EXACT RATIONAL CERTIFICATES FOR REAL TANGENCY COUNTS: 144 TRITANGENT CIRCLES, AND A TWELVE-INTEGER WITNESS FOR CIRCLES TANGENT TO A CONIC AND TWO LINES

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. Three general conics in the plane admit 184 complex circles tangent to all three, and Breiding, Lindberg, Ong and Sommer conjectured that at most 136 of them can be real. Brysiewicz has recently refuted that conjecture by exhibiting a triple of conics with 144 real tritangent circles, certified numerically with interval arithmetic. We give a proof of his lower bound that uses no floating point and no interval library: an exact rational certificate, checked symbolically, for each of the 144 circles. The certificate format is elementary and reusable. Every equation of a marked tangency system has total degree two, so the divided difference $F(x) - F(y) = J_F\left(\frac{x+y}{2}\right)(x - y)$ holds exactly; a Newton-like map is then a contraction on a box as soon as two rational inequalities hold, and the Banach fixed point theorem—rather than Brouwer or degree theory—produces the zero. We apply the same certificate to the constituent problem QL^2, circles tangent to one conic and two lines, whose maximal real count Fiorelli Vilmart posed as an open problem and whose current record of 14, out of 16 complex, is an ingredient of the count 144; his appendix certifies the nine-variable tritangent system and none of the four constituent problems, so that 14 carries no certificate. We certify 14 for his own limiting configuration, and exhibit a second configuration attaining 14 whose conic and two lines have twelve integer coefficients of at most three digits. We also record two octics whose roots are the QL^2 solutions on the two bisectors, the identity $F_1 + F_2 = (1 + m^2)D^2$ they satisfy, and the resulting localisation of the two families of eight in complementary double wedges. The counts 144 and 14 are Brysiewicz's; what is new here is the exact certification, the small witness, and the bisector structure. We do not prove that these counts are exact, and we do not settle whether 16 is attainable. Everything proved below is machine-checked in Lean 4 against *Mathlib*, except where the text says otherwise.

1. INTRODUCTION

1.1. Circles tangent to three conics.

A *circle* in the plane is the zero set of

$$(x - s)^2 + (y - t)^2 - r, \tag{1}$$

with centre (s, t) and *squared* radius r; over $\mathbb{C}$ these are exactly the conics through the two circular points $[1 : \pm i : 0]$. Given three conics C_1, C_2, C_3 in the plane, how many circles are tangent to all three? Emiris and Tzoumas showed that there are at most 184 [4], and Breiding, Lindberg, Ong and Sommer showed that 184 is attained for generic conics [1]. The real question is harder. Breiding–Lindberg–Ong–Sommer exhibit three real conics with 136 real tritangent circles and conjecture that this is optimal:

Conjecture 1.4 of [1]. *The maximal number of real circles tangent to three conics is 136.*

Brysiewicz [3] has refuted it: [3, Theorem 1.1] reads "there exists a triple of conics admitting 144 tritangent circles", and the triple is the zero locus of

$$\begin{aligned} &Q_1(x, y) = 20x^2 - 5y^2 + 1, \\ &Q_2(x, y) = L_1^2 - \delta^2(x - x_1)^2 + \varepsilon, \qquad L_i = y - y_i - m_i(x - x_i), \\ &Q_3(x, y) = L_2^2 - \delta^2(x - x_2)^2 + \varepsilon, \end{aligned} \tag{2}$$

with

$$(x_1, y_1) = \left(\tfrac{833}{500}, \tfrac{2399}{1000}\right), \quad (x_2, y_2) = \left(\tfrac{2497}{1000}, \tfrac{3857}{1000}\right), \quad m_1 = \tfrac{1601}{1000}, \quad m_2 = \tfrac{2261}{1000},$$

and $\delta = 10^{-4}$, $\varepsilon = 10^{-12}$. The evidence offered in [3] is a numerical one: the appendix of that paper runs the interval certification of Breiding–Rose–Timme [2] inside `HomotopyContinuation.jl` with `max_precision` $= 8192$, and reports that all 184 solutions of the marked tangency system are isolated and distinct, that 144 of them are real with positive squared radius, and that their (s, t, r)-coordinates are pairwise distinct.

The conics C_2 and C_3 of (2) are perturbed double lines. Normalised to constant term 1, as in the appendix of [3], their discriminants—the determinants of the associated symmetric 3×3 matrices—are

$$\operatorname{disc} C_2 = \tfrac{-24414062500000000000}{9099831527345428269442492809166947 9} \approx -2.683 \cdot 10^{-17},$$
$$\operatorname{disc} C_3 = \tfrac{-10^{22}}{32752901711195807265038335727772478530881271} \approx -3.053 \cdot 10^{-22},$$

against -100 for C_1. All three are smooth hyperbolas, but the last two are so nearly degenerate that nothing in this problem may be argued from smoothness: every non-degeneracy statement below is an inequality with an explicit number in it.

