0.8347$ (Proposition 4.2). Its target lies slightly below Hatchett's bound 0.83474, and Section 6 compares the two certificates. In the certificates of Section 4, the bounds for three and for four bodies use the Taylor bound of Lemma 3.5 alone; only the bound for five bodies also combines the areas of several polygons (Lemma 3.8).

Local minimization finds placements of the four and of the five bodies with hull areas of about 0.83649 and 0.83730 (Section 6). Every placement bounds the least hull area from above. These two values are computed in floating point and are not certified; up to floating-point error, lower bounds from these bodies cannot go beyond them.

The method. We fix the disk and the rotation of the Reuleaux triangle; a placement of the bodies is then a point p of $\mathbb{R}^5$, $\mathbb{R}^8$ or $\mathbb{R}^{11}$. Let $A(p)$ be the area of the convex hull of the placed bodies, and let τ be the target, the bound to be proved. If the centre of a Reuleaux polygon is more than about 0.2 from the centre of the disk, a safe rather than a sharp distance, the hull of these two bodies already has area larger than τ. The angles can be restricted by the rotational symmetries of the bodies and by the reflection of the whole placement in a line through the centre of the disk parallel to an axis of symmetry of the Reuleaux triangle. So it suffices to show $A > \tau$ on a box X of placements (Section 2), and we do this by a branch and bound over subboxes of X. Bounds for A on a box that use no derivatives lose an amount proportional to the width of the box even where A hardly varies [12, 17], and the first-order bounds of [8, 18] bound the second-order remainder by absolute values of second derivatives. Near a minimizing placement, where A exceeds the target by little, both need very small boxes. Mishra found the four bodies D, B_3, B_5, B_7 out of reach for his method (Section 6).

On a box of placements we replace the hull by a polygon inside it, as in Figure 1. For each box, the vertices of the polygon are computed for the placement c at the centre of the box, as support points of the hull in many directions (Section 4.2). Once chosen, each vertex moves with its body. If, on the whole box, the vertices stay in strict angular order around a point z of the disk chosen for the box, then the area F of the polygon through them, in this order, is at most A (Lemma 3.3). Since each vertex moves rigidly with its body, F is a polynomial in the translations and in the sines and cosines of the angles. On the box we bound F from below through its value and gradient at c and a certified lower bound for the smallest eigenvalue of its Hessian, together with a bound for how much the Hessian varies over the box. Near placements where the combinatorial type of the hull changes, that is, where the corners and arcs that form its boundary change, the certificate for the five bodies bounds instead a convex combination of the areas of several such polygons, weighted so that their gradients at c nearly cancel.

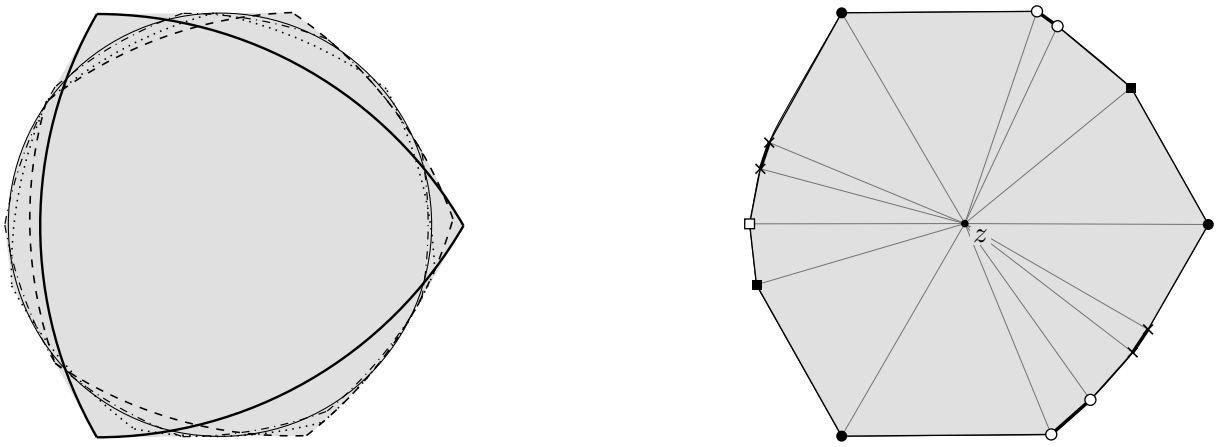

FIGURE 1. Left: the disk D (thin) and the Reuleaux polygons B_3 (solid), B_5 (dashed), B_7 (dotted) and B_9 (dash-dotted) at the placement of Section 6, found by local minimization; their convex hull, shaded, has area about 0.83730. Right: a polygon inside this hull, of the kind used in Section 3 (a witness fan), with z the centre of the disk. Its vertices, the witnesses, are the 14 distinct support points of the hull in 48 equally spaced directions; a corner is the support point for many directions. They lie on D ($\times$), B_3 ($\bullet$), B_5 ($\circ$), B_7 ($\blacksquare$) and B_9 ($\square$). A block of consecutive witnesses on one body is a run, and thick edges join its witnesses. The shaded polygon has area $F \approx 0.83564$, about 0.0017 less than the hull, so this coarse fan only illustrates the construction; the fans of the certificates use 256 or 1024 directions and further support points (Section 4.2).

Outline. Section 2 reduces the problem to a box of placements, and Section 3 proves the bounds on boxes. Section 4 describes the certificates and their checks. A checker that shares no code with the search program verifies all three certificates in ball arithmetic, a form of interval arithmetic, with the Arb library [9]; it relies on the lemmas of Sections 2 and 3. Section 5 describes separate proofs of the bounds of Theorem 1.1 and Proposition 4.2 in Lean 4, with their own bound on boxes and their own certificates, and Lean's kernel checks these proofs. Section 6 discusses how far lower bounds from these test sets can go.

2. Reduction to a box of placements

We first fix notation. For $a, b \in \mathbb{R}^2$ put $\det(a,b) = a_1 b_2 - a_2 b_1$. Let $u(\varphi) = (\cos\varphi, \sin\varphi)$, let R_φ be the rotation of $\mathbb{R}^2$ about the origin by the angle φ, and let $J = R_{\pi/2}$. Rotations preserve det, and J commutes with every R_φ. Let $D(y,r)$ be the closed disk with centre y and radius r, and let $D = D(0,1/2)$. We write area for the Lebesgue measure on $\mathbb{R}^2$, conv for the convex hull, and $|\cdot|$ for the Euclidean norm.

Definition 2.1. For odd $n \geq 3$ let $R_n = 1/(2\cos(\pi/(2n)))$, let $V_{n,l} = R_n\, u(2\pi l/n)$ for $l = 0, \ldots, n-1$, and let $B_n = \bigcap_{l=0}^{n-1} D(V_{n,l}, 1)$.

The points $V_{n,l}$ are the vertices of a regular n-gon. The largest distance between two of them is $|V_{n,0} - V_{n,(n-1)/2}| = 2R_n \cos(\pi/(2n)) = 1$. Hence B_n is the regular Reuleaux n-gon of width 1. It has constant width 1, and hence diameter 1 [10]. We have $0.50 < R_9 < R_7 < R_5 < R_3 < 0.58$.

We fix odd integers $n_1, \ldots, n_k \geq 3$ with $k \geq 2$. Theorem 1.1 uses $(n_1, n_2, n_3) = (3,5,7)$ and $(n_1, \ldots, n_4) = (3,5,7,9)$, and Proposition 4.2 uses $(n_1, n_2) = (3,5)$. A *placement* is a vector

$$p = (t_1, \rho_2, t_2, \ldots, \rho_k, t_k) \in \mathbb{R}^d, \qquad d = 3k - 1,$$

with $t_i \in \mathbb{R}^2$ and $\rho_i \in \mathbb{R}$. We put $\rho_1 = 0$, and for the disk we put $\rho_0 = 0$ and $t_0 = 0$. Let $B^{(0)} = D$ and $B^{(i)} = B_{n_i}$ for $1 \le i \le k$. In the placement p, body i occupies $P_i(p) = R_{\rho_i} B^{(i)} + t_i$. Let

$$K(p) = \operatorname{conv}\big(P_0(p) \cup P_1(p) \cup \cdots \cup P_k(p)\big) \qquad \text{and} \qquad A(p) = \operatorname{area} K(p).$$

For bounded sets $T_1, \dots, T_m \subset \mathbb{R}^2$ let $M(T_1, \dots, T_m)$ be the infimum of $\operatorname{area}\operatorname{conv}(g_1(T_1) \cup \cdots \cup g_m(T_m))$ over all isometries $g_1, \dots, g_m$ of $\mathbb{R}^2$.

