

# Computational Evidence Against Quadratic–Cubic Factorization for the Second Cuboid Quintic

Valery Asiryan

[asiryanvalery@gmail.com](mailto:asiryanvalery@gmail.com)

Randall L. Rathbun

[randallrathbun@gmail.com](mailto:randallrathbun@gmail.com)

January 12, 2026

## Abstract

Let  $Q_{p,q}(t) \in \mathbb{Z}[t]$  be Sharipov’s even monic degree-10 *second cuboid polynomial* depending on coprime integers  $p \neq q > 0$ . Writing  $Q_{p,q}(t)$  as a quintic in  $t^2$  produces an associated monic quintic polynomial. After the weighted normalization  $r = p/q$  and  $s = r^2$  we obtain a one-parameter family  $P_s(x) \in \mathbb{Q}[x]$  such that

$$Q_{p,q}(t) = q^{20} P_s\left(\frac{t^2}{q^4}\right) \quad \text{with} \quad s = \left(\frac{p}{q}\right)^2.$$

Assuming a quadratic divisor  $x^2 + ax + b$  with  $a, b \in \mathbb{Q}$ , we reduce divisibility of  $P_s(x)$  to the vanishing of an explicit remainder

$$R(x) = R_1(s, a, b)x + R_0(s, a, b).$$

A key structural observation is that  $R_1$  and  $R_0$  are quadratic in  $b$  and that, on the equation  $R_1 = 0$ , the second condition becomes linear in  $b$ . This yields a one-direction elimination to a plane obstruction curve  $F(s, a) = 0$  with  $F \in \mathbb{Z}[s, a]$ , without any “lifting-back” issues: when the linear coefficient is nonzero, the parameter  $b$  is forced to be the rational value  $b = C/L$ . We isolate the degenerate locus  $L = C = 0$  and show it produces only  $s = \pm 1$  (hence only  $s = 1$  in the cuboid domain  $s > 0$ ).

Let  $\overline{C} \subset \mathbb{P}^2$  be the projective closure of  $F(s, a) = 0$ . Using MAGMA we perform a height-bounded search for rational points on  $\overline{C}$ . With bound  $H = 10^7$ , the search returns 8 rational points, whose affine part has  $s \in \{-1, 0, 1\}$ . In particular, no affine rational point with  $s > 0$  and  $s \neq 1$  is found up to this bound. This provides strong computational evidence that for rational  $s > 0$ ,  $s \neq 1$ , the quintic  $P_s(x)$  admits no quadratic factor over  $\mathbb{Q}$  (equivalently, no 2 + 3 (quadratic–cubic) factorization over  $\mathbb{Q}$ ), and yields a conditional exclusion assuming completeness of the rational-point enumeration on  $\overline{C}$ .

**Keywords:** perfect cuboid; cuboid polynomials; factorization; resultants; rational points; plane curves; height search; MAGMA.

**Mathematics Subject Classification:** 11D41, 11G30, 14H25, 12E05, 11Y16.

# 1 Introduction

The perfect cuboid problem asks for a rectangular box with integer edges such that all three face diagonals and the space diagonal are integers. In a framework due to R. A. Sharipov [1, 2], one is led to explicit parameter-dependent even polynomials whose irreducibility is conjectured for coprime parameters. In particular, Sharipov defines the *second cuboid polynomial*  $Q_{p,q}(t) \in \mathbb{Z}[t]$  of degree 10 and formulates the conjecture that  $Q_{p,q}(t)$  is irreducible over  $\mathbb{Z}$  for coprime  $p \neq q > 0$ .

**Goal.** We reduce the *quadratic–cubic* (2+3) case for the normalized associated quintic  $P_s(x)$  to rational points on an explicit plane curve  $F(s, a) = 0$ , and we provide computational evidence (via a height-bounded search) that no such factorization occurs for  $s \in \mathbb{Q}_{>0}$  with  $s \neq 1$ .

**Method.** We work directly with the divisibility condition by a generic quadratic  $x^2 + ax + b$ . The Euclidean remainder has the form  $R_1x + R_0$ ; remarkably,  $R_1$  and  $R_0$  are quadratic in  $b$ , and on the locus  $R_1 = 0$  the second equation becomes linear in  $b$ . This yields an explicit plane obstruction curve  $F(s, a) = 0$  in the  $(s, a)$ -plane. Determining all rational points on curves of genus  $> 1$  is a subtle Diophantine problem; finiteness is guaranteed by Faltings’ theorem [3], while explicit determination typically requires additional methods (e.g. Chabauty–Coleman and refinements) [4, 5, 6]. In this note we instead perform a height-bounded search for rational points on the projective closure  $\overline{C}$  of  $F(s, a) = 0$  using MAGMA [7].