1.2. **What is proved here.** Our first result reproves Brysiewicz's lower bound from an exact rational certificate. Write Q_u, Q_v for the partial derivatives of a conic Q.

Theorem A. Let C_1, C_2, C_3 be the three conics of (2). There exist 144 tuples

$$(u_1, v_1, u_2, v_2, u_3, v_3, s, t, r) \in \mathbb{R}^9$$

such that for each $i \in \{1, 2, 3\}$ the point (u_i, v_i) lies on C_i and on the circle (1), the vectors $(u_i - s, v_i - t)$ and $\big(Q_{i,u}(u_i, v_i), Q_{i,v}(u_i, v_i)\big)$ are parallel, and (u_i, v_i) is a smooth point of C_i; such that $r > 0$; and whose 144 triples (s, t, r) are pairwise distinct. In particular the maximal number of real circles tangent to three real conics is at least $144 > 136$, so Conjecture 1.4 of [1] is false.

The count 144 and the parameter point (2) are Brysiewicz's, and we claim neither. What is new in Theorem A is the proof: 144 boxes with rational centres and rational data, 144×90 rational numbers in all, from which the existence of a genuine real solution in each box follows by an argument with no floating-point step, no interval library, and no appeal to the smoothness of C_2 and C_3.

The certificate that does this is stated in Section 3. It is a Krawczyk-type contraction test [6] specialised to systems whose every equation has total degree two, which is the case for every marked tangency system in this paper. The specialisation buys two things. First, for such a system the divided difference is exact,

$$F(x) - F(y) = J_F\Big(\frac{x+y}{2}\Big)(x - y), \tag{3}$$

with no remainder term, so a Newton-like map $K(x) = x - YF(x)$ satisfies $K(x) - K(y) = \big(I - YJ_F(\frac{x+y}{2})\big)(x - y)$ identically and existence follows from the Banach fixed point theorem, not from Brouwer's or from degree theory. Second, J_F is affine in x, so the supremum of each entry of $I - YJ_F$ over a sup-norm box is exact and closed form; no subdivision and no interval arithmetic are needed.

1.3. **The QL^2 cell.** The second half of the paper concerns the constituent problem that Brysiewicz's degeneration leaves open. Following a construction proposed by Fiorelli Vilmart [5, pp. 131–132], one lets two of the three conics degenerate to double lines while the third stays irreducible. The 184 tritangent circles then collide in groups of four, and

$$184 = 4\big(\#QP^2 + \#QPL + \#QLP + \#QL^2\big) = 4(6 + 12 + 12 + 16), \tag{4}$$

where QL^2 is the problem *circles tangent to one conic and two lines*, of complex degree 16. Table 1 of [3] records, for these four problems, the real counts $6, 10, 10, 14$ individually achieved and $6, 8, 8, 14$ achieved simultaneously; the second row is the source of $144 = 4(6 + 8 + 8 + 14)$, and the entry 14 for QL^2 is the new record that makes $160 = 4(6 + 10 + 10 + 14)$ the stated next target.

The maximal real count for QL^2 is open. Fiorelli Vilmart poses it explicitly in the "Perspectives" of her thesis [5, p. 132]:

> **Problème.** *Quel est le nombre maximal de cercles (réels) tangents à deux droites et à une hyperbole.*

She then proposes an approach: the locus $D_{q,d}$ of centres of circles tangent to one line d and one hyperbola q is a curve of degree 8, the centres of circles tangent to two lines are the two bisectors, and "*Le Théorème de Bézout nous prédit donc* 16 *intersections complexes ; reste à savoir combien sont réelles.*" A real count of 12 was known to be possible, and 16 is the trivial upper bound, so with Theorem B the maximum lies between 14 and 16.

The entry 14 carries no certificate in [3]: its appendix certifies the perturbed nine-variable tritangent system, and none of the four constituent problems. We supply certificates, for a configuration of [3] and for a new one.

Theorem B. Let Q be the conic $20u^2 - 5v^2 + 1$ and let

$$\ell_1 :\ -\tfrac{1601}{1000}u + v + \tfrac{134133}{500000} = 0, \qquad \ell_2 :\ -\tfrac{2261}{1000}u + v + \tfrac{1788717}{1000000} = 0$$

be the axes L_1, L_2 of the two degenerating conics of (2). There exist 14 pairwise distinct circles, each tangent to ℓ_1 and to ℓ_2 and tangent to Q at a real smooth point of Q, and each with positive squared radius.