Lemma 2.2 below is the principle behind all the lower bounds above. Its normalization of the placements is that of Brass and Sharifi [3] (see also [12, Lemma 4.3]).

Lemma 2.2. *If $T_1, \dots, T_m$ are planar sets of diameter at most 1, then $\Lambda \ge M(T_1, \dots, T_m)$. Moreover, $M(D, B_{n_1}, \dots, B_{n_k}) = \inf_{p \in \mathbb{R}^d} A(p)$.*

Proof. Let Ω be a universal cover. For each i there is an isometry g_i with $g_i(T_i) \subseteq \Omega$. Since Ω is convex, it contains $\operatorname{conv}\big(\bigcup_i g_i(T_i)\big)$, so $\operatorname{area}\Omega \ge M(T_1, \dots, T_m)$. Taking the infimum over Ω proves the first claim.

Every placement is given by isometries, so $M(D, B_{n_1}, \dots, B_{n_k}) \le \inf A$. Conversely, let $g_0, \dots, g_k$ be isometries. The reflection $S(y_1, y_2) = (y_1, -y_2)$ maps D to itself and permutes the points $V_{n,l}$, so it maps each $B^{(i)}$ to itself. If g_i reverses orientation, we replace it by $g_i \circ S$, which preserves orientation and has the same image of $B^{(i)}$. So we may assume that $g_i(y) = R_{\alpha_i} y + b_i$ for all i. The rigid motion $h(y) = R_{-\alpha_1}(y - b_0)$ satisfies $h \circ g_i(y) = R_{\alpha_i - \alpha_1} y + R_{-\alpha_1}(b_i - b_0)$. Since D is invariant under rotations about the origin, h maps $g_i(B^{(i)})$ onto $P_i(p)$ for all i, where p is the placement with $\rho_i = \alpha_i - \alpha_1$ and $t_i = R_{-\alpha_1}(b_i - b_0)$. As h preserves areas, the hull of $g_0(B^{(0)}), \dots, g_k(B^{(k)})$ has area $A(p) \ge \inf A$. □

Lemma 2.3 (Symmetry)**.** *For a placement p let $\bar{p} = (St_1, -\rho_2, St_2, \dots, -\rho_k, St_k)$. Then $A(\bar{p}) = A(p)$. Moreover, A is periodic in ρ_i with period $2\pi/n_i$ for $2 \le i \le k$. Consequently,* $\inf A$ *equals the infimum of A over the placements with $0 \le \rho_2 \le \pi/n_2$ and $0 \le \rho_i \le 2\pi/n_i$ for $3 \le i \le k$, and the reduction does not change $|t_1|, \dots, |t_k|$.*

Proof. The reflection S of the previous proof satisfies $S \circ R_\varphi = R_{-\varphi} \circ S$ and $S(B^{(i)}) = B^{(i)}$. Hence $S(P_i(p)) = R_{-\rho_i} B^{(i)} + St_i = P_i(\bar{p})$ for all i. So $S(K(p)) = K(\bar{p})$, and S preserves area. The rotation $R_{2\pi/n}$ permutes the points $V_{n,l}$, so $R_{2\pi/n} B_n = B_n$, and this gives the periodicity. Given a placement, we first shift ρ_2 into $[0, 2\pi/n_2)$. If then $\rho_2 > \pi/n_2$, we pass to $\bar{p}$ and shift its second coordinate $-\rho_2$ by $2\pi/n_2$ into $(0, \pi/n_2)$. Finally we shift $\rho_3, \dots, \rho_k$ into the intervals $[0, 2\pi/n_i)$. None of these steps changes $|t_1|, \dots, |t_k|$. □

The next lemma gives the root box used by Brass and Sharifi [3]. In this form, with the area f, it is in [12, Lemma 4.4 and Remark 4.6]. Zeng [18, Sections S10.2 and S10.3] and Hatchett [8] prove the same estimate for B_3 and B_5.

Lemma 2.4 (Corner lemma)**.** *For $s \ge 1/2$ and $m \ge 0$ let*

$$f(s) = \frac{\pi - \arccos(1/(2s))}{4} + \frac{\sqrt{s^2 - 1/4}}{2} \qquad \text{and} \qquad g_n(m) = \sqrt{R_n^2 + m^2 + 2R_n m \cos(\pi/n)}.$$

Then f and g_n are increasing, $g_n(m) \ge R_n > 1/2$, and $A(p) \ge f(g_{n_i}(|t_i|))$ for every placement p and every $1 \le i \le k$.

Proof. A direct computation gives $f'(s) = \sqrt{4s^2 - 1}/(4s) > 0$ for $s > 1/2$. Since $\cos(\pi/n) > 0$, g_n is increasing, and $g_n(0) = R_n > 1/2$ because $\cos(\pi/(2n)) < 1$. Fix $i \ge 1$ and write $n = n_i$, $\rho = \rho_i$ and $t = t_i$. The corners $y_l = R_\rho V_{n,l} + t$ lie in $P_i(p)$. If $t = 0$, then $|y_l| = R_n = g_n(0)$.

Otherwise we write $t = |t|\,u(\psi)$. The directions $\rho + 2\pi l/n$ of the vectors $R_\rho V_{n,l}$ are spaced by $2\pi/n$, so for some l the angle β between $u(\rho + 2\pi l/n)$ and $u(\psi)$ satisfies $\beta \le \pi/n$. For this l,

$$|y_l|^2 = R_n^2 + |t|^2 + 2R_n|t|\cos\beta \ge g_n(|t|)^2.$$

So $K(p)$ contains D and a point y with $s = |y| \ge g_n(|t|) > 1/2$. The set $\operatorname{conv}(D \cup \{y\})$ is the union of two pieces. The first is the quadrilateral bounded by the two tangent segments from y to D and the two radii to their points of contact, of area $\frac{1}{2}\sqrt{s^2 - 1/4}$. The second is the sector of D outside this quadrilateral, of angle $2\pi - 2\arccos(1/(2s))$ and area $(\pi - \arccos(1/(2s)))/4$. Hence $A(p) \ge f(s) \ge f(g_n(|t|))$. □

Corollary 2.5. *Let $\tau > 0$ and $w_1, \dots, w_k > 0$ with $f(g_{n_i}(w_i)) > \tau$ for all i. Let $X \subset \mathbb{R}^d$ be a box that contains every placement with $t_i \in [-w_i, w_i]^2$ for $1 \le i \le k$, $\rho_2 \in [0, \pi/n_2]$ and $\rho_i \in [0, 2\pi/n_i]$ for $3 \le i \le k$. If $A(p) \ge \tau$ for all $p \in X$, then $M(D, B_{n_1}, \dots, B_{n_k}) \ge \tau$, and hence $\Lambda \ge \tau$.*

Proof. Let p be a placement. By Lemma 2.3 there is a placement p' with $A(p') = A(p)$, with rotations in the stated ranges, and with $|t_i'| = |t_i|$ for all i. If $t_i' \in [-w_i, w_i]^2$ for all i, then $p' \in X$ and $A(p) \ge \tau$. Otherwise $|t_i'| > w_i$ for some i, and Lemma 2.4 gives $A(p) \ge f(g_{n_i}(|t_i'|)) \ge f(g_{n_i}(w_i)) > \tau$. Hence $\inf A \ge \tau$, and Lemma 2.2 gives the claim. □

3. The box bound

In this section we bound A from below on a box of placements. A *box* is a set $B = \prod_{a=1}^{d}[c_a - h_a, c_a + h_a]$ with centre c and half-widths $h_a \ge 0$. The *angle* from a nonzero vector v to a nonzero vector v' with $\det(v, v') > 0$ is the number $\theta \in (0, \pi)$ with $v'/|v'| = R_\theta(v/|v|)$.

