Separating Quadratic Roots in Finite Algebras and Smaller Degrees for Diophantine Presentations

13 November 2026

Abstract

We give an explicit polynomial encoding a rational point of a finite algebra subject to a nonzero condition. A triangular linear combination separates quadratic roots without a lower bound on their nonzero radicands. Separate bounds for the base roots and the radicands keep the polynomial weights small. Characteristic polynomials are truncated to the dimension of the relevant nonzero part. The construction includes vanishing radicands, nonreal roots, repeated characteristic values, and nonreduced excluded components. Applied to the existing arithmetic sources, it gives degree bounds below 2^{78} in 25 variables, below 2^{80} in the fully specified 27-variable construction, and below 2^{38} in both conditional 13-variable constructions. The fully specified coefficient-height bound improves to $2^{2^{92}}$. The variable counts, arithmetic hypotheses and sufficient coefficient parameters are unchanged.

1 Applications and their precise scope

Every variable count includes the distinguished input. The degree is total degree, and coefficient height is the largest absolute integer coefficient. The following are bounds for new polynomials with exactly the same rational input projections as the source constructions in the repository.

Source	Variables	Degree at most	Support less than
Inherited arithmetic premises	25	185517288563368898320200	2^{1815}
Fully specified, inherited premises	27	679086760181946108087584	2^{2009}
Weak *abc* at 121/100	13	207969001841	2^{437}
Weak *abc* at 16/15	13	199368913265	2^{436}

The last two rows also retain the elliptic group and height, pole-realization, and prime-pattern inputs of their sources. The first two retain their additional modular and contact-height inputs. This paper changes none of those arithmetic statements. It proves a new algebraic conversion of the same sources. It is not an independent verification of their arithmetic foundations.

For 25 variables the sufficient odd coefficient parameter remains ineffective. For 27 variables the existing certified value $L = 20483$ remains sufficient under the same premises. In both 13-variable families the sufficient odd shift B remains ineffective; the numerical $B = 3$ examples are not certified defining members. Multiplication by the input includes zero in the two 13-variable constructions, exactly as in their sources.

The source polynomials have not been expanded. Thus the displayed degrees and support sizes are upper bounds, not exact degrees or counts. The coefficient specification in Section 4 consists entirely of finite integer-polynomial operations.

2 Finite algebras and the nonzero condition

Let $R = \mathbb{Z}[x_1, \dots, x_a]$. Let

$$B = R[z_1, \dots, z_p]/(f_1(z_1), \dots, f_p(z_p)), \qquad A = B[q_1, \dots, q_s]/(q_j^2 - c_j)_{j=1}^{s},$$

where $p, s \geq 1$, the $f_i \in R[Z]$ are monic of degrees $d_i \geq 2$, and $c_j \in B$. Suppose each f_i is separable at every rational specialization of the base coordinates. Put

$$b = \prod_i d_i, \qquad n = 2^s b.$$

The usual monomials of exponent below the defining degrees are bases of B and A. Write M_v^B or M_v^A for multiplication by v in these bases. Fix $g \in B$ and set

$$G = g q_1 \cdots q_s, \qquad T = g^2 c_1 \cdots c_s \in B.$$

At a rational base point our target condition is

$$\text{there exists a } \mathbb{Q}\text{-algebra map } A \longrightarrow \mathbb{Q} \text{ with } G \neq 0. \tag{1}$$

There are no additional residual equations. The existing source certificates verify this form of the nonzero condition and the independence of each c_j from the q-generators.

At a rational base point B is an etale algebra. On its factors where $T \neq 0$, all the c_j and g are nonzero, and the corresponding part of A is also etale. The other factors of A may have nilpotents. They will not be discarded by an unjustified division.

3 A triangular combination of quadratic roots

Lemma 3.1. *Let $S \geq 1$ be real and let $c_1, \ldots, c_s \in \mathbb{C}^\times$ satisfy $|c_j| \leq S$. For each choice $q_j^2 = c_j$, put*

$$\phi(q_1, \ldots, q_s) = \frac{1}{2S} \sum_{j=1}^{s} (4S)^{1-j} \left(\prod_{k<j} c_k \right) q_j.$$

Its values on the 2^s choices of roots are distinct and have absolute value at most $2/3$. The same absolute-value bound holds when some c_j vanish, with the corresponding root equal to zero.