Theorem C. Let

$$Q = -19u^2 - 48uv + 107v^2 - 71u + 32v + 3, \qquad \ell_1 :\ 24u + 115v - 58 = 0, \qquad \ell_2 :\ 43u + 108v + 46 = 0.$$

Then there exist 14 pairwise distinct circles, each tangent to ℓ_1 and to ℓ_2 and tangent to Q at a real smooth point of Q, and each with positive squared radius. (Q is a smooth hyperbola: its discriminant is $-442183/4 \neq 0$ and its quadratic part $-19u^2 - 48uv + 107v^2$ has $B^2 - 4AC = 10436 > 0$. This parenthetical is one line of rational arithmetic performed outside the formal development, and the theorem does not use it.)

Again the number 14 is not ours. What Theorem C adds is a configuration attaining it whose twelve defining coefficients are integers of at most three digits, against the six-digit denominators that the degeneration of [3] inherits from (2), together with a certificate. Such configurations are not easy to stumble on: in the search reported in Section 8, 14 occurs in 11 of 1411 independent exact hill climbs, and never in 20 000 uniformly sampled configurations.

1.4. **What the literature contains, and what it does not.** One caveat belongs in the introduction rather than in a footnote. The natural place for a small QL^2 witness to already exist is the source that poses the problem, Fiorelli Vilmart's 2009 Geneva thesis [5]; it is written in French and is not on arXiv, and [3] reports that it was unknown to its author until it was located during the preparation of that paper. We have read its "Perspectives", pp. 131–133, where the QL^2 problem is posed, and have searched the text of all 168 pages. What stands in the Perspectives is the complex count 16, the bisector approach quoted above, and—in the estimate table on p. 131, whose $k = 0$ row is *"cercles passant par* 0 *points singuliers, tangents à* 2 *droites et à une hyperbole"*—the value 12, attributed there to the method of Ronga–Tognoli–Vust [9]. That entry is the provenance of the sentence "a real count of 12 was known to be possible" in [3]: the same table yields her estimate $152 = 4(6 + 10 + 10 + 12)$, which [3] reproduces. No count of 14 occurs anywhere in the thesis, the symbol $D_{q,d}$ occurs only in the Perspectives, and the maximal real count is left as a question. We therefore state Theorem C in the form above: a configuration with three-digit integer coefficients attaining the record 14, certified exactly. We do not claim that 14 is new. Our search of the thesis was of its extracted text, so it does not cover content that appears only inside a figure.

1.5. **Grades.** To be explicit about what this paper does and does not settle:

- the counts 144 and 14 are due to [3]; the certificates for them are ours;
- "exactly 144", "exactly 14", "$\#QL^2 \leq 14$" and "$\#QL^2 = 16$ is attainable" are *not* proved here, and Section 8 says what each would cost;
- the octic identities of Section 6 are elementary algebra, recorded because they are the tools an upper bound for QL^2 would use, and because the bisector decomposition they make precise is the one proposed in [5, p. 132].

2. The two tangency systems

Write a conic as $Q(u,v) = Au^2 + Buv + Cv^2 + Du + Ev + F$ and a line as $\ell(u,v) = au + bv + c$, all coefficients rational. A circle with centre (s,t) and squared radius r is tangent to ℓ exactly when

$$\ell(s,t)^2 = r\,(a^2+b^2). \tag{5}$$

Tangency to a conic is expressed by *marking* the contact point, as in [3]: the point (u,v) is required to lie on Q and on the circle, and the two gradients there are required to be parallel.

Definition 2.1. Let Q be a conic and ℓ_1, ℓ_2 lines. A tuple $(u,v,s,t,r) \in \mathbb{R}^5$ is a *marked QL^2 solution* if

$$\begin{aligned} &Q(u,v) = 0, \qquad (u-s)^2 + (v-t)^2 = r, \\ &(u-s)\,Q_v(u,v) = (v-t)\,Q_u(u,v), \qquad \big(Q_u(u,v), Q_v(u,v)\big) \neq (0,0), \\ &\ell_i(s,t)^2 = r\,(a_i^2+b_i^2) \quad (i=1,2), \qquad r > 0. \end{aligned} \tag{6}$$

Two marked solutions determine the same circle exactly when their triples (s,t,r) agree, so "n pairwise distinct circles" means n marked solutions with pairwise distinct (s,t,r).

The first three lines of (6), together with the two conditions (5), are five polynomial equations in the five unknowns (u,v,s,t,r), and *each of them has total degree two*: the tangency determinant $(u-s)Q_v - (v-t)Q_u$ is a difference of two products of linear forms, hence quadratic. The system has complex degree 16, which is $\#QL^2$ in (4).