Lemma 3.1 (Fan lemma)**.** *Let $K \subset \mathbb{R}^2$ be compact and convex, let $z \in K$, and let $x_1, \dots, x_m \in K$ with $m \ge 3$. Indices are taken modulo m. Suppose that $\det(x_j - z, x_{j+1} - z) > 0$ for all j, and let θ_j be the angle from $x_j - z$ to $x_{j+1} - z$. If $\theta_1 + \cdots + \theta_m = 2\pi$, then*

$$\operatorname{area} K \;\ge\; \frac{1}{2}\sum_{j=1}^{m} \det(x_j - z, x_{j+1} - z) \;=\; \frac{1}{2}\sum_{j=1}^{m} \det(x_j, x_{j+1}).$$

Proof. Write $x_1 - z = r_1 u(\varphi_1)$ with $r_1 > 0$, and put $\varphi_{j+1} = \varphi_j + \theta_j$. Then $x_j - z = r_j u(\varphi_j)$ with $r_j > 0$ for all j, and $\varphi_{m+1} = \varphi_1 + 2\pi$. The triangle $\Delta_j = \operatorname{conv}\{z, x_j, x_{j+1}\}$ lies in K because K is convex, and its area is $\frac{1}{2}\det(x_j - z, x_{j+1} - z)$. Since $\theta_j < \pi$, the interior of Δ_j lies in the open sector $\{z + s\,u(\psi) : s > 0,\ \varphi_j < \psi < \varphi_{j+1}\}$. The intervals $(\varphi_j, \varphi_{j+1})$ are disjoint subintervals of $[\varphi_1, \varphi_1 + 2\pi)$, and u is injective on this interval. Hence the sectors are pairwise disjoint, the triangles have disjoint interiors, and $\operatorname{area} K \ge \sum_j \operatorname{area}\Delta_j$. Finally,

$$\sum_j \det(x_j - z, x_{j+1} - z) = \sum_j \det(x_j, x_{j+1}) + \sum_j \det(z, x_j) - \sum_j \det(z, x_{j+1}),$$

and the last two sums are equal. □

Definition 3.2. A *witness fan* consists of a point $z \in \mathbb{R}^2$ with $|z| < 1/2$ and a cyclic sequence of *witnesses* $(i_1, q_1), \dots, (i_m, q_m)$ with $m \ge 3$, where $i_j \in \{0, \dots, k\}$ and $q_j \in B^{(i_j)}$. At a placement p, witness j is at $x_j(p) = R_{\rho_{i_j}} q_j + t_{i_j}$. The *fan area* is

$$F(p) = \frac{1}{2}\sum_{j=1}^{m} \det(x_j(p), x_{j+1}(p)).$$

Thus $x_j(p) \in P_{i_j}(p) \subseteq K(p)$ and $z \in D \subseteq K(p)$. Each $x_j(p)$ is affine in the coordinates of the t_i and in the numbers $\cos\rho_i$ and $\sin\rho_i$. Hence F is a polynomial in these quantities, and in particular F is smooth.

Lemma 3.3 (Fan bound)**.** *Let B be a box with centre c, and let a witness fan satisfy $\det(x_j(p)-z, x_{j+1}(p)-z)>0$ for all j and all $p\in B$. If the angles from $x_j(c)-z$ to $x_{j+1}(c)-z$ add up to 2π, then $A(p)\ge F(p)$ for all $p\in B$.*

Proof. For $p\in B$ let $\theta_j(p)$ be the angle from $x_j(p)-z$ to $x_{j+1}(p)-z$. It depends continuously on p, because the determinant is positive on B. The sum $\Theta(p)=\sum_j\theta_j(p)$ is an integer multiple of 2π, since rotating the direction of $x_1(p)-z$ successively by $\theta_1(p),\dots,\theta_m(p)$ returns it to itself. As B is connected, Θ is constant on B, so $\Theta(p)=\Theta(c)=2\pi$. We apply Lemma 3.1 to $K(p)$, the point z and the points $x_j(p)$. □

Lemma 3.4 (Run identity)**.** *Let R be a rotation and $a,b,t\in\mathbb{R}^2$. Then $\det(Ra+t,Rb+t)=\det(a,b)+\det(t,R(b-a))$. Consequently, if the witnesses $\alpha,\alpha+1,\dots,\beta$ lie on one body i, then for every placement*

$$\sum_{j=\alpha}^{\beta-1}\det\bigl(x_j(p),x_{j+1}(p)\bigr)=\sum_{j=\alpha}^{\beta-1}\det(q_j,q_{j+1})+\det\bigl(t_i,R_{\rho_i}(q_\beta-q_\alpha)\bigr),$$

and $\det(x_\alpha(p)-z,x_{\alpha+1}(p)-z)=\det(q_\alpha,q_{\alpha+1})+\det\bigl(t_i-z,R_{\rho_i}(q_{\alpha+1}-q_\alpha)\bigr)$.

Proof. We have $\det(Ra,Rb)=\det(a,b)$ and $\det(Ra,t)+\det(t,Rb)=\det(t,Rb-Ra)$. This proves the first identity, and summing it over j gives the second, since the sum telescopes. The third is the first with t replaced by t_i-z. □

We split the cyclic sequence of witnesses into maximal *runs* of consecutive witnesses on the same body; in Figure 1, thick edges join the witnesses of a run. Suppose that the witnesses lie on at least two bodies. Then consecutive runs lie on different bodies, also cyclically. Let run r lie on body ι_r and consist of the witnesses $\alpha_r,\dots,\beta_r$. Lemma 3.4 gives

$$F(p)=\frac12\sum_r\Bigl(C_r+\det\bigl(t_{\iota_r},R_{\rho_{\iota_r}}w_r\bigr)+\det\bigl(x_{\beta_r}(p),x_{\alpha_{r+1}}(p)\bigr)\Bigr),\tag{3.1}$$

where $C_r=\sum_{j=\alpha_r}^{\beta_r-1}\det(q_j,q_{j+1})$ and $w_r=q_{\beta_r}-q_{\alpha_r}$. We call $\frac12\det(t_{\iota_r},R_{\rho_{\iota_r}}w_r)$ a *run term* and $\frac12\det(x_{\beta_r}(p),x_{\alpha_{r+1}}(p))$ a *transition term*. A run term depends on the parameters of one body, and it vanishes for the disk. A transition term depends on the parameters of two different bodies.

Lemma 3.5 (Taylor bound)**.** *Let B be a box with centre c and half-widths h, and let F be twice continuously differentiable near B. Put $g=\nabla F(c)$ and $H=\nabla^2F(c)$. Let $\lambda\le\min(0,\lambda_{\min}(H))$, and let W be a symmetric matrix with $|\partial_a\partial_bF(\xi)-H_{ab}|\le W_{ab}$ for all $\xi\in B$ and all a,b. Put*

$$e=-\frac{\lambda}{2}\sum_a h_a^2+\frac12\sum_{a,b}W_{ab}h_ah_b\qquad\text{and}\qquad L=F(c)-\sum_a|g_a|h_a-e.$$

Then $F(p)\ge F(c)+g\cdot(p-c)-e\ge L$ for all $p\in B$.

Proof. Let $p\in B$ and $v=p-c$, so $|v_a|\le h_a$. Taylor's theorem for $s\mapsto F(c+sv)$ gives a point ξ on the segment from c to p with $F(p)=F(c)+g\cdot v+\frac12v^T\nabla^2F(\xi)v$. Here $v^THv\ge\lambda_{\min}(H)|v|^2\ge\lambda\sum_a h_a^2$, since $\lambda\le0$, and $v^T(\nabla^2F(\xi)-H)v\ge-\sum_{a,b}W_{ab}|v_a||v_b|\ge-\sum_{a,b}W_{ab}h_ah_b$. Hence $\frac12v^T\nabla^2F(\xi)v\ge-e$. Finally, $g\cdot v\ge-\sum_a|g_a|h_a$. □

We now compute the derivatives of the terms of (3.1) and bound their variation on a box B with centre c. For a body $i\ge1$ let r_i be the half-width of B in ρ_i, with $r_1=0$, and let $\delta_i=(h_{i,1}^2+h_{i,2}^2)^{1/2}$, where $h_{i,1}$ and $h_{i,2}$ are the half-widths of B in the two coordinates of t_i. Put $r_0=\delta_0=0$. For a witness (i,q) let $e(i,q)=|q|\,r_i+\delta_i$. For a function ϕ on B and $p\in B$ write $\Delta\phi=\phi(p)-\phi(c)$, and let e_1,e_2 be the standard basis of $\mathbb{R}^2$.

