ECC RESEARCH PROGRAM · P1.3

First Fall Is Not Solving: Global Bounds and an Exact Semaev Obstruction

A universal upper bound, an underdetermined lower bound, and exact factor-base-size-two and three families

math.st [1] **@math__street** [1]

with GPT 5.6 Sol · Claude Fable 5

[1]Independent research collective, math.st · July 2026

ABSTRACT

The subexponential complexity claims for index calculus on elliptic curves rest on a heuristic: that the *first fall degree* of the Weil-restricted Semaev system approximates the degree at which a Gröbner-basis engine actually terminates. The problem P1.3 asks for an unconditional, explicit degree bound for these systems that does *not* invoke that heuristic. For the finite-field system obtained by adjoining $x_i^q - x_i$, we prove for every q, n, m and every degree-compatible order

$$d_{\mathrm{reg}} \le m(q-1)+1, \quad \mathsf{sd} \le \max\bigl(m(q-1)+2, m2^{m-1}\bigr). \tag{1}$$

The proof is the monomial coverage of the field-equation top ideal, Semaev's individual-degree formula, and Salizzoni's unconditional regularity bound; it is independent of n and uses no first-fall assumption. We then prove that its dependence on q cannot be removed universally. If the Weil core is proper and has at most $n < m$ generators, Krull height and the closed-space definition force $\mathsf{sd} \ge q$ for every degree-compatible order. An infinite nonsingular $n = 2, m = 3$ Semaev family with non-base targets makes the failure exact:

$$d_{\mathrm{ff}} = 14, \quad d_{\mathrm{reg}} = 2q+1, \quad q \le \mathsf{sd} \le 2q+2. \tag{2}$$

Thus first fall stays constant while solving degree is unbounded, and no first-fall-scale universal theorem can replace the q term. We also sharpen the upper bound at factor-base size two: for odd q, every extension degree, and every non-base target, $\mathsf{sd} \le \max(q, 5)$. For the exact family $n = m = 2$, every nonsingular short-Weierstrass curve over $\mathbb{F}_{q^2}$, and a non-base target x-coordinate, the quadratic Weil system satisfies $d_{\mathrm{ff}} = 5$, $d_{\mathrm{reg}} = q$, and $\mathsf{sd}_{\mathrm{grevlex}} \le q$ *unconditionally*, the last bound obtained through a constant-degree mutant family and Salizzoni's regularity bound rather than through any first-fall assumption. The matching equality $\mathsf{sd} = q$ holds for $q > 5$ exactly when the field equations enlarge the two-coordinate core ideal; the solving-minus-first-fall gap then grows without bound, reaching 18 already at $q = 23$. Crucially, this nonredundancy is *not* automatic: we exhibit an infinite family of genuine on-curve Semaev systems for every $q \equiv 3 \bmod 4$ with redundant field equations, certified concretely at $q = 7$ where $\bigl(d_{\mathrm{ff}}, d_{\mathrm{reg}}, \mathsf{sd}\bigr) = (5, 7, 5)$, and confirmed by exhaustive search over 50,376 eligible systems. The literal all-parameter problem is therefore resolved, and the stronger universal first-fall-scale hope is refuted rather than left open.

Keywords. ECDLP · index calculus · Semaev summation polynomials · Weil restriction · first fall degree · solving degree · Gröbner bases

1 Introduction

Index calculus is the reason elliptic-curve discrete logarithms over *extension* fields are not as hard as their group order suggests. The Semaev–Gaudry–Diem template [1], [2], [3] reduces an ECDLP instance on $E/\mathbb{F}_{q^n}$ to the problem of solving a polynomial system: one writes a summation-polynomial relation $f_{m+1}(x_1, \dots, x_m, x_R) = 0$ forcing m factor-base points to sum to a fixed point R, expands it through a *Weil restriction* into n equations over the base field $\mathbb{F}_q$, and hunts for base-field solutions with a Gröbner-basis engine. The cost of the whole attack is dominated by that Gröbner computation, and the cost of the Gröbner computation is governed by the largest polynomial degree the engine must reach before it terminates.