## 2 The second cuboid polynomial and its associated quintic

### 2.1 Sharipov’s second cuboid polynomial $Q_{p,q}(t)$

Let  $p, q \in \mathbb{Z}_{>0}$  be coprime and  $p \neq q$ . The second cuboid polynomial is the even monic degree-10 polynomial

$$\begin{aligned} Q_{p,q}(t) = & t^{10} + (2q^2 + p^2)(3q^2 - 2p^2)t^8 \\ & + (q^8 + 10p^2q^6 + 4p^4q^4 - 14p^6q^2 + p^8)t^6 \\ & - p^2q^2(q^8 - 14p^2q^6 + 4p^4q^4 + 10p^6q^2 + p^8)t^4 \\ & - p^6q^6(q^2 + 2p^2)(-2q^2 + 3p^2)t^2 - p^{10}q^{10} \in \mathbb{Z}[t]. \end{aligned} \quad (1)$$

This is the polynomial denoted  $Q_{p,q}(t)$  in [1, 2].

### 2.2 Weighted normalization to $Q_r(u)$

The polynomial (1) is weighted-homogeneous of total weight 20 for

$$\deg(p) = \deg(q) = 1, \quad \deg(t) = 2,$$

hence one may normalize to a one-parameter family.

**Lemma 1** (Normalization). *Let  $q \neq 0$  and set*

$$r := \frac{p}{q} \in \mathbb{Q}, \quad u := \frac{t}{q^2} \in \mathbb{Q}.$$

*Then*

$$Q_{p,q}(t) = q^{20} Q_r(u), \quad (2)$$

*where*

$$\begin{aligned} Q_r(u) = & u^{10} + (2 + r^2)(3 - 2r^2)u^8 + (1 + 10r^2 + 4r^4 - 14r^6 + r^8)u^6 \\ & - r^2(1 - 14r^2 + 4r^4 + 10r^6 + r^8)u^4 - r^6(1 + 2r^2)(-2 + 3r^2)u^2 - r^{10} \in \mathbb{Q}[u]. \end{aligned} \quad (3)$$

*Proof.* Substitute  $p = rq$  and  $t = q^2u$  into (1) and factor out  $q^{20}$ .  $\square$

### 2.3 The associated quintic $P_s(x)$

Since  $Q_r(u)$  is even, it is a quintic in  $x = u^2$ .

**Definition 1** (Second cuboid quintic). Let  $s := r^2 \in \mathbb{Q}_{\geq 0}$ . Define  $P_s(x) \in \mathbb{Q}[x]$  by the identity

$$Q_r(u) = P_s(u^2). \quad (4)$$

Equivalently,  $P_s(x)$  is the monic quintic

$$\begin{aligned} P_s(x) = & x^5 + (2 + s)(3 - 2s)x^4 + (1 + 10s + 4s^2 - 14s^3 + s^4)x^3 \\ & - s(1 - 14s + 4s^2 + 10s^3 + s^4)x^2 - s^3(1 + 2s)(-2 + 3s)x - s^5. \end{aligned} \quad (5)$$

*Derivation.* Substitute  $x = u^2$  into (3) and set  $s = r^2$ .  $\square$

**Definition 2** ( $2+3$  factorization). Let  $K$  be a field of characteristic 0. We say that a monic quintic  $P(x) \in K[x]$  admits a  $2+3$  factorization over  $K$  if it is divisible in  $K[x]$  by a quadratic polynomial (equivalently,  $P(x) = D(x)H(x)$  with  $\deg D = 2$  and  $\deg H = 3$ ).

*Remark 1.* In the original cuboid setting we have  $p, q > 0$ , hence  $r > 0$  and  $s = r^2 \in \mathbb{Q}_{>0}$ . Moreover  $p \neq q$  is equivalent to  $r \neq 1$ , i.e.  $s \neq 1$ .