Proof. Every $|q_j| \leq \sqrt{S}$. The sum of the absolute values is at most

$$\frac{\sqrt{S}}{2S} \sum_{j=1}^{s} 4^{1-j} < \frac{2}{3\sqrt{S}} \leq \frac{2}{3}.$$

Consider two distinct choices, and let j be their first differing index. The common earlier factor is nonzero. After dividing the difference by that factor, its leading term is $q_j - \widetilde{q}_j = 2q_j$. For the tail, use $|c_j| = |q_j|^2$ and $|q_k| \leq \sqrt{S}$. The ratio of its absolute value to $2|q_j|$ is bounded above by

$$\frac{|q_j|}{\sqrt{S}} \sum_{\ell \geq 1} 4^{-\ell} \leq \frac{1}{3}.$$

The leading term cannot be cancelled. This proof uses no lower bound for $|c_j|$ and applies equally to nonreal roots. □

Write $f_i(Z) = Z^{d_i} + \sum_{k<d_i} f_{ik} Z^k$ and define scalar polynomials

$$Z_0 = 2 + \sum_{i,k<d_i} f_{ik}^2, \qquad S = b \left(1 + \sum_{j=1}^{s} \sum_{u,v=1}^{b} (M_{c_j}^B)_{uv}^2 \right). \tag{2}$$

At every rational base point $Z_0 \geq 2$ bounds the absolute values of the point roots. Indeed Cauchy's monic root bound is $1 + \max_k |f_{ik}|$, and $1 + t \leq 2 + t^2$ for $t \geq 0$. Also $S \geq b \geq 1$ bounds

the absolute values of all character values of c_j: the spectral radius is at most b times the largest absolute entry, and $|t| \le 1 + t^2$.

Set

$$\delta_i = \mathrm{Disc}(f_i), \qquad \kappa = \max_i \frac{d_i(d_i-1)-2}{2}, \qquad D = \prod_i \delta_i^2,$$
$$K = (2Z_0)^\kappa \prod_i (1+\delta_i^2), \qquad C = D + 4Z_0 K.$$

At a rational base point $D, K > 0$. Put $\epsilon = D/K$ and $L = C/D$. Then $0 < \epsilon \le 1$ and $L = 1 + 4Z_0/\epsilon$.

Lemma 3.2. *Any two distinct roots of any f_i differ in absolute value by at least ϵ.*

Proof. If Δ is the chosen root difference, the discriminant product gives

$$|\delta_i| \le |\Delta|^2 (2Z_0)^{d_i(d_i-1)-2}.$$

For $t > 0$, $t^2/(1+t^2) \le \sqrt{t}$. Therefore

$$\epsilon \le \frac{\delta_i^2}{1+\delta_i^2}(2Z_0)^{-\kappa} \le \frac{\sqrt{|\delta_i|}}{(2Z_0)^{(d_i(d_i-1)-2)/2}} \le |\Delta|.$$

The exponent is the maximum needed for a single polynomial, not the sum of all discriminant exponents. □

Define in A

$$J = 4S, \qquad Q = 2SJ^{s-1}, \qquad \Xi = \sum_{j=1}^{s} J^{s-j} \left(\prod_{k<j} c_k \right) q_j,$$
$$\Omega = Q\left(C^{p+1} + \sum_{i=1}^{p} D^i C^{p+1-i} z_i \right) + D^{p+1}\Xi.$$

These expressions are polynomial and involve no division.

Proposition 3.3. *At every rational base point, Ω has distinct nonzero values on all geometric characters of A with $G \neq 0$.*

Proof. Divide its values by the nonzero rational number QD^{p+1}. The result is

$$\alpha = L^{p+1} + \sum_{i=1}^{p} L^{p+1-i} z_i + \phi.$$

For two characters first differing at z_i, put $k = p+1-i \ge 1$. The leading difference has magnitude at least ϵL^k. The remaining difference is strictly less than

$$2Z_0 \sum_{\ell=0}^{k-1} L^\ell < \frac{2Z_0}{L-1} L^k = \frac{\epsilon}{2} L^k.$$

Here the difference of the two ϕ values is at most $4/3 \le 2Z_0$. If all point generators agree, the radicands agree and are nonzero; Lemma 3.1 separates the remaining root choices. Finally

$$|\alpha - L^{p+1}| \le Z_0 \sum_{\ell=0}^{p} L^\ell < \frac{Z_0}{L-1} L^{p+1} \le \frac{1}{4} L^{p+1}.$$