That governing degree is hard to control directly, so the literature substitutes a proxy. Petit and Quisquater [4] derived their influential subexponential estimate for binary ECDLP under the explicit assumption that the *degree of regularity* of the relevant Weil systems is only slightly larger than their *first fall degree* — the degree at which the first nontrivial degree drop occurs in a Macaulay-style expansion. Hodges, Petit, and Schlather [5] formalized first fall degree through the associated graded algebra of the finite-field function ring and proved general upper bounds for it, while flagging (their §6.3) that its closeness to the true termination degree is a *heuristic*. Kousidis and Wiemers [6] then proved a clean first-fall bound $d_{\mathrm{ff}} \le m^2 - m + 1$ for the binary case, but were careful to note that a first-fall bound is not, by itself, a solving-degree bound.

The problem posed as P1.3 removes the crutch. It asks: given q, n, m, produce an *unconditional* explicit bound on the degree of regularity or solving degree of the Weil-restricted Semaev system $S(q, n, m)$ *without* assuming that its first fall degree approximates either quantity. This is a request for a theorem where the literature has a heuristic.

We answer it in three layers. First comes a global worst-case theorem for every q, n, m: the field equations alone force a finite degree of regularity, and Salizzoni's theorem converts it into a solving-degree bound. Second comes a matching obstruction in the exponent of q: every proper underdetermined core $n < m$ forces solving degree at least q, and an exact $m = 3$ family keeps first fall fixed at 14. Third comes a sharper structural analysis at factor-base size two, culminating in an exact classification when $n = 2$.

Main result. Let $S(q, n, m) = \{g_0, \dots, g_{n-1}\}$ be the coordinate Weil restriction of $f_{m+1}(x_1, \dots, x_m, T)$, and put

$$F = S(q, n, m) \cup \{x_i^q - x_i : 1 \le i \le m\}. \tag{3}$$

For every q, n, m and every degree-compatible order,

$$d_{\mathrm{reg}(F)} \le m(q-1) + 1, \quad \mathsf{sd}(F) \le \max\big(m(q-1) + 2, m2^{m-1}\big). \tag{4}$$

This is unconditional and independent of the extension degree n.

Conversely, if the core ideal is proper and $n < m$, then $\mathsf{sd}_{\sigma(F)} \ge q$. There is an infinite nonsingular $n = 2, m = 3$ family with non-base targets satisfying

$$d_{\mathrm{ff}} = 14, \quad d_{\mathrm{reg}} = 2q + 1, \quad q \le \mathsf{sd}_{\sigma(F)} \le 2q + 2. \tag{5}$$

Hence the universal q-dependence is asymptotically necessary and first fall is not a solving-degree proxy even inside genuine $m > 2$ Semaev systems.

For odd q and $m = 2$, every non-base target in every extension satisfies $\mathsf{sd}_{\text{grevlex}} \leq \max(q, 5)$. In the exact $n = 2$, $q \geq 5$ family, every nonsingular curve $E : Y^2 = X^3 + AX + B$ over $\mathbb{F}_{q^2}$ and every non-base target x-coordinate $T \notin \mathbb{F}_q$ give the quadratic system $F = \{G_0, G_1, x^q - x, y^q - y\}$ satisfies, *unconditionally*,

$$d_{\text{ff}} = 5, \quad d_{\text{reg}} = q, \quad \mathsf{sd}_{\text{grevlex}} \leq q. \tag{6}$$

The first two are *exact* the third is a genuine upper bound obtained by a low-degree mutant family, *not* from a first-fall assumption. The equality $\mathsf{sd} = q$ holds for $q > 5$ *iff* the field equations $x^q - x, y^q - y$ enlarge the core ideal $C = (G_0, G_1)$ — and that nonredundancy is *not* automatic, even for nonsingular curves and on-curve targets. When it holds, the gap $\mathsf{sd} - d_{\text{ff}} = q - 5$ grows without bound.

1.1 Contributions and honest scope

We contribute (i) four fixed degree conventions and a worked system separating all four; (ii) an exact Semaev/Weil pipeline and its measured expansion boundary; (iii) a global unconditional regularity and solving-degree theorem; (iv) a universal underdetermined lower bound; (v) an infinite exact $m = 3$ family with constant first fall and linearly growing solving degree; (vi) an extension-uniform mutant theorem for $m = 2$; (vii) exact first-fall and regularity values for $n = m = 2$; (viii) a sharp quadratic solving bound and conditional equality; and (ix) an infinite genuine-Semaev counterexample to automatic field-equation nonredundancy.

