SIX NEW REALIZABLE TRIPLES OF TOTALLY, PARTIALLY AND MINIMALLY REAL COMMON SECANTS TO A PAIR OF REAL TWISTED CUBICS

KOREA SUPERINTELLIGENCE LABS

Abstract. A general pair of twisted cubic curves in $\mathbb{P}^3(\mathbb{C})$ has ten common secant lines. For a real pair each real common secant is *totally*, *partially* or *minimally* real according to whether it meets the two curves in two real points each, in two real points and a conjugate pair, or in a conjugate pair each; the resulting count (n_t, n_p, n_m) takes 161 admissible values. Aslam, Faust, Hauenstein, Lopez Garcia, Kagy, Regan, Wampler and Zhang recently realized 128 of the 161 by numerical sampling with certification, listed the remaining 33, and asked for the full realizable set. We realize six of the 33: $(4, 6, 0)$, $(4, 5, 1)$, $(4, 4, 2)$, $(3, 5, 2)$, $(3, 7, 0)$ and $(2, 8, 0)$, each by an explicit pair of *rational* twisted cubics given by a 4×4 integer matrix. The certificate is exact rather than numerical: elimination reduces the common-secant system of one pair to a single degree-10 integer polynomial together with a rational univariate representation, and the ten secants and their types are then read off ten integer sign changes and twenty Descartes sign-pattern certificates over $\mathbb{Z}$. Every step is checked by the Lean 4 kernel in arbitrary-precision integer arithmetic; no floating point and no compiled evaluation enters any proof. We also record an erratum to the printed bisecant system of the source, which does not affect any of its conclusions, and report the negative side of our search over roughly 470 000 classified pairs.

1. Introduction

1.1. **Ten common secants.** A *twisted cubic* is a smooth rational curve of degree three in $\mathbb{P}^3$. The standard one is the closure of the image of

$$v(t) = (1, t, t^2, t^3), \qquad C_0 = \{[v(t)] : t \in \mathbb{C}\} \cup \{[0 : 0 : 0 : 1]\},$$

and every twisted cubic is $M \cdot C_0$ for some $M \in \mathrm{PGL}_4$. A *secant* of a curve is a line meeting it in a scheme of length two. That a general pair of twisted cubics in $\mathbb{P}^3(\mathbb{C})$ has exactly ten common secant lines is classical: it is Keynote Question (c) of Chapter 3 of Eisenbud and Harris [3], and it is Theorem 1.2 of [1], which obtains it by Schubert calculus as a consequence of [3, Prop. 3.14].

1.2. **The real refinement.** Now let both curves be real. A common secant line is then either nonreal — and then it occurs in a conjugate pair — or real, and a real common secant meets each of the two curves in a pair of points that is either two real points or a conjugate pair. Following Proposition 2.3 of [1], a real common secant is

- *totally real* if it meets each curve in two real points;

Date: August 31, 2026.

- *partially real* if it meets one curve in two real points and the other in a conjugate pair;
- *minimally real* if it meets each curve in a conjugate pair.

Write (n_t, n_p, n_m) for the three counts and $n_{\mathbb{R}} = n_t + n_p + n_m$ for the number of real common secants. Nonreal common secants come in conjugate pairs, so their number is even; as there are ten common secants in all, $n_{\mathbb{R}}$ is even and $n_{\mathbb{R}} \leq 10$. These are the only constraints, and there are consequently $\sum_{k\in\{0,2,4,6,8,10\}} \binom{k+2}{2} = 1 + 6 + 15 + 28 + 45 + 66 = 161$ *admissible* 3-tuples (Proposition 2.5 of [1]). An admissible 3-tuple is *realizable* if some pair of real twisted cubics attains it.

1.3. **The source and its open question.** Which admissible 3-tuples are realizable is the question raised and attacked in [1]. That paper samples the parameter space of real twisted cubic curves — uniformly in $\mathbb{P}^{15}(\mathbb{R})$, in the 4×4 matrix coordinates of its Algorithm 1 — tracks solutions with Bertini [4] and certifies the resulting approximate solutions with `alphaCertified` [5]; the proof of its Theorem 1.7 reports that "this process generated parameters for 128 out of the 161 admissible 3-tuples". Its Table 4 accordingly splits the 161 into 128 *realized* and 33 *admissible and not realized*, and its Problem 5.1 opens

> Determine the full set of realizable 3-tuples in Table 4.

The 33 unrealized 3-tuples are

$$(0, n_p, 10 - n_p) \;\; (0 \leq n_p \leq 10), \qquad (1, n_p, 9 - n_p) \;\; (0 \leq n_p \leq 9),$$
$$(1,0,7),\ (1,1,6), \quad (2,6,2),\ (2,7,1),\ (2,8,0), \quad (3,5,2),\ (3,6,1),\ (3,7,0),$$
$$(4,0,6),\ (4,4,2),\ (4,5,1),\ (4,6,0),$$

21 of them belonging to the two families singled out in Remark 1.8 of [1], which states that it "remains an open problem whether the admissible 3-tuples of the form $(0, n_p, 10 - n_p)$ for $0 \leq n_p \leq 10$ and $(1, n_p, 9 - n_p)$ for $0 \leq n_p \leq 9$ are realizable". The other twelve are the two with $n_{\mathbb{R}} = 8$ and the ten with $n_{\mathbb{R}} = 10$ and $n_t \leq 4$.