**Lemma 2** (Quadratic factors and even quartic factors). *Let  $s = r^2$  with  $r = p/q \in \mathbb{Q}$  and  $q \neq 0$ . If  $P_s(x)$  is divisible in  $\mathbb{Q}[x]$  by  $x^2 + ax + b$  with  $a, b \in \mathbb{Q}$ , then  $Q_{p,q}(t)$  is divisible in  $\mathbb{Q}[t]$  by the even quartic polynomial*

$$t^4 + aq^4t^2 + bq^8.$$

*Proof.* If  $(x^2 + ax + b) \mid P_s(x)$  then  $(u^4 + au^2 + b) \mid P_s(u^2) = Q_r(u)$ . Substituting  $u = t/q^2$  and multiplying by  $q^8$  yields  $(t^4 + aq^4t^2 + bq^8) \mid Q_{p,q}(t)$  by (2).  $\square$

### 3 Quadratic divisors and explicit remainder equations

Fix  $s \in \mathbb{Q}$  and consider a generic monic quadratic

$$D(x) := x^2 + ax + b, \quad a, b \in \mathbb{Q}. \quad (6)$$

Write the Euclidean division in  $\mathbb{Q}(s, a, b)[x]$  as

$$P_s(x) = Q(x) D(x) + R(x), \quad \deg R < 2, \quad (7)$$

so that  $R(x) = R_1(s, a, b)x + R_0(s, a, b)$ . Then  $D \mid P_s$  is equivalent to  $R_1 = R_0 = 0$ .

**Lemma 3** (Explicit remainder). *Let  $P_s(x)$  be as in (5) and let  $D(x) = x^2 + ax + b$ . Then the remainder in (7) is*

$$R(x) = (b^2 + u(s, a)b + v(s, a))x + (m(s, a)b^2 + n(s, a)b - s^5), \quad (8)$$

where  $u, v, m, n \in \mathbb{Z}[s, a]$  are given explicitly by

$$u(s, a) = -3a^2 + (12 - 4s^2 - 2s)a + (-s^4 + 14s^3 - 4s^2 - 10s - 1), \quad (9)$$

$$\begin{aligned} v(s, a) = & a^4 + (2s^2 + s - 6)a^3 + (s^4 - 14s^3 + 4s^2 + 10s + 1)a^2 \\ & + (s^5 + 10s^4 + 4s^3 - 14s^2 + s)a + (-6s^5 + s^4 + 2s^3), \end{aligned} \quad (10)$$

$$m(s, a) = -2a - 2s^2 - s + 6, \quad (11)$$

$$\begin{aligned} n(s, a) = & a^3 + (2s^2 + s - 6)a^2 + (s^4 - 14s^3 + 4s^2 + 10s + 1)a \\ & + (s^5 + 10s^4 + 4s^3 - 14s^2 + s). \end{aligned} \quad (12)$$

*Proof.* In the quotient ring  $\mathbb{Q}[s, a, b][x]/(x^2 + ax + b)$  we have  $x^2 \equiv -ax - b$ , hence every power  $x^k$  reduces to a linear expression in  $x$ . Reducing each term of  $P_s(x)$  modulo  $D(x)$  yields a remainder of the form (8), and collecting coefficients gives (9)–(12). For completeness and reproducibility, Script A in Appendix A cross-checks (8) against MAGMA's `Quotrem` computation.  $\square$

### 4 Linearization in $b$ and an obstruction curve

#### 4.1 Linearization on the locus $R_1 = 0$

Let

$$R_1(s, a, b) := b^2 + u(s, a)b + v(s, a), \quad R_0(s, a, b) := m(s, a)b^2 + n(s, a)b - s^5. \quad (13)$$

**Lemma 4** (One-direction reduction). *Define*

$$L(s, a) := n(s, a) - m(s, a)u(s, a), \quad C(s, a) := m(s, a)v(s, a) + s^5. \quad (14)$$

*Then, on the equation  $R_1(s, a, b) = 0$ , we have*

$$R_0(s, a, b) = L(s, a)b - C(s, a). \quad (15)$$

*Proof.* If  $R_1 = 0$  then  $b^2 = -ub - v$ . Substituting this into  $R_0 = mb^2 + nb - s^5$  gives

$$R_0 = m(-ub - v) + nb - s^5 = (n - mu)b - (mv + s^5) = Lb - C,$$

which is (15).  $\square$

## 4.2 The obstruction polynomial $F(s, a)$

**Definition 3** (Obstruction polynomial). Let  $u, v, m, n, L, C$  be as in (9)–(12) and (14). Define

$$F(s, a) := C(s, a)^2 + u(s, a)L(s, a)C(s, a) + v(s, a)L(s, a)^2 \in \mathbb{Z}[s, a]. \quad (16)$$

**Proposition 1** (Divisibility criterion). Fix  $s \in \mathbb{Q}$ . The following are equivalent:

1.  $P_s(x)$  admits a  $2+3$  factorization over  $\mathbb{Q}$ ;
2. there exist  $a, b \in \mathbb{Q}$  such that  $R_1(s, a, b) = R_0(s, a, b) = 0$ .