Thus no value is zero. Notice that this last nonvanishing estimate also holds on excluded characters, although their separation is unnecessary. □

4 A single polynomial and all degree-drop cases

Define scalar coefficients by

$$\det_B(I - vM_T) = \sum_{j=0}^{b} a_j v^j, \qquad a_0 = 1.$$

For each $1 \le r \le b$, set

$$h_r(X) = \sum_{j=0}^{r} a_j X^{r-j}, \qquad E_r = a_r - h_r(T), \qquad \omega_r = E_r\Omega, \qquad d_r = 2^s r.$$

Let $H_r(U)$ be the truncation through degree d_r of $\det_A(I - UM_{\omega_r})$. Equivalently, it is the sum of its principal-minor terms with sizes from zero through d_r. Finally set

$$P = H_b \prod_{r=1}^{b-1} \left(H_r^2 + \sum_{j=r+1}^{b} a_j^2 \right). \tag{3}$$

This is an explicit integer polynomial in the a retained base coordinates and just one further rational coordinate U.

Theorem 4.1. *For every rational base point, condition (1) holds if and only if $P(U) = 0$ for some $U \in \mathbb{Q}$.*

Proof. Let r_0 be the number of geometric characters of B on which $T \neq 0$, counted individually, not by distinct values of T. Because B is etale,

$$\det_B(I - vM_T) = \prod_{\chi}(1 - vT(\chi))$$

has degree exactly r_0. If $r = r_0 > 0$, then $a_r \neq 0$ and $h_r(X)$ is the product of $X - T(\chi)$ over the r nonzero character values, with repetitions retained. Hence $E_r = a_r$ on this part and $E_r = 0$ on $T = 0$.

If $r > r_0$, then $a_r = 0$ and $h_r(X) = X^{r-r_0}h_{r_0}(X)$, with $h_0 = 1$ when $r_0 = 0$. This vanishes at every value of T. Thus $E_r = 0$ in B, and also in A; $H_r = 1$. This explains why no additional factor a_r^2 is required in ω_r. If $r < r_0$, a nonzero tail coefficient makes $H_r^2 + \sum_{j>r} a_j^2$ strictly positive at every rational U. Consequently any rational zero of (3) belongs to the unique correct case $r = r_0 > 0$.

In that case E_r kills the entire excluded part, including any nilpotents. The remaining part is etale of dimension d_r. On it $\omega_r = a_r\Omega$ has distinct nonzero character values by Proposition 3.3. Thus the full determinant has degree d_r, so the truncation is exact. Its rational zero gives a nonzero rational character value of ω_r of multiplicity one. The corresponding one-dimensional rational kernel of $I - UM_{\omega_r}$ is preserved by every native multiplication matrix. Their actions on this line are rational scalars satisfying the algebra relations. They define a rational character on which $G \neq 0$.

Conversely, a rational character with $G \neq 0$ has a nonzero rational value of ω_{r_0}. Its reciprocal is a root of H_{r_0}, and all higher a_j vanish. This gives a zero of P. If $r_0 = 0$, every $H_r = 1$ and P has no zero. All assertions concern the complete rational zero set, not a generic open subset. □

5 Degree and support bounds

Give the base coordinates weight one, the z_i weights w_i, and the q_j weights v_j, so that monic reduction does not increase weight. Suppose $\mathrm{wt}(G) \le w_G$. Put

$$t = 2w_G, \quad u = \sum_i d_i(d_i - 1)w_i, \quad b_w = \sum_i (d_i - 1)w_i.$$

The scalar bounds in (2) have degree at most

$$z_d = 2\max_i d_i w_i, \qquad s_d = 2\max_j (2v_j + b_w).$$

Indeed an entry of multiplication by c_j has degree at most $2v_j+$ column weight $-$ row weight. Define

$$d_d = 2u, \qquad c_d = (\kappa+1)z_d + 2u,$$

and

$$A_0 = ss_d + \max\left\{(p+1)c_d, \max_{1\le i\le p}(id_d + (p+1-i)c_d + w_i)\right\},$$
$$A_1 = (p+1)d_d + \max_{1\le j\le s}\left((s-j)s_d + 2\sum_{k<j} v_k + v_j\right),$$
$$A_* = \max(A_0, A_1).$$

These give $\mathrm{wt}(\Omega) \le A_*$.