The tritangent system is the same construction with three conics and no lines: with unknowns $x = (u_1, v_1, u_2, v_2, u_3, v_3, s, t, r)$ and $i = 1,2,3$,

$$f_i = (u_i - s)^2 + (v_i - t)^2 - r, \qquad g_i = Q_i(u_i, v_i), \qquad h_i = \det \frac{\partial(f_i, g_i)}{\partial(u_i, v_i)}, \tag{7}$$

nine equations in nine unknowns, again all of total degree two. Its complex degree is 184 [1], far below the Bézout number $2^9 = 512$. The smoothness condition $\nabla Q_i(u_i, v_i) \neq 0$ in Theorem A is what makes $h_i = 0$ a statement about tangency rather than a vacuous identity at a singular point of Q_i. We do not deduce it from non-degeneracy of C_i: the marked point is only ever known to lie in a small box, and with discriminants of order 10^{-17} and 10^{-22} any gradient bound inherited from non-degeneracy of C_2 or C_3 would be useless at that scale. It is instead certified directly, by the explicit inequality of Lemma 3.4.

3. A rational contraction certificate for quadratic systems

This section is the certificate format. It is standard interval-certification technique [6, 2] with one specialisation, and we claim no novelty for it; we record it because the specialisation is what makes the data in Sections 4 and 5 small enough to check symbolically, and because it is reusable for any square system of quadratics.

Let $F : \mathbb{R}^n \to \mathbb{R}^n$ have components $F^{(1)}, \dots, F^{(n)}$, each a polynomial of total degree at most two with rational coefficients. Write J_F for the Jacobian.

Proposition 3.1 (exact divided difference)**.** *For all $x, y \in \mathbb{R}^n$,*

$$F(x) - F(y) = J_F\Big(\frac{x+y}{2}\Big)\,(x-y).$$

Proof. Both sides are additive in F, so it suffices to treat a single quadratic $q(x) = x^\top Ax + b^\top x + c$. With $m = (x+y)/2$ one has $\nabla q(m) = (A + A^\top)m + b$, and $(A + A^\top)m \cdot (x-y) = x^\top Ax - y^\top Ay$ by expanding; adding $b^\top(x-y)$ gives $q(x) - q(y)$. □

There is no error term and no derivative bound: the identity is algebra, valid over any field of characteristic zero. A second consequence of total degree two is that J_F is *affine* in its argument, so on a sup-norm ball each entry of J_F varies by at most a computable rational multiple of the radius.

Fix a rational centre $z \in \mathbb{Q}^n$, a rational radius $\rho > 0$, a rational matrix $Y \in \mathbb{Q}^{n\times n}$ and a rational $\kappa \in [0,1)$. Let B be the closed sup-norm ball of radius ρ about z. Writing the quadratic part of $F^{(k)}$ as $\sum_{p\le q} c^{(k)}_{pq} x_p x_q$, put

$$\mathrm{jvar}_k(j) \;=\; \sum_{p<j} \bigl|c^{(k)}_{pj}\bigr| + 2\bigl|c^{(k)}_{jj}\bigr| + \sum_{q>j} \bigl|c^{(k)}_{jq}\bigr|,$$

the exact ℓ^1 modulus of the linear part of the j-th column of J_F, so that this column moves by at most $\rho\,\mathrm{jvar}_k(j)$ across a ball of radius ρ. The certificate consists of the two rational inequalities

$$\text{(A)}\quad \sum_{j=1}^{n} \Bigl(\bigl| \bigl(I - Y J_F(z)\bigr)_{aj} \bigr| + \rho \sum_{k=1}^{n} |Y_{ak}|\,\mathrm{jvar}_k(j) \Bigr) \;\le\; \kappa \qquad \text{for every } a, \tag{8}$$

$$\text{(B)}\quad \Bigl| \bigl(Y\,F(z)\bigr)_a \Bigr| \;\le\; (1-\kappa)\,\rho \qquad \text{for every } a. \tag{9}$$

Theorem 3.2. *If* (8) *and* (9) *hold then F has a zero in B.*

Proof sketch. Let $K(x) = x - YF(x)$. By Proposition 3.1, $K(x) - K(y) = \bigl(I - Y J_F(m)\bigr)(x-y)$ with $m = (x+y)/2$, exactly. For $x, y \in B$ the midpoint m lies in B, and since J_F is affine, each entry of $I - Y J_F(m)$ differs from its value at z by at most $\rho \sum_k |Y_{ak}|\,\mathrm{jvar}_k(j)$; hence (8) bounds every row sum of $I - Y J_F(m)$ by κ, and K is κ-Lipschitz on B for the sup norm. Condition (9) says $\|K(z) - z\|_\infty \le (1-\kappa)\rho$, whence $K(B) \subseteq B$ by the triangle inequality. Banach's fixed point theorem gives $y \in B$ with $K(y) = y$, i.e. $YF(y) = 0$. Finally Y is injective: (8) at $\rho = 0$ says $\|I - Y J_F(z)\|_\infty \le \kappa < 1$, so $w = (I - Y J_F(z))w$ forces $w = 0$, so $Y J_F(z)$ has trivial kernel and is therefore invertible, and $\det Y \ne 0$. Hence $F(y) = 0$. ☐