Moreover, if such  $a, b$  exist then either

- (A)  $L(s, a) \neq 0$  and  $F(s, a) = 0$ , in which case necessarily  $b = C(s, a)/L(s, a)$ ; or
- (B)  $L(s, a) = 0$  and  $C(s, a) = 0$  (the degenerate locus).

*Proof.* The equivalence (1)  $\Leftrightarrow$  (2) is immediate from  $D \mid P_s \Leftrightarrow$  remainder  $R$  vanishes identically, i.e.  $R_1 = R_0 = 0$ .

Assume  $R_1 = R_0 = 0$ . By Lemma 4 we have  $R_0 = Lb - C$ , hence either  $L \neq 0$  and  $b = C/L$ , or  $L = 0$  and  $C = 0$ . If  $L \neq 0$ , substituting  $b = C/L$  into  $R_1 = b^2 + ub + v = 0$  and clearing denominators gives  $F(s, a) = 0$  by (16).  $\square$

**Proposition 2** (Degrees and the special fiber  $s = 1$ ). The polynomial  $F(s, a) \in \mathbb{Z}[s, a]$  satisfies

$$\deg_s F = 16, \quad \deg_a F = 10.$$

Moreover,

$$F(1, a) = -a^4(a - 2)^6.$$

*Proof.* This is verified by MAGMA in Appendix A (see the transcript in Script A). The specialization at  $s = 1$  reflects the factorization

$$P_1(x) = (x - 1)(x + 1)^4,$$

so that both  $x^2 - 1$  (corresponding to  $a = 0$ ) and  $(x + 1)^2$  (corresponding to  $a = 2$ ) divide  $P_1(x)$ .  $\square$

## 5 The degenerate locus $L = C = 0$

The reduction in Proposition 1 is one-direction and produces the explicit plane curve  $F(s, a) = 0$  when  $L \neq 0$ . The remaining possibility is the degenerate locus  $L = C = 0$ .

**Proposition 3** (Degenerate locus classification). The system

$$L(s, a) = 0, \quad C(s, a) = 0$$

has the following rational solutions:

$$(s, a) = (1, 2) \quad \text{and} \quad (s, a) = (-1, 2).$$

In particular, for  $s \in \mathbb{Q}_{>0}$  with  $s \neq 1$  the degenerate locus is empty.

*Computational proof in MAGMA.* We eliminate  $s$  by the resultant  $\text{Res}_s(L, C) \in \mathbb{Q}[a]$ . MAGMA computes

$$\text{Res}_s(L, C) = (a - 2)^6 \cdot G(a),$$

where  $G(a) \in \mathbb{Q}[a]$  has degree 21 and has no rational roots. Hence any rational solution must satisfy  $a = 2$ . Substituting  $a = 2$  and computing  $\gcd(L(s, 2), C(s, 2))$  yields  $(s - 1)^2(s + 1)$ , so  $s = \pm 1$ . The relevant transcript is included in Appendix A (Script A, Step 4).  $\square$

## 6 Rational points on the obstruction curve and the $2+3$ case

Let  $F(s, a)$  be as in Definition 3. Let  $\widehat{F}(S, A, Z)$  be the homogeneous polynomial of total degree 17 obtained by homogenizing  $F(S/Z, A/Z)$  in  $\mathbb{Q}[S, A, Z]$ , and let

$$\overline{C} : \quad \widehat{F}(S, A, Z) = 0 \subset \mathbb{P}_{\mathbb{Q}}^2 \tag{17}$$

be the projective closure.

**Proposition 4** (Genus and singularities). *The plane curve  $\overline{C}$  has degree 17, arithmetic genus 120, and geometric genus 7. Its singular rational points in  $\mathbb{P}^2(\mathbb{Q})$  are*

$$(-1 : 2 : 1), (0 : 0 : 1), (1 : 0 : 1), (1 : 2 : 1), (-1 : 1 : 0), (0 : 1 : 0).$$

*Computational proof in MAGMA.* This follows from MAGMA's commands `Degree`, `Genus`, `GeometricGenus`, `ArithmeticGenus`, and `SingularPoints` applied to  $\overline{C}$ . See Script A in Appendix A, Step 5.  $\square$

**Proposition 5** (Height-bounded rational points on  $\overline{C}$ ). *Let  $H = 10^7$ . The MAGMA command `RationalPoints(Cproj : Bound := H)` returns the following 8 rational points on  $\overline{C}$ :*

$$\{(1 : 2 : 1), (0 : 1 : 0), (0 : 0 : 1), (0 : 6 : 1), (1 : 0 : 0), (-1 : 2 : 1), (1 : 0 : 1), (-1 : 1 : 0)\}. \tag{18}$$

In particular, among these points the affine rational points (with  $Z \neq 0$ ) are exactly

$$(s, a) \in \{(1, 2), (1, 0), (0, 0), (0, 6), (-1, 2)\},$$

so no affine rational point with  $s > 0$  and  $s \neq 1$  is found within this search.