Theorem 5.1. *Put $h_r = 2^s r(rt + A_* + 1)$. Then*

$$\deg P \le h_b + 2\sum_{r=1}^{b-1} \max(h_r, bt) =: \mathcal{D}, \tag{4}$$
$$\deg_U P \le 2^s b^2 =: \mathcal{E}. \tag{5}$$

If $V = a + 1$ is the total number of coordinates and $\mathcal{E} \le \mathcal{D}$, then

$$\#\,\mathrm{supp}(P) \le \binom{\mathcal{D}+V}{V} - \binom{\mathcal{D}-\mathcal{E}+V-1}{V}.$$

Proof. Principal minors cancel row and column basis weights. Thus $\deg a_j \le jt$. The constant term cancels in $E_r = a_r - h_r(T)$, leaving r terms of weight at most rt. Hence ω_r has weight at most $rt + A_*$. A principal minor of size j, including the factor U^j, has total degree at most $j(rt + A_* + 1)$. Only $j \le 2^s r$ occur in H_r. Each tail coefficient has degree at most bt. This proves (4). The bound (5) follows from $2^s(b + 2\sum_{r<b} r) = 2^s b^2$. Counting monomials by the exponent of U gives the displayed binomial difference. □

For independent numerical checking, the sum of the h_r with the indicated multiplicities is

$$2^s\left[t\frac{2b^3+b}{3} + (A_*+1)b^2\right].$$

The correction for the initial interval $1 \le r \le r_*$ where $h_r < bt$ is $2\sum_{r=1}^{r_*}(bt - h_r)$. The direct summation and this closed formula are checked separately in the accompanying programs.

6 Coefficient bounds

We supply the bounds used for the fully specified 27-variable polynomial; the same formulas also give correctly labelled bounds for the ineffective families' numerical fixtures. Write $\ell(m) = \lceil \log_2 m \rceil$ for positive integers m. Use the weighted column norm over the coefficient ℓ^1 norm. Suppose

$$\|M_{z_i}\| \le 2^{\gamma_i}, \quad \|M_{q_j}\| \le 2^{\nu_j}, \quad \|M_G\| \le 2^{\eta},$$

and $\log_2 \|\delta_i\|_1 \le \lambda_i$. Put $b_\gamma = \sum_i (d_i - 1)\gamma_i$ and $v = \sum_i \lambda_i$. Valid scalar logarithmic norm bounds are

$$\begin{aligned}
z_l &= \ell(2 + \sum_i d_i) + 2 \max_i d_i \gamma_i, \\
s_l &= \ell(b) + \ell(1 + sb^2) + 2 \max_j (2\nu_j + b_\gamma), \\
d_l &= 2v, \qquad c_l = \kappa(1 + z_l) + p + d_l + z_l + 3, \\
q_l &= s s_l + 2s - 1, \\
\xi_l &= \ell(s) + \max_j \left((s - j)(s_l + 2) + 2 \sum_{k<j} \nu_k + \nu_j \right).
\end{aligned}$$

Here the restriction of multiplication by q_j^2 to B bounds $M_{c_j}^B$ in the inherited basis scaling. Hence these estimates do not assume that the unweighted basis has operator norm one.

A bound for $\log_2 \|M_\Omega\|$ is

$$\begin{aligned}
a_l = 1 + \max \Big\{ & q_l + \ell(p+1) + \max\left((p+1)c_l, \max_i (i d_l + (p + 1 - i)c_l + \gamma_i)\right), \\
& (p+1)d_l + \xi_l \Big\}.
\end{aligned}$$

Set $\mu = 2\eta + \ell(b)$ and

$$k_r = 2^s r(r\mu + \ell(r) + a_l + \ell(n) + 1).$$

Then

$$\log_2 \|P\|_1 \le k_b + \sum_{r=1}^{b-1} \left(2 \max(k_r, b\mu) + \ell(b+1)\right). \tag{6}$$

To verify this, principal-minor bounds give $\|a_j\|_1 \le \binom{b}{j} 2^{2j\eta} \le 2^{j\mu}$. The r terms of E_r give norm at most $2^{r\mu + \ell(r)}$. For the truncated determinant, each principal minor has norm bounded by the corresponding column-norm product. Bounding $\binom{n}{j} \le n^j$ and $d_r + 1 \le 2^{d_r}$ yields k_r. Squaring, adding at most $b + 1$ terms, and multiplying the factors proves (6).