Lemma 3.6 (Derivatives and variation bounds)**.** *Let B be a box with centre c, and let $p \in B$.*

(a) *We have $\|R_{\rho_i(p)} - R_{\rho_i(c)}\| \le r_i$ and $|\Delta t_i| \le \delta_i$. The position x of a witness (i,q) satisfies $|\Delta x| \le e(i,q)$.*

(b) *Let (i,q) and (i',q') be consecutive witnesses with positions x and y, and let $\eta = \det(x-z, y-z)$. If $i = i' = 0$, then $\Delta\eta = 0$. If $i = i' \ge 1$, then $|\Delta\eta| \le |q'-q|(\delta_i(1+r_i)+|t_i(c)-z|\,r_i)$. If $i \ne i'$, then*

$$|\Delta\eta| \le e(i,q)(|y(c)-z| + e(i',q')) + |x(c)-z|\,e(i',q').$$

(c) *Let $G = \frac{1}{2}\det(t_i, R_{\rho_i} w)$ be a run term. If $i = 1$, then G is linear in t_1. If $i \ge 2$, the second derivatives of G that do not vanish identically are $\partial^2 G/\partial\rho_i^2 = -\frac{1}{2}\det(t_i, R_{\rho_i} w)$ and $\partial^2 G/\partial\rho_i\partial t_i = \frac{1}{2} R_{\rho_i} w$, and on B*

$$\Big|\Delta\frac{\partial^2 G}{\partial\rho_i^2}\Big| \le \frac{|w|}{2}(\delta_i(1+r_i) + |t_i(c)|\,r_i), \qquad \Big|\Delta\frac{\partial^2 G}{\partial\rho_i\partial t_{i,a}}\Big| \le \frac{|w|}{2}\,r_i \quad (a = 1,2).$$

(d) *Let $G = \frac{1}{2}\det(x,y)$ be a transition term, where x is the position of a witness (i,q) and y that of a witness (i',q') with $i \ne i'$, and put $e = e(i,q)$ and $e' = e(i',q')$. The second derivatives of G with respect to the coordinates of t_i and $t_{i'}$ are constant. The other second derivatives ϕ of G that do not vanish identically, and bounds for $|\Delta\phi|$ on B, are as follows, where $a, b \in \{1,2\}$:*

$$\phi = \frac{\partial^2 G}{\partial\rho_i\,\partial t_{i',b}} = \frac{1}{2}\det(JR_{\rho_i} q, e_b), \qquad |\Delta\phi| \le \tfrac{1}{2}|q|\,r_i,$$

$$\phi = \frac{\partial^2 G}{\partial t_{i,a}\,\partial\rho_{i'}} = \frac{1}{2}\det(e_a, JR_{\rho_{i'}} q'), \qquad |\Delta\phi| \le \tfrac{1}{2}|q'|\,r_{i'},$$

$$\phi = \frac{\partial^2 G}{\partial\rho_i\,\partial\rho_{i'}} = \frac{1}{2}\det(R_{\rho_i} q, R_{\rho_{i'}} q'), \qquad |\Delta\phi| \le \tfrac{1}{2}|q|\,|q'|\,(r_i + r_{i'}),$$

$$\phi = \frac{\partial^2 G}{\partial\rho_i^2} = -\frac{1}{2}\det(R_{\rho_i} q, y), \qquad |\Delta\phi| \le \tfrac{1}{2}|q|(r_i(|y(c)| + e') + e'),$$

$$\phi = \frac{\partial^2 G}{\partial\rho_{i'}^2} = -\frac{1}{2}\det(x, R_{\rho_{i'}} q'), \qquad |\Delta\phi| \le \tfrac{1}{2}|q'|(r_{i'}(|x(c)| + e) + e).$$

Only derivatives with respect to existing parameters occur: t_i exists for $i \ge 1$ and ρ_i for $i \ge 2$.

Proof. (a) For rotations, $\|R_\varphi - R_{\varphi'}\| = 2|\sin((\varphi-\varphi')/2)| \le |\varphi-\varphi'|$. Hence $|\Delta x| \le \|\Delta R_{\rho_i}\|\,|q| + |\Delta t_i| \le e(i,q)$.

(b) If $i = i' = 0$, then x and y are constant. If $i = i' \ge 1$, Lemma 3.4 gives $\eta = \det(q,q') + \det(t_i - z, R_{\rho_i} w)$ with $w = q' - q$. Writing $R = R_{\rho_i}$ and $R_c = R_{\rho_i(c)}$, we get

$$\Delta\eta = \det(\Delta t_i, R_c w) + \det(t_i(c) - z, (R - R_c)w) + \det(\Delta t_i, (R - R_c)w),$$

and (a) bounds the three terms by $\delta_i|w|$, $|t_i(c) - z|\,r_i|w|$ and $\delta_i r_i|w|$. If $i \ne i'$, then $\Delta\eta = \det(\Delta x, y - z) + \det(x(c) - z, \Delta y)$, and $|y - z| \le |y(c) - z| + e(i',q')$ by (a).

(c) We have $\partial_\varphi R_\varphi = R_\varphi J$ and $J^2 = -I$. Hence $\partial G/\partial\rho_i = \frac{1}{2}\det(t_i, R_{\rho_i} Jw)$, $\partial^2 G/\partial\rho_i^2 = -\frac{1}{2}\det(t_i, R_{\rho_i} w)$, and $\partial^2 G/\partial\rho_i\partial t_{i,a} = \frac{1}{2}\det(e_a, JR_{\rho_i} w) = \frac{1}{2}(R_{\rho_i} w)_a$, while G is linear in t_i. The variation of $\det(t_i, R_{\rho_i} w)$ is bounded as in (b), with $t_i(c)$ in place of $t_i(c) - z$, and $|\Delta(R_{\rho_i} w)_a| \le r_i|w|$ by (a).

(d) The point x depends only on the parameters of body i, and y only on those of body i'. We have $\partial x/\partial t_{i,a} = e_a$, $\partial x/\partial\rho_i = JR_{\rho_i} q$ and $\partial^2 x/\partial\rho_i^2 = -R_{\rho_i} q$, and all other second derivatives of x vanish. The same holds for y. Hence the mixed derivatives are $\frac{1}{2}\det(\partial x, \partial y)$ for one parameter

of each body, the second derivatives in ρ_i and in $\rho_{i'}$ are as stated, and the remaining second derivatives vanish. The derivatives in two coordinates of t_i and $t_{i'}$ are $\frac{1}{2}\det(e_a, e_b)$. Using $\det(Ja, Jb) = \det(a, b)$ and (a), we get $|\det(JR_{\rho_i}q, e_b) - \det(JR_{\rho_{i(c)}}q, e_b)| \le r_i|q|$, the same bound for the second line, and

$$|\Delta\det(R_{\rho_i}q, R_{\rho_{i'}}q')| \le |\det(\Delta(R_{\rho_i}q), R_{\rho_{i'}}q')| + |\det(R_{\rho_{i(c)}}q, \Delta(R_{\rho_{i'}}q'))| \le |q|\,|q'|(r_i + r_{i'}).$$

Finally, $|\Delta\det(R_{\rho_i}q, y)| \le r_i|q|\,|y| + |q|\,|\Delta y| \le |q|(r_i(|y(c)| + e') + e')$, and the last line is symmetric. □

Let W be the symmetric $d \times d$ matrix obtained by adding, over all run terms and transition terms of (3.1), the bounds of Lemma 3.6(c) and (d) at the corresponding entries, symmetrically. Since $\nabla^2 F$ is the sum of the Hessians of these terms, W satisfies the hypothesis of Lemma 3.5. All entries of W are nonnegative.