*Computational proof in MAGMA.* This is the output of the computation recorded in Appendix A, Script A, Step 5, with search bound  $H = 10^7$ .  $\square$

**Conjecture 1** (Completeness of the rational-point list). *The points listed in (18) are all rational points on  $\overline{C}$ , i.e.  $\overline{C}(\mathbb{Q})$  consists of exactly these 8 points.*

**Theorem 1** (Conditional exclusion of 2+3 factorization). *Assume Conjecture 1. Let  $s \in \mathbb{Q}_{>0}$  with  $s \neq 1$ . Then the quintic  $P_s(x)$  admits no 2+3 factorization over  $\mathbb{Q}$  (equivalently, it has no quadratic factor over  $\mathbb{Q}$ ).*

*Proof.* Assume, for contradiction, that  $P_s$  admits a 2+3 factorization over  $\mathbb{Q}$  for some  $s \in \mathbb{Q}_{>0}$  with  $s \neq 1$ . Then by Proposition 1 there exist  $a, b \in \mathbb{Q}$  with  $R_1(s, a, b) = R_0(s, a, b) = 0$ .

By Proposition 3, the degenerate case  $L = C = 0$  can occur for  $s > 0$  only when  $s = 1$ , which is excluded. Hence  $L(s, a) \neq 0$  and Proposition 1(A) applies, giving  $F(s, a) = 0$ . Thus  $(s, a)$  is an affine rational point on  $\bar{C}$ .

By Conjecture 1, every affine rational point on  $\bar{C}$  has  $s \in \{-1, 0, 1\}$ . Since  $s > 0$  and  $s \neq 1$ , no such point exists. This contradiction shows that  $P_s$  has no quadratic factor over  $\mathbb{Q}$ , hence admits no 2 + 3 factorization.  $\square$

**Corollary 1** (Conditional exclusion of even quartic factors of  $Q_{p,q}(t)$ ). *Assume Conjecture 1. Let  $p, q \in \mathbb{Z}_{>0}$  be coprime with  $p \neq q$ , and set  $s = (p/q)^2$ . Then  $Q_{p,q}(t)$  has no even quartic factor over  $\mathbb{Q}$ .*

*Proof.* If  $Q_{p,q}(t)$  had an even quartic factor, then by Lemma 2 the associated  $P_s$  would have a quadratic factor, contradicting Theorem 1.  $\square$

*Remark 2* (Irreducibility of  $Q_{p,q}(t)$ ). The reduction above isolates the 2 + 3 case within the normalized quintic family  $P_s(x)$ . The computational evidence in Proposition 5 supports the expectation that no such factorization occurs for  $s \in \mathbb{Q}_{>0}$  with  $s \neq 1$ , but a complete determination of  $\bar{C}(\mathbb{Q})$  would be required for an unconditional theorem; cf. the general context of rational points on higher-genus curves [3, 4, 5, 6].

## A MAGMA script and transcript

All computer-assisted steps in this note are executed in MAGMA [7]. Script A constructs the obstruction polynomial  $F(s, a)$ , cross-checks it against the Euclidean remainder and the resultant in  $b$ , classifies the degenerate locus  $L = C = 0$ , and performs a height-bounded search for rational points on  $\bar{C}$  via `RationalPoints(Cproj : Bound := H)` with  $H = 10^7$ .