Three remarks. (i) No inverse of Y is supplied; injectivity is derived from (8). Carrying an exact inverse instead would cost n^2 rationals of several hundred bits per witness—about 1.4 megabytes of certificate data for Theorem A alone. (ii) Nothing is assumed about Y: it is in practice a rounded numerical inverse of $J_F(z)$, and a wrong guess simply fails (8). (iii) Both inequalities are decidable statements about rational numbers, so the whole verification is a finite exact computation.

Distinctness of the certified zeros is free.

Lemma 3.3. *If two certificates with centres $z^{(1)}, z^{(2)}$ and radii ρ_1, ρ_2 satisfy $|z^{(1)}_i - z^{(2)}_i| > \rho_1 + \rho_2$ for some coordinate i, then their zeros differ in that coordinate.*

Smoothness of the marked contact point is certified the same way, by an inequality rather than by a discriminant.

Lemma 3.4. *Let Q be a conic and (u,v) a point with $|u - z_u| \le \rho$ and $|v - z_v| \le \rho$ for rationals $z_u, z_v, \rho \ge 0$. If*

$$\rho\bigl(2|A| + |B|\bigr) < |2Az_u + Bz_v + D| \qquad \textit{or} \qquad \rho\bigl(|B| + 2|C|\bigr) < |Bz_u + 2Cz_v + E|,$$

then $\nabla Q(u,v) \ne 0$.

4. The 144 real tritangent circles

Proof of Theorem A. We first fix the parameter point. The appendix of [3] lists the three conics through a flat vector p_{144} of 15 rationals, normalised so that each constant term is 1; expanding (2) symbolically over $\mathbb{Q}$ and dividing each conic by its constant term reproduces p_{144} read column-major, coefficient by coefficient in exact rational arithmetic. This is a check we ran before anything else, and it is the only point at which our data touches [3].

The system is (7) with these coefficients: nine quadratics in nine unknowns, so Theorem 3.2 applies. The certificate consists of 144 records, one per circle, each carrying a dyadic centre $z \in \mathbb{Q}^9$ with 80 fractional bits and a dyadic matrix $Y \in \mathbb{Q}^{9\times 9}$ with 36 fractional bits, i.e. $144 \times 90 = 12\,960$ rational numbers; the contraction constant is $\kappa = 1/2$ and the radius $\rho = 2^{-60}$ for every record. The finite computation that carries the proof is the following exhaustive check, performed in exact rational arithmetic:

- conditions (8) and (9) for each of the 144 records (largest row sum observed: 0.1386, against $\kappa = 1/2$; largest preconditioned residual: $9.5 \cdot 10^{-7}\,(1-\kappa)\rho$);

- $\rho < z_9$ for each record, which gives $r > 0$ by Theorem 3.2; the smallest certified squared radius is $0.0736\ldots$;
- the hypothesis of Lemma 3.4 for each of the 3×144 marked points; the tightest margins are on C_2 and C_3, where the certified gradient component exceeds the displacement the box allows by factors $1.4 \cdot 10^7$ and $1.1 \cdot 10^7$;
- the hypothesis of Lemma 3.3 in one of the coordinates s, t, r for each of the $\binom{144}{2} = 10\,296$ pairs; the smallest separation is $3.6 \cdot 10^{-5}$ against $2\rho \approx 1.7 \cdot 10^{-18}$.

Every item is a comparison of explicit rational numbers. Theorem 3.2 then produces a real solution of (7) in each box, Lemma 3.4 makes each marked point a smooth point of its conic, the bound $r > 0$ follows from $|r - z_9| \le \rho < z_9$, and Lemma 3.3 separates the triples (s, t, r). ☐

Remark 4.1. The lower bound is all that a refutation of Conjecture 1.4 needs. We do not prove that the triple (2) has *exactly* 144 real tritangent circles; see Section 8.