The main theorem of [1], its Theorem 1.7, states a sufficient condition: an admissible 3-tuple is realizable whenever

$$n_{\mathbb{R}} \in \{0, 2, 4, 6\}, \quad \text{or} \quad n_{\mathbb{R}} = 8 \text{ and } n_t \neq 1, \quad \text{or} \quad n_{\mathbb{R}} = 10 \text{ and } n_t \in \{5, 6, 7, 8, 9, 10\}.$$

That condition holds for 108 of the 161 admissible 3-tuples, whereas Table 4 records 128 as realized. The two counts do not conflict: the 108 are a subset of the 128, and the twenty further cells — the six with $n_{\mathbb{R}} = 8$ and $n_t = 1$, and the fourteen with $n_{\mathbb{R}} = 10$ and $n_t \in \{2, 3, 4\}$ — are the "partial results" for $n_{\mathbb{R}} \in \{8, 10\}$ that Remark 1.8 of [1] points to in the same breath as the two open families, recorded in Table 4 but left out of the clean statement of the theorem. The finer information, and the source of the list of 33, is therefore Table 4 rather than Theorem 1.7, and it is Table 4 that the results below act on.

1.4. **Results.** We settle six of the 33 cells, all of them with $n_{\mathbb{R}} = 10$.

(i) *Six new realizable 3-tuples* (Section 5). Each of

$$(4,6,0), \quad (4,5,1), \quad (4,4,2), \quad (3,5,2), \quad (3,7,0), \quad (2,8,0)$$

is realizable, by an explicit pair C_0, $M \cdot C_0$ of *rational* twisted cubics with M an integer 4×4 matrix (Theorems 7–12). All six are printed in the "admissible and not realized" column of Table 4 of [1] and are among the twelve unrealized cells outside the two families of its Remark 1.8. This reduces the unrealized list from 33 to 27 and leaves, outside those two families, $(1,0,7)$, $(1,1,6)$, $(2,6,2)$, $(2,7,1)$, $(3,6,1)$ and $(4,0,6)$. The certified data behind the 128 realizations of [1] live in a public repository [2], which we have not consulted; what is claimed here is therefore that these six cells are not realized in `arXiv:2603.25003v1` and that we have found no later work realizing them.

(ii) *An exact certificate in place of a numerical one* (Sections 2–4). For a pair of rational twisted cubics the ten common secants and their three types are decided by finitely many integer facts: ten sign changes of one degree-10 integer polynomial, four polynomial identities over $\mathbb{Z}$, and twenty Descartes sign-pattern certificates. Nothing approximate enters. The same machinery run on the already realized cell $(7,2,1)$ reproduces it (Theorem 14) and serves as a control on the whole construction.

(iii) *An erratum to the printed bisecant system* (Remark 2). The displayed system of [1], its equation (6), prints $f_2 = p_4 - (t_1^2 + 2t_1t_2 + t_2^2)p_2 + t_1t_2p_1$, where the 3×3 minor it is derived from gives $f_2 = p_4 - (t_1^2 + t_1t_2 + t_2^2)p_2 + t_1t_2(t_1+t_2)p_1$. The error is confined to the printed equation; the computations of [1] are made with the correct system.

(iv) *What the search did not reach* (Section 7). Two further cells, $(1,1,6)$ and $(1,0,7)$, were reached by the search but are reported here only as measurements, since their type classification was not certified. Across roughly 470 000 exactly classified pairs, no pair with $n_{\mathbb{R}} = 10$ and $n_t \le 1$ was ever seen, and none with $(n_t, n_p) = (4,0)$. We are explicit that this is a report about a search and not evidence about realizability.

1.5. **What rests on computation.** The realizability statements below are proved from finitely many exact integer facts, each checked by the kernel of the Lean 4 proof assistant on arbitrary-precision integers. The facts are of three shapes only: the sign of an integer polynomial at an integer argument; the sign pattern of the coefficient list of a Möbius-transformed integer polynomial; and an identity between two integer polynomials. There are 308 of them, 44 per configuration. No floating-point arithmetic and no compiled evaluation occurs in any proof.

Three things are *not* part of that formal development, and we name them once here. First, the elementary translation between geometry and algebra of Section 2 — Lemma 1 and Proposition 3, two short pieces of linear algebra — which turns "the line through two points of C_0 meets C_1 twice" into the divisibility conditions the certificates decide. Second, the count of ten common secants: the classical count is for a *general* pair, and of each of the seven explicit pairs below we assume, as [1] does of its own parameter points, that the certified ten are all of them (Convention 4). Third, the *elimination* of Section 3: the passage from a matrix to the degree-10 polynomial and its rational univariate representation was carried out in exact rational arithmetic in PARI/GP [9] and is a search device, not a step of any proof — what the proofs use is only its output, and only through four polynomial identities over $\mathbb{Z}$ that the kernel checks directly. Likewise, the matrices themselves were found by a directed search (Section 7) whose conduct is irrelevant to the validity of the certificates it produced.

2. The common-secant system

Throughout, M is an invertible real 4×4 matrix, C_0 is the standard twisted cubic above and $C_1 = M \cdot C_0$. Write

$$p_i(s) = M_{i1} + M_{i2}s + M_{i3}s^2 + M_{i4}s^3 \qquad (1 \le i \le 4),$$

so that $Mv(s) = (p_1(s), p_2(s), p_3(s), p_4(s))$.