### Script A: Obstruction curve and rational points

**Code.**

```
// ----- Pretty printing -----
procedure Banner(msg)
    print
    ↵ "\n-----";
    print msg;
    print
    ↵ "-----\n";
end procedure;

// Setup rational field
Q := RationalField();

Banner("Step 1. Define u,v,m,n,L,C,F in Q[s,a] (closed-form, no Resultant)");

// Work ring in (s,a)
R<s,a> := PolynomialRing(Q, 2);
```

```

// Explicit polynomials u,v,m,n
u := -3*a^2 + (12 - 4*s^2 - 2*s)*a + (-s^4 + 14*s^3 - 4*s^2 - 10*s - 1);

v := a^4 + (2*s^2 + s - 6)*a^3
+ (s^4 - 14*s^3 + 4*s^2 + 10*s + 1)*a^2
+ (s^5 + 10*s^4 + 4*s^3 - 14*s^2 + s)*a
+ (-6*s^5 + s^4 + 2*s^3);

m := -2*a - 2*s^2 - s + 6;

n := a^3 + (2*s^2 + s - 6)*a^2
+ (s^4 - 14*s^3 + 4*s^2 + 10*s + 1)*a
+ (s^5 + 10*s^4 + 4*s^3 - 14*s^2 + s);

// Linearized condition on R1=0: L*b - C = 0
L := n - m*u;
C := m*v + s^5;

// Main obstruction polynomial in Q[s,a]
F := C^2 + u*L*C + v*L^2;

print "deg_s F =", Degree(F, 1);
print "deg_a F =", Degree(F, 2);

Banner("Step 2 (cross-check). Compute remainder by division in Q[s,a,b][x] and verify
↪ u,v,m,n and F=Res_b(R1,R0)");

// Ring in parameters (s,a,b)
R3<s3,a3,b3> := PolynomialRing(Q, 3);
Px<x> := PolynomialRing(R3);

// Coefficients of Ps(x)
c4 := (2+s3)*(3-2*s3);
c3 := 1 + 10*s3 + 4*s3^2 - 14*s3^3 + s3^4;
c2 := -s3*(1 - 14*s3 + 4*s3^2 + 10*s3^3 + s3^4);
c1 := -s3^3*(1+2*s3)*(-2+3*s3);
c0 := -s3^5;

Ps := x^5 + c4*x^4 + c3*x^3 + c2*x^2 + c1*x + c0;
D := x^2 + a3*x + b3;

_, Rem := Quotrem(Ps, D);
R1_div := Coefficient(Rem, 1);
R0_div := Coefficient(Rem, 0);

print "deg_b R1 (division) =", Degree(R1_div, 3);
print "deg_b R0 (division) =", Degree(R0_div, 3);

// Coerce u,v,m,n to R3 by substitution
u3 := Evaluate(u, [s3, a3]);
v3 := Evaluate(v, [s3, a3]);
m3 := Evaluate(m, [s3, a3]);
n3 := Evaluate(n, [s3, a3]);

```

```

R1_model := b3^2 + u3*b3 + v3;
R0_model := m3*b3^2 + n3*b3 - s3^5;

print "Check R1_div == R1_model ? ", (R1_div - R1_model) eq 0;
print "Check R0_div == R0_model ? ", (R0_div - R0_model) eq 0;

// Verify F = Res_b(R1,R0) in Q[s,a]
S<ss,aa> := PolynomialRing(Q, 2);
T<bb> := PolynomialRing(S);

uS := Evaluate(u, [ss, aa]);
vS := Evaluate(v, [ss, aa]);
mS := Evaluate(m, [ss, aa]);
nS := Evaluate(n, [ss, aa]);

R1S := bb^2 + uS*bb + vS;
ROS := mS*bb^2 + nS*bb - ss^5;

Fres := Resultant(R1S, ROS);
FS := Evaluate(F, [ss, aa]);

print "Check Resultant == F ?      ", (Fres - FS) eq 0;
print "deg_s(Resultant) =", Degree(Fres, 1), " ; deg_a(Resultant) =", Degree(Fres, 2);

// ----- Fiber tests -----
Banner("Step 3. Fiber tests: specialize s=s0 and check rational roots in a");

procedure CheckFiber(s0)
  Pa<av> := PolynomialRing(Q);
  F_s0 := Evaluate(F, [s0, av]);

  print "\n--- Fiber s =", s0, "---";
  print "Factorization(F_s0):", Factorization(F_s0);

  rts := Roots(F_s0);
  print "Rational roots in a:", rts;

  if #rts gt 0 then
    print "Derived (a,b) solutions (when L!=0):";
    for rt in rts do
      a0 := rt[1];
      L0 := Evaluate(L, [s0, a0]);
      C0 := Evaluate(C, [s0, a0]);

      if L0 ne 0 then
        b0 := C0/L0;

        u0 := Evaluate(u, [s0, a0]);
        v0 := Evaluate(v, [s0, a0]);
        m0 := Evaluate(m, [s0, a0]);
        n0 := Evaluate(n, [s0, a0]);

        ok1 := (b0^2 + u0*b0 + v0) eq 0;
        ok0 := (m0*b0^2 + n0*b0 - s0^5) eq 0;