5. Circles tangent to a conic and two lines

Proof of Theorems B and C. Both are the same computation with $n = 5$ instead of $n = 9$. For each configuration the certificate consists of 14 records, each a dyadic centre $z \in \mathbb{Q}^5$ with 80 fractional bits and a dyadic $Y \in \mathbb{Q}^{5\times 5}$ with 36 fractional bits, with $\kappa = 1/2$ and $\rho = 2^{-60}$; the exhaustive check is item for item the one in the proof of Theorem A, with $\binom{14}{2} = 91$ separation pairs and one marked point per record. The largest row sums observed are $5.8 \cdot 10^{-8}$ for Theorem B and $1.5 \cdot 10^{-4}$ for Theorem C, the largest preconditioned residuals $9.1 \cdot 10^{-7}(1-\kappa)\rho$ and $8.9 \cdot 10^{-7}(1-\kappa)\rho$; the smallest certified squared radii are $0.07362\ldots$ and $0.17026\ldots$, and the smallest separations in (s, t, r) are 0.0194 and 0.0541, both enormous against 2ρ. ☐

The approximate solutions that the certificates surround were found in two independent ways, neither of which the proof depends on. For an arbitrary rational configuration one may eliminate: writing the centre as $O = p + \lambda \nabla Q(p)$ for a contact point $p = (u, v)$ on Q, so that $r = \lambda^2 \|\nabla Q(p)\|^2$, each line condition (5) becomes a quadratic in λ, and $\mathrm{Res}_v\big(Q, \mathrm{Res}_\lambda(E_1, E_2)\big)$ is a univariate polynomial of degree 16 over $\mathbb{Q}$ whose real roots correspond to the real QL^2 solutions. For both configurations of this section that eliminant is irreducible and squarefree with 14 real roots (8 positive, 6 negative), its coefficients occupying 270 and 220 bits respectively. Independently, solving the five-variable system (6) numerically at 250 digits from those roots returns 14 real solutions in each case, all with $r > 0$. Both computations are outside the certified development; they located the boxes, and Theorem 3.2 is what proves the theorem.

Remark 5.1. A consistency check between the two halves of the paper, again numerical and carrying no claim: the smallest squared radius among the 14 limiting QL^2 circles of Theorem B is $0.0736224\ldots$, and the smallest among the 144 real tritangent circles of Theorem A is $0.0736179\ldots$. The two differ by $4.5 \cdot 10^{-6}$; the configurations differ by the perturbation $\delta = 10^{-4}$, $\varepsilon = 10^{-12}$ of (2), so this is the degeneration of [3] seen from both ends.

6. Two octics, and where the sixteen solutions sit

The identities in this section are elementary; we record them because they make the bisector decomposition proposed in [5, p. 132] explicit, and because they are the tools that an upper bound for QL^2 would use.

The problem is invariant under the similarities of the plane, which carry circles to circles and preserve tangency, so for two non-parallel lines we may normalise their common bisectors to the coordinate axes and write the lines as $v = mu$ and $v = -mu$. A circle tangent to both has its centre on a bisector: on the u-axis, with squared radius $m^2 s^2/(1 + m^2)$, or on the v-axis. Parametrise the conic rationally, $\theta \mapsto \big(X(\theta) : Y(\theta) : W(\theta)\big)$, and set

$$a = X'W - XW', \quad b = Y'W - YW', \quad S = a^2 + b^2, \quad P = Xa + Yb, \quad D = Xb - Ya, \quad U = Y^2 - m^2 X^2.$$

The tangency parameters of circles centred on the u-axis are the roots of

$$F_1 = (1+m^2)Y^2S - m^2P^2,$$

and those of circles centred on the v-axis the roots of $F_2 = (1+m^2)X^2S - P^2$; both are octics in θ, and $8+8=16=\#QL^2$.

Proposition 6.1. *As polynomial identities,*

$$F_1 + F_2 = (1+m^2)D^2, \qquad F_1 = S\,U + m^2D^2, \qquad F_2 = D^2 - S\,U, \qquad D = W\,(XY' - YX').$$

Moreover, let q be the homogenisation of the conic and put $\Phi = q(X,Y,W)$. If $\Phi = 0$ identically—that is, if the parametrisation lies on the conic—then $a\,q_X(X,Y,W) + b\,q_Y(X,Y,W) = 0$, where q_X, q_Y are the first two partial derivatives of q.

The first identity is Lagrange's; the second and third follow from it; the fourth is one line; the last is Euler's relation combined with $\frac{d}{d\theta}\Phi = 0$. Their content is that $U = (Y-mX)(Y+mX)$ is the product of the two line forms while S is a sum of two squares, which separates the two families of eight.

Proposition 6.2. *Over $\mathbb{R}$, the values F_1 and F_2 are never both negative. At a real parameter where $S>0$: if $F_1 = 0$ there then $U \le 0$, and if $F_2 = 0$ there then $U \ge 0$. In particular $F_1 \ne 0$ at a real parameter with $S>0$ and $U>0$, and $F_2 \ne 0$ at one with $S>0$ and $U<0$.*

Proof. $F_1 + F_2 = (1+m^2)D^2 \ge 0$ gives the first claim. If $F_1 = 0$ then $SU = -m^2D^2 \le 0$, so $U \le 0$; if $F_2 = 0$ then $SU = D^2 \ge 0$, so $U \ge 0$. □

The two families of eight are therefore separated by the two lines: the u-axis solutions sit in the closed double wedge $U \le 0$ and the v-axis solutions in $U \ge 0$. A conic whose parametrisation stays strictly inside one of the two double wedges, and is regular there so that $S > 0$, contributes no solution on the corresponding bisector, so at most eight of its sixteen solutions can be real—an immediate consequence of Proposition 6.2. The pointwise half of this is formalised; the passage to "at most eight of the sixteen" is not.