Lemma 3.7 (Eigenvalue certificate)**.** *Let H be a real symmetric $d \times d$ matrix, let $\lambda \in \mathbb{R}$ and $N = H - \lambda I$. For $a = 1, \dots, d$ define recursively*

$$L_{ab} = \frac{1}{D_b}\Big(N_{ab} - \sum_{\gamma<b} L_{a\gamma}L_{b\gamma}D_\gamma\Big) \quad (b < a), \qquad D_a = N_{aa} - \sum_{\gamma<a} L_{a\gamma}^2 D_\gamma.$$

If the recursion yields $D_1, \dots, D_d > 0$, then $\lambda_{\min}(H) > \lambda$.

Proof. The recursion gives $N = LDL^T$, where L is unit lower triangular with entries L_{ab} below the diagonal and $D = \operatorname{diag}(D_1, \dots, D_d)$. For $v \neq 0$ we have $L^T v \neq 0$, so $v^T N v = \sum_a D_a\big((L^T v)_a\big)^2 > 0$. □

If the entries of H are known only up to enclosing intervals and the recursion is evaluated in interval arithmetic, then the computed intervals contain the numbers D_a of the exact matrix, so positive lower endpoints of these intervals certify $\lambda_{\min}(H) > \lambda$.

Close to a change in the combinatorial type of the hull, a single fan bound loses in its first-order term, because fans built on the two sides of the change have gradients of different signs. The next lemma combines several fan bounds on the same box.

Lemma 3.8 (Combination bound)**.** *Let B be a box with centre c and half-widths h. For $i = 1, \dots, m$ let a witness fan satisfy the hypotheses of Lemma 3.3 on B, let F_i be its fan area, put $g_i = \nabla F_i(c)$, and let $e_i \in \mathbb{R}$ be such that $F_i(p) \ge F_i(c) + g_i \cdot (p - c) - e_i$ for all $p \in B$. Let $\kappa_1, \dots, \kappa_m \ge 0$ with $\kappa_1 + \cdots + \kappa_m = 1$. Then for all $p \in B$*

$$A(p) \;\ge\; \sum_{i=1}^{m} \kappa_i(F_i(c) - e_i) - \sum_a \Big|\sum_{i=1}^{m} \kappa_i g_{i,a}\Big| h_a.$$

Proof. Let $p \in B$. By Lemma 3.3, $A(p) \ge F_i(p)$ for every i, and hence $A(p) \ge \sum_i \kappa_i F_i(p)$. By the hypothesis on the e_i, this sum is at least $\sum_i \kappa_i(F_i(c) - e_i) + u \cdot (p - c)$ with $u = \sum_i \kappa_i g_i$, and $u \cdot (p - c) \ge -\sum_a |u_a| h_a$. □

By Lemma 3.5, the number e defined there can serve as e_i. For $m = 1$ the lemma then gives the bound L of Lemma 3.5.

4. The certificates and their verification

4.1. **Certificates.** A certificate for the bodies $D, B_{n_1}, \dots, B_{n_k}$ and a target τ records a root box X, a grid of equal cells on X, and for each cell a binary tree of boxes, given in depth-first preorder by the coordinate in which each box is split at its midpoint. Each leaf is marked as a *bound leaf*, closed by the fan bound, a *combination leaf*, closed by Lemma 3.8, or a *far leaf*, closed by the corner lemma. For a combination leaf the certificate lists the number m of fans,

sign vectors $\sigma_1, \dots, \sigma_m \in \{-1, 0, 1\}^d$ and weights $\tilde{\kappa}_1, \dots, \tilde{\kappa}_m$. The certificate also records the parameters N and ε of the finer witness set of Section 4.2, which the checker reuses in steps (5) and (6) below. The cells are distributed over P parts, which can be checked separately. The repository describes the file format.

4.2. **The search.** The search program is a depth-first branch and bound in double precision. At a box with centre c it builds a witness fan in three steps. First, it takes the support points of $K(c)$ in N equally spaced directions. Each of them is a point of the disk, a corner of a placed Reuleaux polygon or a point of one of its arcs, and is recorded as a witness on the corresponding body. Second, it repeatedly inserts, for each edge of the current polygon, the support point of $K(c)$ in the direction of the outer normal of the edge if this point lies more than ε outside the edge. Third, it chooses the fan centre z among nine points of D and drops witnesses until a floating-point version of the inequalities of Lemma 3.6(b) holds. It then evaluates the bound L of Lemma 3.5, with W from Lemma 3.6 and the numerically computed $\lambda_{\min}(H)$. The finer witness set uses $N = 1024$ directions and $\varepsilon = 10^{-6}$, and the coarser one $N = 256$ and $\varepsilon = 10^{-5}$; for the certificates with B_7 and B_9 the search tries the coarser one first. A box is closed when $L \geq \tau + 10^{-6}$. For the certificate with B_9, at some of the boxes that a single fan does not close, the search also builds fans from the support points of $K(c)$ and of $K(c + \sigma \circ h)$, where $\sigma \circ h = (\sigma_a h_a)_a$, for five sign vectors σ chosen from the gradient, and chooses their weights by a linear program that maximizes the bound of Lemma 3.8. Otherwise it splits the box in the coordinate that contributes most to the loss in L. The released code contains one version of the search for each certificate.

4.3. **The checker.** The checker works in ball arithmetic [9]. The box coordinates are double-precision numbers, which ball arithmetic represents exactly. Every comparison that decides whether a part is accepted is made in ball arithmetic or exactly, and the double-precision inputs of the comparisons in ball arithmetic, such as box endpoints, half-widths and the distances used at far leaves, are exact. The checker reads τ as the shortest decimal number that represents the header value, here 0.8347, 0.836 and 0.8366. For each part it performs the following steps.

(1) *Presence.* It verifies that all P parts exist and that their headers agree in the bodies, τ, X, the grid and P.
(2) *Root box.* For each body $i \geq 1$ let w_i be the smallest of the numbers $-\ell$ and u over the two coordinate ranges $[\ell, u]$ of t_i in X. The checker verifies $w_i > 0$ and $f(g_{n_i}(w_i)) > \tau$. It also verifies that the range of ρ_2 in X contains $[0, \pi/n_2]$ and that the range of ρ_i contains $[0, 2\pi/n_i]$ for $i \geq 3$. Thus X satisfies the hypotheses of Corollary 2.5.
(3) *Tree.* It decodes the trees and computes the boxes, splitting each box at the double-precision midpoint of the split coordinate. It rejects unknown codes, a tree that is cut off and data after the last tree, and it rejects a part whose data for combination leaves miss such a leaf or describe another node.
(4) *Far leaves.* At a far leaf it verifies $f(g_{n_i}(\mu_i)) > \tau$ for some i, where μ_i is the smallest value of $|t_i|$ on the leaf. Then $A > \tau$ on the leaf by Lemma 2.4.
(5) *Bound leaves.* At a bound leaf it computes the centre c and the half-widths h in double precision and verifies, in rational arithmetic, that $c \pm h$ are exactly the endpoints of the leaf box. It builds a witness fan with its own implementation of the heuristic of Section 4.2; the certificate does not store the fan. It tries the coarser witness set first and, if the verification below fails, the finer one. It moves the witnesses slightly towards the centres of their bodies. It then verifies in ball arithmetic that $|z|^2 < 1/4$, that each witness lies in its body ($|q|^2 < 1/4$ for the disk, $|q - V_{n,l}|^2 < 1$ for all l for B_n), that $\det(x_j(c) - z, x_{j+1}(c) - z)$ exceeds the bound of Lemma 3.6(b) for all j, and that the computed sum of the angles at c differs from 2π by

less than 1. It evaluates $F(c)$, $\nabla F(c)$ and $\nabla^2 F(c)$ through (3.1) and computes W. It puts $\lambda = \min(0, \lambda_f) - 10^{-9}(1 + |\lambda_f|)$, evaluated in double precision, where λ_f is a floating-point estimate of $\lambda_{\min}(\nabla^2 F(c))$, and certifies $\lambda_{\min}(\nabla^2 F(c)) > \lambda$ by Lemma 3.7. Finally it verifies $L > \tau$.