```

```

        print <a0, b0, ok1, ok0>;
    else
        print <a0, "L=0", "C=0 ?", (C0 eq 0)>;
    end if;
end for;
end if;
end procedure;

CheckFiber(Q!1);
CheckFiber(Q!4);
CheckFiber(Q!(4/9));
CheckFiber(Q!2);

// ----- Degenerate locus L=C=0 -----
Banner("Step 4. Degenerate locus: solve L(s,a)=0 and C(s,a)=0 via resultant in s");

Qa<aa> := PolynomialRing(Q);
Ts<ss> := PolynomialRing(Qa);

L_ss := Evaluate(L, [ss, aa]);
C_ss := Evaluate(C, [ss, aa]);

ResA := Resultant(L_ss, C_ss);
ResA := PrimitivePart(ResA);

print "Resultant Res_s(L,C) as polynomial in a has degree:", Degree(ResA);
print "Factorization of Res_s(L,C) in Q[a]:";
facResA := Factorization(ResA);
print facResA;

linroots := [];
for fe in facResA do
    f := fe[1];
    ex := fe[2];
    if Degree(f) eq 1 then
        c1 := Coefficient(f, 1);
        c0 := Coefficient(f, 0);
        r := -c0/c1;
        Append(~linroots, <r, ex>);
    end if;
end for;

print "Rational a-roots forced by Res_s(L,C)=0 (linear factors only):", linroots;

if #linroots gt 0 then
    for rr in linroots do
        a0 := rr[1];

        Qs<sv> := PolynomialRing(Q);
        L_s := Evaluate(L, [sv, a0]);
        C_s := Evaluate(C, [sv, a0]);

        g := GCD(L_s, C_s);

        print "\n--- Degenerate analysis at a =", a0, "---";

```

```

        print "gcd_s(L,C) =", g;
        print "Roots of gcd in s (rational):", Roots(g);
        print "Factorization of L(s,a0):", Factorization(L_s);
        print "Factorization of C(s,a0):", Factorization(C_s);
    end for;
end if;

// ----- Geometry and rational points -----
Banner("Step 5. Projective curve defined by F(s,a)=0: singularities and genus");

P2<X,Y,Z> := ProjectiveSpace(Q, 2);
F_XY := Evaluate(F, [X, Y]);
Fh := Homogenization(F_XY, Z);
Cproj := Curve(P2, Fh);

print "Projective curve defined. Degree =", Degree(Cproj);

try
    sing := SingularPoints(Cproj);
    print "Singular points (projective):";
    print sing;
catch e
    print "SingularPoints warning:", e;
end try;

gA := ArithmeticGenus(Cproj);
gG := GeometricGenus(Cproj);
g := Genus(Cproj);

print "Arithmetic genus =", gA;
print "Geometric genus  =", gG;
print "Genus           =", g;

H := 10^7;
print "Computing rational points on Cproj with bound H =", H;

pts := RationalPoints(Cproj : Bound := H);
print "\nRational Points found on Cproj:";
print pts;

print "\nInterpretation:";
for pt in pts do
    if pt[3] ne 0 then
        s_val := pt[1]/pt[3];
        a_val := pt[2]/pt[3];
        print "Affine solution (s, a) =", <s_val, a_val>;
    else
        print "Point at infinity:", pt;
    end if;
end for;