Lemma 1. *Let $t_1 \neq t_2$ and $w \in \mathbb{C}^4$. Then $[w]$ lies on the line through $[v(t_1)]$ and $[v(t_2)]$ if and only if the two 3×3 minors of the matrix $\big(v(t_1) \mid v(t_2) \mid w\big)$ taken on rows $\{1, 2, 3\}$ and on rows $\{1, 2, 4\}$ both vanish.*

Proof. The 2×2 minor of the first two columns on rows $1, 2$ is $t_2 - t_1 \neq 0$, so there are unique λ, μ with $w - \lambda v(t_1) - \mu v(t_2) = r$ having $r_1 = r_2 = 0$. Subtracting multiples of the first two columns from the third leaves the minor on rows $\{1, 2, k\}$ equal to $r_k\,(t_2 - t_1)$ for $k = 3, 4$. Both vanish precisely when $r_3 = r_4 = 0$, that is, when $w \in \langle v(t_1), v(t_2)\rangle$. $\square$

Expanding those two minors along the third column and dividing by $t_2 - t_1$ gives, with $e_1 = t_1 + t_2$ and $e_2 = t_1t_2$,

$$\begin{aligned} g_1(s) &= p_3(s) - e_1\, p_2(s) + e_2\, p_1(s), \\ g_2(s) &= p_4(s) - (e_1^2 - e_2)\, p_2(s) + e_1e_2\, p_1(s), \end{aligned} \tag{1}$$

using $t_1^2 + t_1t_2 + t_2^2 = e_1^2 - e_2$ and $t_1t_2(t_1 + t_2) = e_1e_2$. Both are cubics in s whose coefficients are polynomial in (e_1, e_2); the pair $\{t_1, t_2\}$ enters only through e_1, e_2.

Remark 2. An erratum to [1], established by the computation just made and outside the formal development below. The bisecant system of [1] — its displayed equation (6), and the unnumbered display of f_1, f_2 that immediately precedes it — prints

$$f_1 = p_3 - (t_1 + t_2)p_2 + t_1t_2p_1, \qquad f_2 = p_4 - (t_1^2 + 2t_1t_2 + t_2^2)p_2 + t_1t_2p_1.$$

The first agrees with g_1. The second does not agree with g_2: expanding the minor on rows $\{1, 2, 4\}$ of $\big(v(t_1) \mid v(t_2) \mid Mv(s)\big)$ gives

$$p_1\, t_1t_2(t_2^2 - t_1^2) - p_2\,(t_2^3 - t_1^3) + p_4\,(t_2 - t_1),$$

and division by $t_2 - t_1$ leaves $p_4 - (t_1^2 + t_1t_2 + t_2^2)p_2 + t_1t_2(t_1 + t_2)p_1$, so the printed coefficient of p_2 should have t_1t_2 in place of $2t_1t_2$ and the printed coefficient of p_1 should carry the extra factor $t_1 + t_2$. The ten solutions printed in the worked example of [1] — its Example 2.4, one representative (t_1, t_2, s_1, s_2) from each of the ten orbits, to four decimal places — satisfy the corrected equation to the accuracy of those four decimals and do not satisfy the printed one. The twenty residuals $f_2(t_1, t_2, s_i)$ of the corrected form are all below $1.3 \cdot 10^{-2}$, on the scale set by the twenty residuals of the printed f_1, which the same computation puts below $6 \cdot 10^{-3}$; the residuals of the printed f_2 run from $2.5 \cdot 10^{-2}$ to 54.9. So this is a transcription slip in the displayed equation and not an error in the computations of [1], all of whose conclusions stand.

Proposition 3. *Let $e_1, e_2, u_1, u_2 \in \mathbb{R}$ satisfy $\delta_t := e_1^2 - 4e_2 \neq 0$ and $\delta_s := u_1^2 - 4u_2 \neq 0$, and let t_1, t_2 be the roots of $X^2 - e_1X + e_2$ and s_1, s_2 those of $X^2 - u_1X + u_2$. Then the line ℓ through $[v(t_1)]$ and $[v(t_2)]$ is a real common secant of C_0 and C_1, meeting*

C_0 in $[v(t_1)], [v(t_2)]$ and C_1 in $[Mv(s_1)], [Mv(s_2)]$, if and only if $X^2 - u_1X + u_2$ divides both g_1 and g_2 in $\mathbb{C}[X]$. Its type is

$$\textit{totally real if } \delta_t > 0 \textit{ and } \delta_s > 0; \qquad \textit{partially real if } \delta_t\delta_s < 0;$$
$$\textit{minimally real if } \delta_t < 0 \textit{ and } \delta_s < 0.$$

Proof. Since $\delta_t \neq 0$ we have $t_1 \neq t_2$, so ℓ is well defined and, the set $\{t_1, t_2\}$ being stable under conjugation, ℓ is a real line meeting C_0 in the two distinct points $[v(t_1)], [v(t_2)]$. Since $\delta_s \neq 0$ we have $s_1 \neq s_2$, so $[Mv(s_1)] \neq [Mv(s_2)]$ are two distinct points of C_1. By Lemma 1, $[Mv(s_i)] \in \ell$ for $i = 1, 2$ if and only if $g_1(s_i) = g_2(s_i) = 0$ for $i = 1, 2$, that is, if and only if $X^2 - u_1X + u_2$ divides g_1 and g_2. The type is the reality of the two pairs, which is the sign of the two discriminants. □

Written out on coefficients, divisibility of a cubic $a_0 + a_1X + a_2X^2 + a_3X^3$ by $X^2 - u_1X + u_2$ is the vanishing of the two entries of its remainder,

$$a_1 + a_2u_1 + a_3(u_1^2 - u_2) = 0, \qquad a_0 - u_2(a_2 + a_3u_1) = 0. \tag{2}$$

Applying (2) to g_1 and to g_2 gives four equations in (e_1, e_2, u_1, u_2); we call them *the common-secant system* of M and denote it $\mathrm{Sys}(M)$. This is the system of [1] with t_1, t_2 replaced by their elementary symmetric functions, and Proposition 3 is its Proposition 2.3 in that form.