(6) *Combination leaves.* At a combination leaf it computes c and h and verifies that $c \pm h$ are exactly the endpoints of the leaf box, as in step (5). It reads $\sigma_1, \dots, \sigma_m$ and $\tilde{\kappa}_1, \dots, \tilde{\kappa}_m$ from the certificate, rejects the leaf if a weight is negative or not a number or if all weights are 0, and puts $\kappa_i = \tilde{\kappa}_i/(\tilde{\kappa}_1 + \cdots + \tilde{\kappa}_m)$ in ball arithmetic. For each i it builds a witness fan from the support points of $K(c + \sigma_i \circ h)$, with the parameters N and ε of the header, and verifies the conditions of step (5) on the whole leaf, up to and including the angle sum at c. A fan that fails them is skipped if $\tilde{\kappa}_i = 0$, and otherwise the leaf is rejected. For each remaining fan it computes $F_i(c)$, $g_i = \nabla F_i(c)$, W_i and λ_i as in step (5), and e_i by Lemma 3.5. Finally it verifies that the right-hand side of Lemma 3.8 exceeds τ.

If the factorization in step (5) or (6) fails, the checker puts $\lambda = \min(0, \gamma)$, where γ is a lower endpoint, computed in ball arithmetic, of $\min_a(H_{aa} - \sum_{b \neq a} |H_{ab}|)$ for $H = \nabla^2 F(c)$. By Gershgorin's theorem, $\lambda_{\min}(H) \geq \gamma$, so again $\lambda \leq \min(0, \lambda_{\min}(H))$. The search of Section 4.2 is not part of the proof, and neither are the witnesses of steps (5) and (6) or the sign vectors: only the inequalities verified in ball arithmetic enter it.

4.4. **Proofs of Theorem 1.1 and Proposition 4.2.**

Proposition 4.1. *For the three certificates of Table 1, the checker accepts all parts. All box coordinates in the trees are exact in double precision, and the leaves tile the root box.*

Proposition 4.1 is verified by computation: the checker verifies its first sentence, and the tree decoders of Section 4.5 verify the second.

Proposition 4.2. $M(D, B_3, B_5) \geq 0.8347$.

Proofs of Theorem 1.1 and Proposition 4.2. Consider the certificate for $(n_1, n_2) = (3, 5)$ and $\tau = 0.8347$, the certificate for $(n_1, n_2, n_3) = (3, 5, 7)$ and $\tau = 0.836$, or the certificate for $(n_1, \dots, n_4) = (3, 5, 7, 9)$ and $\tau = 0.8366$, and let X be its root box. By step (2), X satisfies the hypotheses of Corollary 2.5. By step (1) the cells of all parts together form the grid of X, and by Proposition 4.1 the leaves of their trees tile X. On a far leaf, $A > \tau$ by step (4) and Lemma 2.4. Let B be a bound leaf with centre c.

We show that $A > \tau$ on B. The checker verified step (5) on B itself. By Lemma 3.6(b) the determinants $\det(x_j(p) - z, x_{j+1}(p) - z)$ are positive for all $p \in B$. In particular each angle at c lies in $(0, \pi)$, so the sum of the angles at c is a multiple of 2π, and the check of step (5) shows that it equals 2π. Lemma 3.3 gives $A \geq F$ on B. The witnesses lie on at least two bodies. Indeed, the points $x_j(c) - z$ do not lie in an open half-plane bounded by a line through the origin, since their angles lie in $(0, \pi)$ and add up to 2π. So z lies in the convex hull of the points $x_j(c)$. If all witnesses lay on one body i, then $z \in P_i(c)$, and Lemma 3.1 with $K = P_i(c)$ and the isodiametric inequality would give $F(c) \leq \operatorname{area} P_i(c) \leq \pi/4 < \tau$. Here the checker evaluates $F(c)$ by grouping the witnesses into runs, and by Lemma 3.4 this gives $F(c)$ also when there is only one run. But $L \leq F(c)$, because $\lambda \leq 0$ and W has nonnegative entries, and the checker verified $L > \tau$. So (3.1) applies, and the matrix W computed by the checker bounds the variation of $\nabla^2 F$ on B by Lemma 3.6. Lemma 3.7, or Gershgorin's theorem in the fallback, gives $\lambda \leq \min(0, \lambda_{\min}(\nabla^2 F(c)))$. Now Lemma 3.5 gives $F \geq L > \tau$ on B.

Let B be a combination leaf with centre c, and consider one of its fans that the checker did not skip. As for a bound leaf, the checks of step (6) and Lemma 3.6(b) show that the fan satisfies the hypotheses of Lemma 3.3 on B. If its witnesses lie on at least two bodies, then (3.1) applies,

W_i bounds the variation of $\nabla^2 F_i$ on B by Lemma 3.6, $\lambda_i \le \min(0, \lambda_{\min}(\nabla^2 F_i(c)))$ as in step (5), and Lemma 3.5 gives $F_i(p) \ge F_i(c) + g_i \cdot (p - c) - e_i$ for all $p \in B$. If all its witnesses lie on one body, then F_i is constant on B, because the sum of Lemma 3.4 over the whole cyclic sequence equals $\sum_j \det(q_j, q_{j+1})$. The checker computes the gradient of F_i as the sum of the derivatives of its run term and of the term that closes the run, from its last witness back to its first, so its value encloses $\nabla F_i(c) = 0$, and $e_i \ge 0$ because $\lambda_i \le 0$ and W_i has nonnegative entries. The same inequality therefore holds. The skipped fans have weight 0. The weights κ_i are nonnegative and add up to 1, and the enclosure computed by the checker contains the right-hand side of Lemma 3.8 for these weights. Lemma 3.8 gives $A > \tau$ on B.

Hence $A > \tau$ on X, and Corollary 2.5 gives $M(D, B_{n_1}, \dots, B_{n_k}) \ge \tau$ and $\Lambda \ge \tau$. □

4.5. **Further checks.** We ran further programs on the certificates; the repository describes them, their output and further tests of the checker. Two tree decoders, the second written separately from the checker, rebuild every box of the trees in exact rational arithmetic and confirm that the box verified at each leaf is the exact leaf box and that the leaves tile the root box. A verifier written separately from the checker and the search uses a different bound. For fixed rotations, every determinant $\det(x_j - z, x_{j+1} - z)$ and the fan area F are affine in each translation coordinate, so their minima over a box are attained at vertices of the box of translations, and the verifier bounds their minima over the rotations from below in ball arithmetic. At a combination leaf it builds the fans of positive weight from the sign vectors and weights of the certificate and bounds $\sum_i \kappa_i F_i$ in the same way. It thus uses neither Lemma 3.5 nor Lemma 3.8, only the fan bound and the inequality $A \ge \sum_i \kappa_i F_i$. It re-verified all 16,193,402 leaves of the certificate for the five bodies, 9,018 of them after bisection (Table 1), and stratified samples of the leaves of the other two, including those with the smallest checker bounds; a further program confirms from its output that every leaf of the certificate for the five bodies was verified.

TABLE 1. The certificates of Theorem 1.1 and Proposition 4.2 and their verification.

	D, B_3, B_5	D, B_3, B_5, B_7	D, B_3, B_5, B_7, B_9
Parameters d; target τ	5; 0.8347	8; 0.836	11; 0.8366
Half-widths $w_1, \dots, w_k$ of X	0.193613, 0.196856	0.198977, 0.201023, 0.199964	0.201432, 0.202937, 0.201775, 0.201176
Nodes	53,752	1,552,274	32,384,756
Leaves (far leaves)	27,388 (0)	808,905 (0)	16,193,402 (33)
leaves closed by Lemma 3.8	0	0	10,883,512
Smallest accepted leaf bound	0.834700004923	0.836000001625	0.836600000032
Smallest root margin $f(g_{n_i}(w_i)) - \tau$	4.0×10^{-9}	4.5×10^{-9}	3.0×10^{-9}
Second verifier: leaves (split)	451 (7)	350 (7)	16,193,402 (9,018)

5. Proofs in Lean

The bounds of Theorem 1.1 and Proposition 4.2 and their consequences for Λ are also proved in Lean 4 [13] with Mathlib [11]. Each of them has a proof in which the Lean kernel checks every step, and the bound 0.8366 also has a proof that runs its certificate checks as compiled code. None of the formal proofs checks the certificates of Section 4. They check separate certificates, built for a box bound that is easier to formalize (Table 2).