Finally, a real root of F_1 is a real *circle*, not merely a real root.

Proposition 6.3. *Let θ be a real parameter with $W(\theta) \ne 0$ and $a(\theta) \ne 0$ at which the two identities $\Phi = 0$ and $a\,q_X + b\,q_Y = 0$ of Proposition 6.1 hold and $F_1(\theta) = 0$. Put $s = P/(Wa)$. Then the point $(X/W, Y/W)$ lies on the conic and on the circle of centre $(s,0)$ and squared radius $m^2s^2/(1+m^2)$, that circle and the conic have parallel gradients there, and the circle is tangent to both lines $v = \pm mu$.*

7. Controls on the checker

A certificate checker that accepts everything proves nothing. We therefore also verified, by the same exact rational computation, that the checker rejects perturbations of the data that ought to be rejected.

Proposition 7.1. *For each of the two QL^2 configurations of Section 5 the checker returns* false *on each of the following: the first certificate with its centre displaced by $2^{-30} \gg \rho$ in one coordinate; the same certificate at box radius $\rho = 2^{-4}$; the same certificate with Y replaced by the identity matrix; the certificate whose centre is the midpoint of two certified centres; and the certificate obtained from the first by replacing the contact-point coordinate u of its centre with the real part of a non-real root of the degree-16 eliminant of Section 5. Moreover the system is not the zero system: its conic equation evaluates at the origin to the constant term of Q.*

Proposition 7.2. *For the tritangent system of Theorem A the checker returns* false *on the first certificate with its centre displaced by 2^{-30}, on the same certificate at box radius 2^{-4}, and on the certificate centred at the midpoint of two certified centres; and the first conic equation of the system evaluates at the origin to* 1.

Two remarks on the fifth control. The degree-16 eliminant of each of the two configurations has exactly two non-real roots—$16-14$—so the real part of one of them is the nearest thing the elimination offers to a fifteenth circle; the checker refuses the input built from it. It is only the u-coordinate that is replaced, the remaining four coordinates being those of a certified centre, so the refused point is far from the solution variety and the refusal is comfortable rather than delicate: it fails (9) by factors $7.0 \cdot 10^{18}$ and $8.5 \cdot 10^{21}$, for the configurations of Theorems B and C respectively, against $2.9 \cdot 10^{18}$ and $1.4 \cdot 10^{19}$ for the midpoint control. This control is therefore no sharper than the midpoint one, and we claim no more for it than that the checker does not manufacture a fifteenth circle out of a non-real root. A second calibration is worth recording, about the radius control: at $\rho = 2^{-10}$ a genuine certificate still passes, correctly—a larger box is a weaker true statement—so the radius control has to be pushed to 2^{-4}, where the contraction genuinely fails.

8. What is not proved, and what it would cost

Exactly 144, exactly 14. Neither is established here. A count from above needs a bound on the number of complex solutions of a zero-dimensional system, for which we have no formal route; the refutation of a conjectured maximum needs only the lower bound. For QL^2 the obstacle is different and smaller: what is missing is an exact real-root *count* for the degree-16 eliminant. Descartes' rule alone does not deliver it here: the eliminant of Theorem C has 8 sign variations and so does its reflection, and that of Theorem B has 10 and 6, so in both cases the rule gives only ≤ 16, which the degree already gives. An isolation layer of Vincent/Alesina–Galuzzi type, or a Sturm chain, would have to be built.

$\#QL^2 \leq 14$. Together with Theorem B this would settle Fiorelli Vilmart's question. The tools of Section 6 put the two octics into a pencil that also contains $S\,U$, which has at most four real roots since S is a sum of two squares, and the perfect square $(1+m^2)D^2$. One design pass shows that neither hyperbolicity interlacing nor $F_1 + F_2 \geq 0$ yields a contradiction on its own: already in degree two, $(x+2)(x+1) + (x-1)(x-2) = 2x^2 + 4 > 0$ with both summands hyperbolic. The empirical pattern to aim at is $n_1 = 8 \Rightarrow n_2 \leq 4$, where n_1, n_2 are the numbers of real roots of F_1, F_2.