Convention 4. Realizability of a 3-tuple, in the sense of [1], asks for a pair of real twisted cubics having *ten* common secant lines split as prescribed. What is classical, and what [1, Thm. 1.2] states on the strength of [3, Ch. 3, Keynote Question (c) and Prop. 3.14], is the count of ten for a *general* pair; neither reference bounds the number of distinct common secants of a *special* pair, and we prove no such bound here. We therefore proceed exactly as [1] does when it reads a 3-tuple off ten certified solutions at one explicit parameter point, stating the step rather than leaving it implicit:

> for each of the seven explicit pairs below, we *assume* that the ten common secants the certificates exhibit are all of the common secants of that pair.

This is the second of the three inputs named in Section 1.5, and it is the only thing carrying the final clause of each theorem below, "the pair realizes (n_t, n_p, n_m)". Everything before that clause is unconditional and kernel-checked: the ten lines exist, are pairwise distinct, are common secants of C_0 and C_1, and have the stated types. The elimination of Section 3 is evidence for the assumption — it returns, for each of the seven pairs, a nonzero integer polynomial of degree 10 whose ten roots are simple, real, and exactly the ten certified secants — but it is a computation outside the formal development, made in the chart in which both parameters of the intersection with C_0 are finite, and we do not offer it as a proof.

3. Elimination and a rational univariate representation

Fix now an integer matrix M with $\det M \neq 0$, so that C_0 and $C_1 = M \cdot C_0$ are rational twisted cubics. Put $z = -e_1$. Eliminating e_2, u_1, u_2 from $\mathrm{Sys}(M)$ — through the Plücker, rank-one description of the chordal surface of C_0 — leaves a polynomial of degree 12 in z. Two of its roots are extraneous and equal: the Plücker equations vanish to order two along the unique chord of C_0 through the point $[Me_4]$, where $e_4 = (0,0,0,1)$ — the point of C_1 at parameter $s = \infty$ — and that chord is available in closed form, so the double factor is divided out exactly and there remains a single polynomial

$$E \in \mathbb{Z}[z], \qquad \deg E = 10,$$

together with integer polynomials D, C_e, A_1, A_2 and the *rational univariate representation*

$$(3) \qquad e_1 = -z, \qquad e_2 = \frac{C_e(z)}{D(z)}, \qquad u_1 = \frac{A_1(z)}{D(z)}, \qquad u_2 = \frac{A_2(z)}{D(z)},$$

valid on the zero set of E. Here $D = W \cdot E'$ for an integer constant W; taking the derivative of E rather than a cleared integer denominator costs nothing and is worth about a factor of five in coefficient size. For the seven matrices below, $\deg D = 9$ and the coefficients of E and D run to 54 and 61 decimal digits respectively.

This computation was performed in exact rational arithmetic in PARI/GP. It plays no role in any proof. What is used is that the four equations of $\mathrm{Sys}(M)$, after substituting (3) and clearing the denominator D^3, become four integer polynomials $N_1, \ldots, N_4$ in z of degrees $28, 28, 29, 29$, and that these are multiples of E:

$$(4) \qquad E \cdot H_i = N_i \quad \text{in } \mathbb{Z}[z], \qquad i = 1,2,3,4,$$

for explicit cofactors $H_i \in \mathbb{Z}[z]$. The four identities (4) are verified coefficient by coefficient; their coefficients reach 197 decimal digits.

Finally the two discriminants of Proposition 3 are, on the zero set of E, the signs of two integer polynomials. From (3),

$$(5) \quad (e_1^2 - 4e_2)\, D^2 = P_t := D \cdot (z^2 D - 4C_e), \qquad (u_1^2 - 4u_2)\, D^2 = P_s := A_1^2 - 4A_2 D.$$

The polynomials P_t and P_s have degrees 20 and 18. The correcting factor D^2 is positive wherever it is nonzero, so P_t and P_s carry the signs of δ_t and δ_s respectively; and $P_t \neq 0$ forces $D \neq 0$, so no separate non-vanishing certificate for the denominator is needed.

Conditioning. Write $\Delta_K = \mathrm{diag}(1, K, K^2, K^3)$. Since $\Delta_K\, v(t) = v(Kt)$, the projective transformation Δ_K fixes C_0 setwise and multiplies its parameter by K. Replacing M by $\Delta_K M$ replaces the pair (C_0, C_1) by its image under that transformation, so leaves (n_t, n_p, n_m) unchanged, while scaling the roots of E by K. Each configuration below carries the $K \in \{50, 200, 1000\}$ that separates the ten real roots of E into ten *disjoint unit windows* with integer endpoints. Unit windows are not a convenience: on the wider windows obtained by splitting at midpoints, the Descartes certificates of the next section fail at every K we tried.

4. Certificates

The certificate layer used here is not new and is not a contribution of this paper: it is a small apparatus for isolating real roots of an integer polynomial given as a coefficient list, written for an unrelated real-root problem — the growth-factor polynomials of Chen, Edelman and Urschel [6] — and imported unchanged. We describe only what is needed to read the proofs.

A polynomial is carried as its list of coefficients in ascending order, and sums, products, negation and evaluation at an integer are the evident list operations. For integers $a < b$ the substitution $x = (a + bt)/(1 + t)$ is an increasing bijection

$(0,\infty) \to (a,b)$; multiplying by $(1+t)^N$, where N is the length of the list, clears denominators and leaves an integer coefficient list $T_{a,b}\,p$ with

$$(T_{a,b}\,p)(t) = (1+t)^N\, p\left(\frac{a+bt}{1+t}\right) \qquad (t>0), \tag{6}$$

a positive multiple of $p(x)$ at the corresponding x. Say that p satisfies $\mathrm{Pos}(a,b)$ if every coefficient of $T_{a,b}\,p$ is ≥ 0 and at least one is > 0. A list with nonnegative coefficients, one of them positive, is positive at every $t>0$, so by (6):

Lemma 5. *If p satisfies $\mathrm{Pos}(a,b)$ then $p(x)>0$ for all $x\in(a,b)$; if $-p$ satisfies $\mathrm{Pos}(a,b)$ then $p(x)<0$ for all $x\in(a,b)$.*

Everything now assembles into a single lemma, one application of which produces one certified common secant of one prescribed type.