5.1. **Statements.** For each of the families D, B_3, B_5 and D, B_3, B_5, B_7 and D, B_3, B_5, B_7, B_9, the formal statements say that its least hull area M is at least its bound and that Λ is at least that bound. They also state the bound for the weakest of the readings mentioned after

Theorem 1.1, which gives its strongest form: every convex set that contains a congruent copy of every convex set of diameter 1 has area at least the bound. The repository gives the names of the theorems. In these statements the plane is $\mathbb{R}^2$ with Lebesgue measure, congruent copies are images under isometries, reflections included, and Λ is the infimum of the areas of convex sets that contain a congruent copy of every set of diameter at most 1.

5.2. **The box bound.** Each rotation angle ρ is replaced by the coordinate $s = \tan(\rho/2)$, so that the cosine and the sine of ρ are rational functions of s, and the trees split boxes in these coordinates. On a leaf, a rotation is the rotation at the centre of the leaf followed by a rotation by an angle δ, and $C = \cos\delta - 1$ and $S = \sin\delta$ lie in intervals whose rational end points are computed from the end points of the leaf. The positions of the witnesses are affine in the translations and in C and S, so the fan area is exactly a quadratic polynomial in these variables. The checker adds multiples of $2C + C^2 + S^2$, which vanishes since $(1 + C)^2 + S^2 = 1$. Treating C and S as independent variables, it bounds the sum from below on the box by its value and gradient at the centre and a diagonal shift that makes the Hessian positive semidefinite; an exact $LDL^\top$ factorization certifies this shift. This bound takes the place of Lemma 3.5 and has no remainder term. The determinants $\det(x_j - z, x_{j+1} - z)$ are quadratic in the same variables, and the checker bounds them from below by their values and gradients at the centre and the absolute values of their second-order coefficients. At the centre it uses rational upper bounds for the angles to check that they add up to less than 4π, and hence to 2π. A combination leaf combines such bounds for several fans as in Lemma 3.8. The vertices of the Reuleaux polygons enter through rational approximations within 2^{-36}, proved in Lean, and a witness on B_n must lie in the disks of radius $1 - 2^{-36}$ about them.

5.3. **The checker and the reduction.** A checker written in Lean verifies the leaves in exact rational arithmetic, and Lean proves that a leaf it accepts has hull area greater than the target at every placement in the leaf. Like the checker of Section 4, it builds the witnesses with floating-point heuristics, and here it builds the fan centres, the shifts and the multipliers in the same way. The soundness theorem holds for all choices of these data. The reduction from arbitrary isometries to placements in the root box, the fan bound, the convexity of the bodies and their diameters, the soundness of the checker and of the decoding of the trees, and the fact that the cells cover the root box are proved in Lean and checked by the kernel. So is the bound for the placements outside the root box, which uses a polygon inscribed in the hull instead of the area formula of Lemma 2.4.

5.4. **The kernel-checked proofs.** In the kernel-checked proofs, the data of each leaf were computed beforehand and stored in the modules. For each leaf, a theorem states that the checker accepts it and is proved by evaluating the checker in the Lean kernel. Further theorems, proved in the same way, state that the leaves of each cell are exactly the boxes of its tree and that the cells make up the root box. These proofs therefore use only the three standard axioms of Lean, `propext`, `Classical.choice` and `Quot.sound`, and their trusted base is Lean's kernel, including its built-in arithmetic on natural numbers.

The certificates of the kernel-checked proofs have their own root boxes, and Table 2 gives their cells and leaves.

TABLE 2. The certificates of the kernel-checked Lean proofs.

	D, B_3, B_5	D, B_3, B_5, B_7	D, B_3, B_5, B_7, B_9
Cells	1,024	65,536	2,048
Leaves (combination leaves)	25,214 (0)	278,093 (0)	9,239,121 (5,599,347)

The leaf data of the certificate for D, B_3, B_5, B_7, B_9 were computed from the certificate of the proof with compiled checks, by programs whose output the kernel checks leaf by leaf. For D, B_3, B_5 and D, B_3, B_5, B_7, however, the translation bounds of Table 1 would leave the polygon used for the placements outside the root box with area below the target. These bounds are therefore enlarged by 0.6% and 0.4%, which raises the area of the polygon from 0.834675 to 0.834955 and from 0.835975 to 0.83617.

For D, B_3, B_5, B_7, since $R_{2\pi/3}B_3 = B_3$, rotating a placement as a whole by $2\pi/3$ about the centre of the disk gives a placement with the same $|t_i|$ and with ρ_2 shifted by $2\pi/3$; together with Lemma 2.3 this restricts ρ_2 to $[0, \pi/15]$, a third of the range in Corollary 2.5.

5.5. **The proof with compiled checks.** The proof with compiled checks uses the same tree as the kernel-checked proof for D, B_3, B_5, B_7, B_9 and has the same statements. Each of its modules of certificate data applies the checker to its data with `native_decide`, a Lean tactic that evaluates a decidable statement with compiled code instead of the kernel and records the result as an auxiliary axiom. Besides the three standard axioms, this proof thus uses one auxiliary axiom for each module, asserting that the checker accepts the data of that module. These rest on the Lean compiler and runtime and on the compiled checker, and the rest of the proof is checked by the Lean kernel.

6. The least hull areas of the test sets

We record some numerical observations, not used in the proofs, on how far lower bounds from these test sets can go.

Mishra's placement of D, B_3, B_5, mentioned in Section 1, gives $M(D, B_3, B_5) \le 0.834781191$ [12, Section 3]. The bound 0.83474 of Hatchett [8] is therefore within 4.2×10^{-5} of $M(D, B_3, B_5)$, and the bound of Proposition 4.2 within 8.2×10^{-5}. Our certificate for Proposition 4.2 has 53,752 nodes and Hatchett's certificate of 0.83474 has 922,408. Hatchett's target, however, is about twice as close as ours to 0.834781191; for a given method, certificates grow as the target approaches the least hull area. Mishra's certificate of 0.8344, for a lower target, has 486,799,600 nodes. Local minimization found no placement with hull area below 0.8347809458.

For D, B_3, B_5, B_7, Mishra located a placement with hull area 0.836494901 numerically [12, Section 6.3]. Local minimization finds a placement whose hull area, computed in floating point by integrating the support function of the hull in closed form, is 0.83649045598. Rounded to ten decimals, this placement is

$$t_1 = (-0.0025482897, -0.0019350278), \qquad t_2 = (0.0250869718, -0.0032906511),$$
$$t_3 = (0.0028934171, -0.0127181545), \qquad \rho_2 = 0.0287183302, \qquad \rho_3 = 0.7016242528,$$

and the full values are in the archive. At the rounded placement the same computation gives 0.83649045600. There the polygon spanned by the support points in 2^{24} equally spaced directions has area 0.836490455978, and the polygon cut out by the corresponding support lines has area 0.836490465924. Numerically, therefore, the four bodies cannot give more than 0.8364904560. The first bound of Theorem 1.1 is within 5×10^{-4} of this value. Our search for this bound examined 1,552,274 boxes, the nodes of its certificate. For these four bodies, Mishra fitted a power law to the box counts of his eight-dimensional runs, as a function of the distance between the target and the least hull area. From this fit he estimated that certifying even 0.8344, the bound of his proof with three bodies, would take about 8.6×10^{11} boxes with his method. He notes that in his five-dimensional runs the box count grew more slowly near the least hull area than such a fit predicts, and he concludes that allowing for this reduces the figure substantially, but not to a feasible size [12, Section 6.3].