$\#QL^2 = 16$. Not found. The following is a numerical experiment, reported as evidence and not as a theorem. In the normalised two-bisector parametrisation of Section 6 we ran 1411 independent hill climbs from random integer restarts, with an exact Sturm real-root count as the objective, over three seeds and three integer ranges: 4 234 411 exact evaluations, 2.0 CPU-hours. The terminal real counts were $4, 6, 8, 10, 12$ or 14; 12 occurred 1164 times, 14 occurred 11 times, and 16 never. A further 512 restarts in the independent general-form eliminant parametrisation, and a scan of 20 000 uniformly sampled exact configurations, likewise never exceeded 14 and 12 respectively. That is 1923 independent climbs in two different coordinate systems pressing against the same ceiling. It is also the measurement behind the remark after Theorem C: a configuration with 14 occurs in 0.8% of climbs. All three of the best configurations found, one per seed, split as $n_1 + n_2 = 6 + 8$, never $8 + 6$ and never $7 + 7$.

A certified region rather than a point. Also a numerical experiment: the first-order sensitivity of the 144 solutions to relative changes of the conic coefficients reaches $2.7 \cdot 10^{17}$, and the contraction constant of Section 3 grows linearly in the half-width of a parameter box, already exceeding 1 at half-width 10^{-18}. A certificate valid on a positive-volume set of conic triples is therefore not within reach of this method, and Theorem A is a statement about one parameter point.

9. Verification

The Lean 4 development [7, 8] contains two layers. The reasoning layer—Proposition 3.1, Theorem 3.2, Lemmas 3.3 and 3.4, the assembly of many certificates into a distinctness statement, and all of Section 6—is checked by the Lean kernel from the axioms of Mathlib alone. The arithmetic layer—the finitely many rational inequalities (8) and (9), the positivity, smoothness and separation comparisons enumerated in the proofs of Theorems A, B and C, and the rejections of Section 7—is discharged by compiled evaluation inside Lean. Each such evaluation introduces one axiom, and those axioms occur among the dependencies of exactly the statements just listed and of no others. No proof uses `sorry`. So Theorems A, B and C (apart from the parenthetical in the last), Theorem 3.2, Propositions 3.1, 6.1, 6.2 and 6.3, Lemmas 3.3 and 3.4, and Propositions 7.1 and 7.2 are machine-checked in full.

Everything else asserted in this paper is exact rational arithmetic or a numerical experiment performed outside the development, and is flagged where it occurs: the discriminants computed in Section 1 and the identification of ℓ_1, ℓ_2 in Theorem B with the axes of (2); the reproduction of the p_{144} vector of [3] in the proof of Theorem A; the parenthetical in Theorem C; the margin figures reported in the proofs of Sections 4 and 5; the eliminant, sign-variation and homotopy computations of Sections 5 and 8; Remark 5.1; the passage from Proposition 6.2 to "at most eight of the sixteen" after it; the calibration figures of Section 7; and the searches and sensitivity figures of Section 8. None of them is used in the proof of any theorem above. Repository reference to be added at submission.

References

[1] P. Breiding, J. Lindberg, W. J. G. Ong, L. Sommer, *Real circles tangent to 3 conics*, Le Matematiche **78** (2023), no. 1, 149–175; `doi:10.4418/2023.78.1.5`, `arXiv:2211.06876`.

[2] P. Breiding, K. Rose, S. Timme, *Certifying zeros of polynomial systems using interval arithmetic*, ACM Trans. Math. Software **49** (2023), no. 1, article 11, 14 pp.; `doi:10.1145/3580277`, `arXiv:2011.05000`.

[3] T. Brysiewicz, *144 real circles tangent to three conics*, `arXiv:2609.01521v1` (submitted 1 September 2026). Still `v1` and unpublished when this paper was written; all numbered references above are to that version.

[4] I. Z. Emiris, G. M. Tzoumas, *Algebraic study of the Apollonius circle of three ellipses*, Proc. European Workshop on Computational Geometry (EWCG), Eindhoven, March 9–11, 2005, 147–150.

[5] S. Fiorelli Vilmart, *Étude de cercles tangents à des coniques*, thèse de doctorat no. Sc. 4160, Université de Genève, 2009; `doi:10.13097/archive-ouverte/unige:5152`.

[6] R. Krawczyk, *Newton-Algorithmen zur Bestimmung von Nullstellen mit Fehlerschranken*, Computing **4** (1969), no. 3, 187–201; `doi:10.1007/BF02234767`.

[7] L. de Moura, S. Ullrich, *The Lean 4 theorem prover and programming language*, Automated Deduction — CADE-28, Lecture Notes in Computer Science **12699**, Springer, 2021, 625–635.

[8] The mathlib Community, *The Lean mathematical library*, Proc. 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), 367–381.

[9] F. Ronga, A. Tognoli, T. Vust, *The number of conics tangent to five given conics: the real case*, Rev. Mat. Univ. Complut. Madrid **10** (1997), no. 2, 391–421.