Lemma 6 (window lemma)**.** *Let M be an integer matrix as above, with associated polynomials E, D, C_e, A_1, A_2, $H_1,\dots,H_4$ and P_t, P_s as in Section 3, and suppose the four identities (4) hold. Let $a<b$ be integers, let $\varepsilon_t,\varepsilon_s\in\{+1,-1\}$, and suppose*

1. *$E(a)$ and $E(b)$ are nonzero of opposite signs, and*
2. *$\varepsilon_t P_t$ and $\varepsilon_s P_s$ both satisfy $\mathrm{Pos}(a,b)$.*

Then there is $x\in(a,b)$ with $E(x)=0$, and for any such x the quadruple (3) evaluated at $z=x$ is a real solution of $\mathrm{Sys}(M)$ with $\operatorname{sign}\delta_t=\varepsilon_t$ and $\operatorname{sign}\delta_s=\varepsilon_s$. It therefore determines, by Proposition 3, a real common secant of C_0 and $C_1=M\cdot C_0$ that meets C_0 in the two points with parameter sum $e_1=-x$, and whose type is totally, partially or minimally real according to $(\varepsilon_t,\varepsilon_s)$ being $(+,+)$, of mixed sign, or $(-,-)$.

Proof. Existence of x is the intermediate value theorem applied to the polynomial function E on $[a,b]$. By Lemma 5, $\varepsilon_t P_t(x)>0$ and $\varepsilon_s P_s(x)>0$; in particular $P_t(x)\neq 0$, whence $D(x)\neq 0$ by (5), so (3) is defined at x. From (4) and $E(x)=0$ we get $N_i(x)=0$ for $i=1,\dots,4$; dividing by $D(x)^3\neq 0$ turns these into the four equations of $\mathrm{Sys}(M)$ at the quadruple (3). Finally $D(x)^2>0$, so by (5) the signs of δ_t,δ_s at that quadruple are those of $P_t(x),P_s(x)$, namely $\varepsilon_t,\varepsilon_s$; both are nonzero, so Proposition 3 applies. □

Applying Lemma 6 on ten disjoint windows $(a_0,a_0+1),\dots,(a_9,a_9+1)$ with $a_0<a_0+1\leq a_1<\dots$ yields ten roots $x_0<x_1<\dots<x_9$ of E, hence ten distinct values $e_1=-x_j$, hence ten common secants with pairwise distinct intersection divisors on C_0 — and two distinct lines cannot meet C_0 in the same pair of points, so the ten lines are pairwise distinct. The hypotheses consumed are 44 integer facts: the four identities (4), twenty evaluations of E at integer endpoints, and twenty Pos certificates.

5. Six new realizable triples

The seven configurations are recorded in Table 1. Each is an integer matrix $M=\mathrm{diag}(1,K,K^2,K^3)\,M_0$ with M_0 small, and $\det M_0\neq 0$ is displayed so that invertibility — and hence the fact that $C_1=M\cdot C_0$ is a twisted cubic — can be checked by inspection. Table 2 records the corresponding ten windows.

In each of the six theorems below and in Theorem 14, the existence of ten pairwise distinct common secants of the stated types is certified outright; the last clause,

	(n_t, n_p, n_m)	K	$\det M_0$	M_0
A	$(7,2,1)$	50	91	$\begin{pmatrix} 4 & -5 & 0 & 5 \\ -4 & 2 & -1 & -2 \\ 5 & 5 & 3 & -4 \\ -5 & 0 & 1 & 6 \end{pmatrix}$
B	$(4,6,0)$	50	-63852	$\begin{pmatrix} 4 & 9 & -7 & -17 \\ 6 & -2 & -11 & 5 \\ -16 & 21 & 1 & -13 \\ -30 & 7 & -6 & 11 \end{pmatrix}$
C	$(4,5,1)$	200	153014	$\begin{pmatrix} 2 & -2 & 1 & -21 \\ -7 & 21 & -20 & -14 \\ 10 & -8 & -11 & -7 \\ -9 & -13 & 0 & 5 \end{pmatrix}$
D	$(4,4,2)$	1000	105780	$\begin{pmatrix} 3 & -4 & -1 & -19 \\ -7 & 17 & -18 & -15 \\ 10 & -8 & -10 & -6 \\ -11 & -9 & 1 & 5 \end{pmatrix}$
E	$(3,5,2)$	1000	108848	$\begin{pmatrix} 2 & -4 & 0 & -19 \\ -7 & 15 & -17 & -15 \\ 10 & -8 & -11 & -6 \\ -11 & -9 & 1 & 5 \end{pmatrix}$
F	$(3,7,0)$	1000	-82272	$\begin{pmatrix} 4 & 6 & -7 & -14 \\ 5 & -3 & -10 & 10 \\ -18 & 24 & 2 & -11 \\ -27 & 7 & -5 & 12 \end{pmatrix}$
G	$(2,8,0)$	1000	-79699	$\begin{pmatrix} 4 & 8 & -6 & -17 \\ 6 & -2 & -9 & 5 \\ -16 & 23 & 1 & -12 \\ -31 & 8 & -7 & 10 \end{pmatrix}$

TABLE 1. The seven configurations. The matrix of the pair is $M = \operatorname{diag}(1, K, K^2, K^3)\, M_0$ and the pair is C_0, $M \cdot C_0$.