For the certified parameter $L = 20483$ in the 27-variable source this gives

$$\log_2 \|P\|_1 \le 458233681089781199894138750 1 < 2^{92}, \qquad H(P) < 2^{2^{92}}.$$

For the three numerical fixtures the respective logarithmic bounds are

25 variables, $L = 3$	1154691810099707471428725
13 variables, $B = 3$, $\kappa = 121/100$	509178610649
13 variables, $B = 3$, $\kappa = 16/15$	496284465113.

None of these three fixture parameters is asserted to define the integers.

7 Application checks and reproducibility

The exact source versions are pinned in

`computation/few_variables/triangular_elimination_v24/inputs.json`.

The point counts are nine, nine, three and three; their scalar monic polynomials all have degree four, weight six, and logarithmic operator norm bound fourteen. The pole counts are two, three, two and two. The source certificates include $G = g \prod q_j$, no additional residual equations, and complete finite coefficient circuits.

For clarity, the source point polynomials have the form $Y^4 - 4a'Y^2 + 8(b')^2$, obtained from $h^4 - D_0 = a + b\sqrt{2}$ by the invertible transformation recorded in the source proofs. Their discriminants are

$$2^{15}(b')^2(2a^2 - b^2)^4(a^2 - 2b^2)^2.$$

The equation $h^4 = D_0$, with $D_0 = (3 - \sqrt{2})^2$, would force a rational fourth power to equal 49 after taking norms, which is impossible. The quadratic factors are anisotropic over $\mathbb{Q}$. Also $b' = -4a^3 + 6ab^2 + 3b^3$ has no nonzero rational zero: for $b \neq 0$ use Eisenstein at 3 on $4X^3 - 6X - 3$, and treat $b = 0$ directly. Thus the separability hypothesis holds at every rational retained base point, including those with no rational elliptic witnesses.

The exact values of (b, n, A_*, t) are

	b	n	A_*	t
25	262144	1048576	10545336	3861794
27	262144	2097152	15810084	7068076
13 (121/100)	64	256	523872	285114
13 (16/15)	64	256	486528	273690.

The degree sum includes respectively $254, 179, 3, 3$ cases in which the tail coefficients dominate the truncated determinant bound. Omitting these cases would give an incorrect numerical bound.

The producer and a separate checker verify the exact bounds. Thirteen small algebras are also computed using exact multiplication matrices: these include vanishing radicands and excluded nilpotents, nonreal point and pole roots, repeated values of T, a zero intermediate characteristic coefficient, a very small radicand, an empty nonzero locus, and a base algebra with two point generators and radicands depending on both. A deliberate omission of E_r is rejected by the empty-locus test. These are finite tests of the formulas; the universal assertions are proved above. No large source polynomial has been expanded, and no non-author review is represented by these computations.

The new specifications preserve the source projections for every retained base point. Consequently the arithmetic soundness and completeness proofs, including their quantifier order and exceptional input treatment, apply without change. The source construction for 13 variables is multiplied by X after conversion; this adds one to its degree bound, preserves the coefficient multiset and support size, and introduces no variable.

References

[1] *Separation in finite algebras on the nonzero locus*, repository companion source, `papers/finite_algebra/active_finite_algebra_20261109_v15.tex`. The present construction replaces its separating element and characteristic-polynomial bounds.

[2] *A defining polynomial in twenty-five variables*, `papers/few_variables25/few_variables25_merged_20261110_v19.tex`.

[3] *An explicit defining polynomial in twenty-seven variables*, `papers/few_variables27/explicit27_20261110_v19.tex`.

[4] *Thirteen variables from direct elliptic index comparison*, `papers/conditional_few_variables/direct_input13_20261110_v22.tex`.

[5] Zhi-Wei Sun, *$\mathbb{Z}$ is Diophantine over $\mathbb{Q}$ with 28 unknowns*, arXiv:2611.14605v1, 10 November 2026, https://arxiv.org/html/2611.14605v1. Its finite-root combination is related background; no arithmetic theorem from that paper is newly assumed in this conversion.