For D, B_3, B_5, B_7, B_9, Gibbs's annealing found the hull area 0.83699098, with the arcs replaced by polygons of diameter 1 [5]. These polygons lie in the bodies, so this value is no upper bound for $M(D, B_3, B_5, B_7, B_9)$. Local minimization from many starting points, among them the placement above extended by a placement of B_9 and the leaf centres of the certificate with the smallest hull areas, finds a placement with hull area 0.83729500640, computed as above (Figure 1). Its full values are in the archive. The two polygons built in the same way have areas 0.837295006402 and 0.837295033965. So, numerically, the second bound of Theorem 1.1 is within 7×10^{-4} of $M(D, B_3, B_5, B_7, B_9)$.

With Gibbs's upper bound, $0.8366 \leq \Lambda \leq 0.8440935944$. Numerically, the five bodies cannot give lower bounds beyond about 0.83730, so lower bounds above this value need other test sets.

Data availability

The certificates, the checker `lbcheck.py`, the tree decoder `treecheck.py`, the search programs, the placements and the program for the polygon bounds of Section 6, and the second verifiers and decoders with the output of their runs on the certificate with B_9, the minimization and the tests of the checker (Section 4.5) are archived at doi:10.5281/zenodo.23717912 and available at `https://github.com/tejasvi/lebesgue-cover-bound/tree/v9`. The repository also gives the running times of the search, the checker and the Lean builds. The certificates are xz-compressed tar files of 17,308, 487,316 and 293,113,544 bytes, which also contain lists of the SHA-256 hashes of their files. Because of their size, the certificate for D, B_3, B_5, B_7, B_9, with 2,048 parts in 6,144 files, and the output of the first pass of the second verifier on it, an xz-compressed tar file of 116,500,532 bytes, are archived only at the DOI. The Lean files of Section 5 are in the directory `formal` of the repository, except the generated modules, which are archived at the DOI. The 77,175 generated modules of the proof with compiled checks, which hold its certificate and its final theorems, and their compiled files are in two zstd-compressed tar files of 133,521,541 and 481,071,638 bytes. The generated modules of the kernel-checked proofs for D, B_3, B_5 and D, B_3, B_5, B_7, with the output of their searches, and their compiled files are in four more, of 10,869,411 and 3,568,240,020 bytes for D, B_3, B_5 and of 1,155,309,716 and 936,081,748 bytes for D, B_3, B_5, B_7. The 406,888 generated modules of the kernel-checked proof for D, B_3, B_5, B_7, B_9 are archived without their compiled files, which take about 238 GB. The modules of the 2,048 cells, in one compressed archive per cell as it was built, are grouped into sixteen tar files of 29,879,869,440 bytes in all. The 75,126 modules that walk the trees of the cells and collect the cells into the final theorems are in a zstd-compressed tar file of 66,701,378 bytes, as they were generated before the build. A further zstd-compressed tar file, of 66,568,744 bytes, lists the SHA-256 hashes of the sixteen tar files, of every generated module and of every compiled file of the build, so that a rebuild can be compared file by file. The file `formal/README.md` describes how to build and check all of them. The SHA-256 hashes of twelve of the archives, the last two of them for the kernel-checked proof for D, B_3, B_5, B_7, B_9, are

`2026ebe7e5339b89542e0429e5ad704b1a956278e3ae455b6d667b4c11892846` (D, B_3, B_5),
`d8a7f09dc236a7c647147bacc3e903f3c9e2bd2cadb601d000d1a67a2a237681` (D, B_3, B_5, B_7),
`6b5d28bc488edcfde9c6a49f3cb364f9086f445a58f85f166da23727036cf122` (D, B_3, B_5, B_7, B_9),
`0cf9696eb47681382492bc547d44519beeb69f492ee0cf26c520ec8254e1562b` (first pass),
`acb85d373917295c26f77acd2b2144c2f47256fcc6d9418dface3ff78c00133a` (compiled checks, modules),
`9a356edf6e801783658a296ebe9f52430212006e4ee700c3be5a1b285f12dbab` (compiled checks, compiled files),
`31a2058b782dab1dd5131267bf5a7e075bc343e963703bf684e1ed0c01235f4c` (D, B_3, B_5 in the kernel, modules),
`0caa58bf3ac7f5494053fe948dac88b16d08147c7a55e8334057196357e683e6` (D, B_3, B_5 in the kernel, compiled),
`3a0ff3ea18eb81b481f8a513ba632304af503f6140dfad6479317ec708491191` (D, B_3, B_5, B_7 in the kernel, modules),
`42091e9314c44daae000798e1bfb85365e00cc22bbb0a6ba73053f5535c5a70e` (D, B_3, B_5, B_7 in the kernel, compiled),
`765203c48ea883ec00ce50b1fcc5a48adc9bf7da7e9f4741c3b8a89308faac6c` (D, B_3, B_5, B_7, B_9 in the kernel, tree walks),
`1b96415125a178a4c16014a9c7b96c272adc8e32f7ac03291d7d3d95a4aa5234` (D, B_3, B_5, B_7, B_9 in the kernel, hash lists).

The checker needs Python 3 with NumPy and python-flint, and the Lean proofs need Lean 4 `v4.35.0-rc3` and Mathlib at the same tag.

References

[1] J. C. Baez, K. Bagdasaryan and P. Gibbs, *The Lebesgue universal covering problem*, J. Comput. Geom. **6** (2015), 288–299.

[2] P. Brass, W. Moser and J. Pach, *Research Problems in Discrete Geometry*, Springer, New York, 2005.

[3] P. Brass and M. Sharifi, *A lower bound for Lebesgue's universal cover problem*, Internat. J. Comput. Geom. Appl. **15** (2005), 537–544.

[4] G. Elekes, *Generalized breadths, circular Cantor sets, and the least area UCC*, Discrete Comput. Geom. **12** (1994), 439–449.

[5] P. Gibbs, *A new slant on Lebesgue's universal covering problem*, arXiv:1401.8217, 2014.

[6] P. Gibbs, *An upper bound for Lebesgue's covering problem*, arXiv:1810.10089, 2018.

[7] H. C. Hansen, *Small universal covers for sets of unit diameter*, Geom. Dedicata **42** (1992), 205–213.

[8] J. Hatchett, *Replay certificate for a* 0.83474 *lower bound in Lebesgue's universal covering problem*, software, Zenodo, 2026, doi:10.5281/zenodo.22135010, with a description in the repository `https://github.com/newmattock/lebesgue-cover-0.83474-certificate`.

[9] F. Johansson, *Arb: efficient arbitrary-precision midpoint-radius interval arithmetic*, IEEE Trans. Comput. **66** (2017), 1281–1292.

[10] H. Martini, L. Montejano and D. Oliveros, *Bodies of Constant Width: An Introduction to Convex Geometry with Applications*, Birkhäuser, Cham, 2019.

[11] The mathlib Community, *The Lean mathematical library*, in: Proc. 9th ACM SIGPLAN Int. Conf. Certified Programs and Proofs (CPP 2020), 2020, 367–381.

[12] U. Mishra, *Curves of constant width and Lebesgue's covering problem*, arXiv:2608.30538v2, 2026.

[13] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction – CADE 28, Lecture Notes in Comput. Sci. **12699**, Springer, 2021, 625–635.

[14] J. Pál, *Über ein elementares Variationsproblem*, Danske Vid. Selsk. Mat.-Fys. Medd. **3** (1920), no. 2, 1–35.

[15] R. Sprague, *Über ein elementares Variationsproblem*, Mat. Tidsskr. B (1936), 96–99.

[16] T. Tao et al., *Optimization constants in mathematics*, `https://teorth.github.io/optimizationproblems/`, 2026.

[17] N. Xie, *A certified lower bound for Lebesgue's universal cover problem*, arXiv:2606.04458, 2026.

[18] S. Zeng, *An exact hierarchy for Lebesgue's universal covering constant and a certified* 0.834 *lower bound*, arXiv:2609.01284, 2026.

ORCID: `https://orcid.org/0000-0003-4668-3639`