A	-2155^p, -955^t, -573^t, -268^t, -173^t, -97^p, -6^m, 118^t, 142^t, 161^t
B	-365^p, -227^t, -153^p, -138^p, -124^t, -33^p, 15^p, 33^t, 50^p, 85422^t
C	-3175^p, -488^p, -76^t, -11^m, 124^p, 147^p, 346^t, 385^t, 515^t, 1193^p
D	-20202^p, -1483^p, -200^t, 68^m, 460^m, 1150^t, 1330^p, 1550^t, 2247^t, 5478^p
E	-6702^p, -1541^p, -218^t, 35^m, 606^p, 1251^p, 1518^t, 1572^p, 1829^t, 4564^m
F	-25740^p, -9333^t, -2571^p, -2471^p, -1764^t, -283^p, 344^p, 1035^t, 1253^p, 1368^p
G	-10646^t, -2574^t, -2462^p, -2071^p, -549^p, 563^p, 607^p, 1882^p, 2157^p, 44478^p

TABLE 2. The ten windows of each configuration. An entry a^τ means that the window is $(a, a+1)$ and that the secant it produces is totally ($\tau = t$), partially ($\tau = p$) or minimally ($\tau = m$) real. The windows are listed in increasing order and are pairwise disjoint; the corresponding secant meets C_0 in the two points whose parameters have sum $e_1 \in (-a-1, -a)$.

that the pair *realizes* the 3-tuple, is the one that invokes Convention 4, namely that these ten are all the common secants of the pair.

Theorem 7. *Let M be the matrix of configuration B of Table 1. Then C_0 and $M \cdot C_0$ are real twisted cubics having ten pairwise distinct common secant lines, four of them totally real and six partially real; the pair realizes $(4,6,0)$, so the 3-tuple $(4,6,0)$ is realizable.*

Theorem 8. *Let M be the matrix of configuration C of Table 1. Then C_0 and $M \cdot C_0$ have ten pairwise distinct common secant lines, four totally real, five partially real and one minimally real; the pair realizes $(4,5,1)$, so that 3-tuple is realizable.*

Theorem 9. *Let M be the matrix of configuration D of Table 1. Then C_0 and $M \cdot C_0$ have ten pairwise distinct common secant lines, four totally real, four partially real and two minimally real; the pair realizes $(4,4,2)$, so that 3-tuple is realizable.*

Theorem 10. *Let M be the matrix of configuration E of Table 1. Then C_0 and $M\cdot C_0$ have ten pairwise distinct common secant lines, three totally real, five partially real and two minimally real; the pair realizes $(3,5,2)$, so that 3-tuple is realizable.*

Theorem 11. *Let M be the matrix of configuration F of Table 1. Then C_0 and $M\cdot C_0$ have ten pairwise distinct common secant lines, three totally real and seven partially real; the pair realizes $(3,7,0)$, so that 3-tuple is realizable.*

Theorem 12. *Let M be the matrix of configuration G of Table 1. Then C_0 and $M\cdot C_0$ have ten pairwise distinct common secant lines, two totally real and eight partially real; the pair realizes $(2,8,0)$, so that 3-tuple is realizable.*

Proof of Theorems 7–12. Identical in each case. Fix the configuration. Its matrix M is integral with $\det M = K^6 \det M_0 \neq 0$, so $C_1 = M\cdot C_0$ is a twisted cubic, real because M is real. The four identities (4) for M are checked coefficient by coefficient over $\mathbb{Z}$; this is one exhaustive comparison of two integer coefficient lists of degree 28 or 29 per identity, four in all. For each of the ten windows $(a, a+1)$ of Table 2 we then check four integer facts: the signs of $E(a)$ and $E(a+1)$, which are opposite, and the two $\mathrm{Pos}(a, a+1)$ certificates for $\varepsilon_t P_t$ and $\varepsilon_s P_s$, with $(\varepsilon_t, \varepsilon_s)$ determined by the type marked in Table 2: $(+,+)$ for t, $(-,-)$ for m, and $(+,-)$ or $(-,+)$ for p. Each such check is the sign pattern of a single integer coefficient list. Lemma 6 then gives, for each window, a common secant of the marked type meeting C_0 in the two points whose parameters sum to $e_1 \in (-a-1, -a)$. The ten windows are disjoint, so the ten values of e_1 are distinct, so the ten secants are pairwise distinct. Counting the marks in the row of Table 2 gives the stated numbers of totally and partially real secants. By Convention 4 these ten are all the common secants of the pair, so the remaining count n_m is 10 minus the two others, and the pair realizes the 3-tuple.

There is no case analysis and no search inside the proof: the windows and the signs $\varepsilon_t, \varepsilon_s$ are data, and the whole finite check for one configuration is the 44 integer facts listed above. All 308 of them, over the seven configurations, are checked by the Lean 4 kernel; see Section 8. □

Remark 13. The certificates also show that none of the seventy secants is tangent to either curve and that none of the pairs of intersection points degenerates: on every window both P_t and P_s are certified of one strict sign, so both discriminants are nonzero, and each secant meets each of the two curves in two distinct points.

6. The control configuration

Configuration A realizes $(7,2,1)$, which is already in the realized column of Table 4 of [1]. We state it because it is the control on the entire construction: the same code path, run on a cell whose realizability is known, must reproduce it, and does.