```

## Transcript.

---

Step 1. Define u,v,m,n,L,C,F in Q[s,a] (closed-form, no Resultant)

```
-----  
deg_s F = 16  
deg_a F = 10
```

```
-----  
Step 2 (cross-check). Compute remainder by division in Q[s,a,b][x] and verify  
u,v,m,n and F=Res_b(R1,RO)  
-----
```

```
deg_b R1 (division) = 2  
deg_b RO (division) = 2  
Check R1_div == R1_model ? true  
Check R0_div == R0_model ? true  
Check Resultant == F ? true  
deg_s(Resultant) = 16 ; deg_a(Resultant) = 10
```

```
-----  
Step 3. Fiber tests: specialize s=s0 and check rational roots in a  
-----
```

```
--- Fiber s = 1 ---  
Factorization(F_s0): [  
    <av - 2, 6>,  
    <av, 4>  
]  
Rational roots in a: [ <0, 4>, <2, 6> ]  
Derived (a,b) solutions (when L!=0):  
<0, -1, true, true>  
<2, "L=0", "C=0 ?", true>  
  
--- Fiber s = 4 ---  
Factorization(F_s0): [  
    <av^10 + 120*av^9 + 3795*av^8 - 32830*av^7 - 2213145*av^6 + 21454836*av^5 +  
     456975685*av^4 - 10459046190*av^3 + 83904838560*av^2 - 309104177760*av +  
     369152308224, 1>  
]  
Rational roots in a: []  
  
--- Fiber s = 4/9 ---  
Factorization(F_s0): [  
    <av^10 - 1672/81*av^9 + 42505/243*av^8 - 417479710/531441*av^7 +  
     87234203815/43046721*av^6 - 1196665550188/387420489*av^5 +  
     798522439495909/282429536481*av^4 - 35430471909028750/22876792454961*av^3 +  
     101165418048128800/205891132094649*av^2 -  
     154140701583484000/1853020188851841*av +  
     3719235255680000/617673396283947, 1>  
]  
Rational roots in a: []  
  
--- Fiber s = 2 ---  
Factorization(F_s0): [  
    <av^10 + 16*av^9 - 81*av^8 - 1698*av^7 + 5403*av^6 + 68604*av^5 -  
     302727*av^4 - 763506*av^3 + 6817596*av^2 - 14294840*av + 9825088, 1>
```

```

]

Rational roots in a: []

-----  

Step 4. Degenerate locus: solve L(s,a)=0 and C(s,a)=0 via resultant in s  

-----  

Resultant Res_s(L,C) as polynomial in a has degree: 27
Factorization of Res_s(L,C) in Q[a]:
[  

<aa - 2, 6>,  

<aa^21 + 285345/2048*aa^20 - 52389295807/16777216*aa^19 +  

522650508851/16777216*aa^18 - 12868810960899/67108864*aa^17 +  

55282038601431/67108864*aa^16 - 88360707927419/33554432*aa^15 +  

1747468207486969/268435456*aa^14 - 855371582178461/67108864*aa^13 +  

2687766826029291/134217728*aa^12 - 1696891713504949/67108864*aa^11 +  

6789739499416729/268435456*aa^10 - 1288675394382575/67108864*aa^9 +  

659577032682517/67108864*aa^8 - 3879986488883/2097152*aa^7 -  

15490767375299/8388608*aa^6 + 4080050071429/2097152*aa^5 -  

1864350017295/2097152*aa^4 + 55694069793/262144*aa^3 -  

23895604035/1048576*aa^2 + 179891901/262144*aa + 2099601/262144, 1>  

]  

Rational a-roots forced by Res_s(L,C)=0 (linear factors only): [ <2, 6> ]  

--- Degenerate analysis at a = 2 ---  

gcd_s(L,C) = sv^3 - sv^2 - sv + 1  

Roots of gcd in s (rational): [ <-1, 1>, <1, 2> ]  

Factorization of L(s,a0): [  

<sv - 1, 2>,  

<sv + 1, 1>,  

<sv^3 - 13*sv^2 - 14*sv + 18, 1>
]  

Factorization of C(s,a0): [  

<sv - 1, 2>,  

<sv + 1, 1>,  

<sv^4 - 19/4*sv^3 + 15/4*sv^2 + 9*sv - 7, 1>
]  

-----  

Step 5. Projective curve defined by F(s,a)=0: singularities and genus  

-----  

Projective curve defined. Degree = 17
Singular points (projective):
{@ (-1 : 2 : 1), (0 : 0 : 1), (1 : 0 : 1), (1 : 2 : 1), (-1 : 1 : 0), (0 : 1 : 0) @}
Arithmetic genus = 120
Geometric genus = 7
Genus = 7
Computing rational points on Cproj with bound H = 10000000

Rational Points found on Cproj:
{@ (1 : 2 : 1), (0 : 1 : 0), (0 : 0 : 1), (0 : 6 : 1), (1 : 0 : 0), (-1 : 2 : 1), (1 : 0 : 1), (-1 : 1 : 0) @}

```

```

Interpretation:
Affine solution (s, a) = <1, 2>
Point at infinity: (0 : 1 : 0)
Affine solution (s, a) = <0, 0>
Affine solution (s, a) = <0, 6>
Point at infinity: (1 : 0 : 0)
Affine solution (s, a) = <-1, 2>
Affine solution (s, a) = <1, 0>
Point at infinity: (-1 : 1 : 0)

```

## References

- [1] R. A. Sharipov, *Perfect cuboids and irreducible polynomials*, Ufa Math. J. **4** (2012), no. 1, 153–160.
- [2] R. A. Sharipov, *Asymptotic approach to the perfect cuboid problem*, Ufa Math. J. **7** (2015), no. 3, 95–107.
- [3] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.
- [4] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885.
- [5] R. F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770.
- [6] M. Stoll, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214.
- [7] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. **24** (1997), 235–265.