Theorem 14. *Let M be the matrix of configuration A of Table 1. Then C_0 and $M\cdot C_0$ have ten pairwise distinct common secant lines, seven totally real, two partially real and one minimally real; the pair realizes $(7,2,1)$.*

Proof. Word for word the proof of Theorems 7–12, with the row A of Table 2. □

Three further controls were run outside the certified development and are reported here as computations, not as theorems. First, three of the eleven examples of [1] that print an exact parameter matrix: its Example 2.4 and its Examples 4.9 and 4.10, whose 3-tuples are stated there as $(10, 0, 0)$, $(1, 0, 3)$ and $(0, 0, 0)$. Taking each printed matrix as an exact rational one and rebuilding from the definitions of Section 2, the elimination returns a degree-10 polynomial and those same three 3-tuples. Second, the distribution of $n_{\mathbb{R}}$ over 20 000 uniformly sampled integer matrices with entries in $[-12, 12]$, exactly classified, is

$$n_{\mathbb{R}} = 0, 2, 4, 6, 8, 10: \qquad 2185,\ 11367,\ 5378,\ 918,\ 100,\ 9$$
$$(10.9\%,\ 56.8\%,\ 26.9\%,\ 4.6\%,\ 0.50\%,\ 0.045\% \text{ of the } 20\,000),$$

the remaining 43 samples being matrices on which the elimination degenerates and which were discarded. Figure 5 of [1] reports the distribution of the same quantity over 100 000 parameter points sampled uniformly in $\mathbb{P}^{15}(\mathbb{R})$, with bin counts 10 620, 55 741, 27 979, 4 940, 660, 60, that is 10.6%, 55.7%, 28.0%, 4.9%, 0.66%, 0.060%. The two agree bin by bin to about one percentage point. They are not the same experiment — integer matrices with bounded entries are not uniform in $\mathbb{P}^{15}(\mathbb{R})$ — so the agreement is a coarse consistency check on the classifier and not a statistical test. Third, a geometric check bypassing the whole Plücker route: for each of the seventy secants, the four points $v(t_1)$, $v(t_2)$, $Mv(s_1)$, $Mv(s_2)$ of $\mathbb{P}^3(\mathbb{C})$ were formed in floating point at a working precision of 77 significant decimal digits from (3), and all sixteen 3×3 minors of the 4×4 matrix they span were evaluated after normalising each point by its largest coordinate. Every one of those 1120 minors vanished to the working precision, the largest in modulus being below $3 \cdot 10^{-77}$; and counting the reality of the four points directly returns the 3-tuples of Table 1. The Plücker route and the four-point definition of a common secant therefore agree.

7. The search, and what it did not reach

Nothing in this section is a theorem; it is a report on how the matrices of Table 1 were found, and on where the same instrument stopped.

Uniform sampling does not reach these cells. In the 20 000-sample experiment above, $n_{\mathbb{R}} = 10$ occurred nine times, and every uniformly sampled pair with $n_{\mathbb{R}} = 10$ that we recorded had $n_t \geq 7$. What worked is a directed walk across the walls of the classification. Across a codimension-one wall a real intersection pair collides and becomes a conjugate pair, so (n_t, n_p, n_m) can only change by $(-1, +1, 0)$ or $(0, -1, +1)$, or by ± 2 in one coordinate when a pair of real secants becomes nonreal. Annealing on

$$d(v, u) = |v_t - u_t| + |v_m - u_m| + 3\,|n_{\mathbb{R}}(v) - n_{\mathbb{R}}(u)|,$$

with perturbations of one to three matrix entries by a few parts per thousand of $\max|M_{ij}|$ per step, therefore walks the lattice of 3-tuples directly. Each proposal costs one exact classification, 1.5 to 3.5 milliseconds in PARI/GP. The run that produced Table 1 consisted of fourteen chases of 20 000 to 60 000 proposals, each started from a random matrix already at the target $n_{\mathbb{R}}$; it returned twelve hits on eight distinct previously unrealized 3-tuples. An earlier round of eight chases started from the parameter point of the $(10, 0, 0)$ example of [1], with coarser steps, descended only to $n_t = 5$ and produced nothing — a fact about the search, not about the geometry. Six further chases of 200 000 proposals in total, seeded at the new low-n_t hits and aimed at $(0, 10, 0)$, $(1, 9, 0)$, $(0, 9, 1)$, $(1, 0, 9)$, $(0, 0, 10)$ and

$(4,0,6)$, re-found the same eight cells and no new one. The search cost about 1.4 CPU-hours in all.

Two of the eight hits are not among the theorems above. The cells $(1,1,6)$ and $(1,0,7)$, both with $n_{\mathbb{R}} = 8$, were reached by the matrices

$$\begin{pmatrix} 5 & 0 & -11 & 6 \\ 10 & 8 & -1 & -11 \\ 6 & 13 & 11 & 10 \\ -17 & -5 & -11 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 12 & 2 & 10 & -6 \\ 7 & -10 & 2 & -12 \\ -2 & -9 & 7 & 4 \\ -8 & -2 & 3 & -10 \end{pmatrix}$$

respectively. For these two the count of real common secants is exact — it is a real root count of the integer eliminant — but the three-way split into types was made from floating-point discriminant signs without Descartes certificates, and an $n_{\mathbb{R}} = 8$ claim additionally needs a certified bound on the number of real roots of a degree-10 polynomial, which the present certificates do not provide (they use only the free bound that ten sign changes of a degree-10 polynomial account for all of its real roots). We therefore record $(1,1,6)$ and $(1,0,7)$ as measured, not proved, and make no claim about their realizability.

Finally, the negative side. Over everything classified for this work — the 20 000 uniform samples and roughly 450 000 annealed proposals, about 470 000 exactly classified pairs in all — no configuration with $n_{\mathbb{R}} = 10$ and $n_t \leq 1$ was ever seen, and none with $(n_t, n_p) = (4,0)$. The two families of Remark 1.8 of [1] were therefore never reached, and neither was $(4,0,6)$. This is a statement about a search. "Not found" is not "not realizable", and we draw no conclusion from it; we record it because the next attempt on those cells should know that the instrument used here does not reach them, and should either sharpen the objective — annealing on the smallest discriminant among the secants whose sign change would move the 3-tuple toward the target, rather than on the 3-tuple alone — or look for a real obstruction.

8. Verification

The certificate half of this paper is formalised in Lean 4 [7] against Mathlib [8] and checked by the Lean kernel: the common-secant system in the form (2), the three types as the sign conditions of Proposition 3, Lemmas 5 and 6, and, for each of the seven configurations, its ten applications of Lemma 6 together with the conclusion that there are ten strictly ordered parameters carrying common secants of the listed types — which is the whole content of Theorems 7–12 and 14 except for the last clause of each. What is not formalised is listed in Section 1.5, together with Remark 2, the three controls at the end of Section 6 and the whole of Section 7, which report computations made in PARI/GP [9]. The toolchain is `leanprover/lean4:v4.32.0` and Mathlib is taken at revision `81a5d257c8e410db` `227a6665ed08f64fea08e997`. The finite data — for each of the seven configurations, its sixteen matrix entries and the nine integer coefficient lists E, D, C_e, A_1, A_2, H_1, H_2, H_3, H_4 — and the 308 finite checks over them (44 per configuration: four identities, twenty integer evaluations, twenty Pos certificates) live in a module that imports nothing beyond the list arithmetic, so every product, Möbius transform and sign sweep is decided by the kernel on core integer and list operations; the real content of Sections 2–4 is supplied separately over Mathlib. In Lean's terms every decision procedure used is `decide +kernel`, and *no use of* `native_decide` *occurs anywhere*, so neither a compiler nor a runtime is part of the trusted base; there is no `sorry`, and every formalised statement depends only on `propext`, `Classical.choice` and `Quot.sound`, the three axioms of Lean's standard foundation. The development is about 1 560 lines and compiles in under four minutes of wall time, the import-free data module accounting for 61 seconds of that at a peak of 5.9 GB. Four negative controls are formalised alongside the theorems, to guard against a statement that is true for the wrong reason: that the common-secant system is not satisfied by an arbitrary quadruple; that the three types are pairwise exclusive; that configuration B does *not* realize $(10, 0, 0)$, one of its secants being partially real; and that it does *not* realize $(0, 10, 0)$, another being totally real. Independently of the formalisation, all 308 integer certificates and the 3-tuples they produce were recomputed in a second, unrelated implementation, which agreed in every case. The repository is private at the time of writing; repository reference to be added at submission.

Acknowledgement of provenance

The problem, the classification of real common secants into totally, partially and minimally real, the count of 161 admissible 3-tuples, the realization of 128 of them and the list of the remaining 33 are due to Aslam, Faust, Hauenstein, Lopez Garcia, Kagy, Regan, Wampler and Zhang [1], as is the numerical work behind them; the count of ten common secants is classical [3]. What is offered here is the realization of six of the 33 cells, the exact certificate that replaces the numerical one, the erratum of Remark 2, and the negative report of Section 7. We have not touched the monodromy theorem of [1], which is a certified path-tracking computation and not a finite check of this kind.

References

[1] S. Aslam, M. Faust, J. D. Hauenstein, J. Lopez Garcia, B. Kagy, M. H. Regan, C. W. Wampler and A. Zhang, *Common Real Secants to Pairs of Real Twisted Cubic Curves*, arXiv:2603.25003v1 (26 March 2026), 20 pages. As of 31 August 2026 there is no later version, no journal reference and no DOI other than the arXiv one, so all theorem, proposition, remark, problem, figure, equation and table references above are to `arXiv:2603.25003v1`.

[2] *Secants of two cubics mrc2025*, 2025. The software and data repository listed as reference [1] of `arXiv:2603.25003v1` — printed there without an author line and in exactly this form — at `https://github.com/mattfaust/SecantsofTwoCubicsMRC2025`. It is where that paper says its code, sample parameter points and certified solution data live. Not consulted for this work.

[3] D. Eisenbud and J. Harris, *3264 and All That: A Second Course in Algebraic Geometry*, Cambridge University Press, Cambridge, 2016. (Chapter 3, Keynote Question (c) and Proposition 3.14.)

[4] D. J. Bates, J. D. Hauenstein, A. J. Sommese and C. W. Wampler, *Bertini: Software for Numerical Algebraic Geometry*, `https://bertini.nd.edu`.

[5] J. D. Hauenstein and F. Sottile, *Algorithm 921: alphaCertified: certifying solutions to polynomial systems*, ACM Trans. Math. Software **38** (2012), no. 4, Art. 28, 20 pp. This article, and not only the software, is what [1] cites as its reference [11].

[6] J. Chen, A. Edelman and J. Urschel, *The largest 5th pivot may be the root of a 61st degree polynomial*, arXiv:2602.20390v2 (15 March 2026). The subject of the companion development from which the certificate layer of Section 4 is taken unchanged; that layer is not a contribution of the present paper.

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

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

[9] The PARI Group, *PARI/GP*, version 2.13.3, Univ. Bordeaux, 2021. Used for the elimination of Section 3, for the search of Section 7 and for the independent checks reported in Section 6. Available at `https://pari.math.u-bordeaux.fr/`.