The scope has two different boundaries. The *global upper bound* covers every q, n, m, while the *strong obstruction* covers every proper core with $n < m$ and therefore rules out a universal first-fall-scale replacement. The exact quadratic classification is only for $n = m = 2$ in odd characteristic. Automatic nonredundancy is false, so its equality half is genuinely conditional. Sharper constants for square or overdetermined cores $n \geq m > 2$ remain a classification problem, but they cannot restore the refuted universal claim.

2 Setting and notation

Fix a finite base field $\mathbb{F}_q$ and an extension $\mathbb{F}_{q^n}$; the exact short-Weierstrass classification later assumes odd q. Let $R = \mathbb{F}_q[x_1, \ldots, x_m]$ be the factor-base polynomial ring, and let $B_q = R/(x_1^q, \ldots, x_m^q)$ be the finite-field function ring in which first fall is computed. For a curve $E/\mathbb{F}_{q^n}$, Semaev's $(m+1)$-th summation polynomial $f_{m+1}(X_1, \ldots, X_{m+1})$ vanishes exactly when there exist points $P_i \in E$ with $x(P_i) = X_i$ and $P_1 + \cdots + P_{m+1} = O$ [1]. Fixing $X_{m+1} = x(R)$ for a target point R and substituting $x_i \in \mathbb{F}_q$-valued factor-base variables gives one equation over $\mathbb{F}_{q^n}$; choosing a polynomial basis $\mathbb{F}_{q^n} = \mathbb{F}_q[\alpha]$ and equating the n coordinate polynomials to zero produces the *Weil-restricted* system $S(q, n, m) = \{g_0, \ldots, g_{n-1}\} \subset R$. We write x, y for x_1, x_2 in the quadratic case, and throughout use the grevlex order with $x_1 > \cdots > x_m$ (i.e. $x > y$).

The three ideal-theoretic invariants below are the fixed literature conventions; the fourth is a run statistic we keep separate on purpose.

3 Four degree invariants and an exact separation

The first task in P1.3, following its session-one target, is to stop conflating distinct quantities. We adopt the conventions of Caminata and Gorla [7], tracing the first-fall definition back to Hodges, Petit, and Schlather [5].

Definition 1 (the four degrees). CITED For a nonhomogeneous system $F = \{f_1, \dots, f_s\} \subset R$ with top (highest-degree) parts f_i^{top}:

(a) First fall degree. With $\mathrm{Syz}(F^{\mathrm{top}})$ the syzygy module of the top parts and Triv its trivial submodule (Koszul syzygies together with the $\left(f_i^{\mathrm{top}}\right)^{q-1} e_i$ induced by B_q),

$$d_{\mathrm{ff}(F)} = \min\left\{ d : \mathrm{Syz}(F^{\mathrm{top}})_d / \mathrm{Triv}(F^{\mathrm{top}})_d \neq 0 \right\}. \tag{7}$$

(b) Degree of regularity. When the top ideal is Artinian, $d_{\mathrm{reg}(F)} = \min\left\{ d : (F^{\mathrm{top}})_d = R_d \right\}$.

(c) Solving degree. For a degree-compatible order σ, $\mathsf{sd}_{\sigma(F)}$ is the least cutoff d for which the closed degree-d Macaulay row space $V_{F,d}$ contains a σ-Gröbner basis of (F).

Remark 2 (a fourth, non-invariant quantity). PROVED The largest degree *printed* by a concrete engine, $D_{\mathcal{A}}(F, \sigma, \theta)$ under a full option set θ, is a *run statistic*, not an ideal invariant: pair-selection criteria and preprocessing change it without changing (F). Salizzoni's $V_{F,d}$ construction [8] and the closed Macaulay space in (c) are the *same* invariant (the mutant solving degree of the XL literature), whereas the highest Magma step degree reported by Kousidis and Wiemers [6] belongs to the $D_{\mathcal{A}}$ column. Conflating these is precisely the confusion P1.3 exists to remove.

These four notions are genuinely different, and a single small system makes the gaps concrete. It is the $q = 5$ specialization of Caminata–Gorla's Example 4.2 [7], augmented with the algorithm-trace measurement.

Proposition 3 (a system separating all four degrees). PROVED Over $\mathbb{F}_5[x_1, x_2, x_3]$ with grevlex $x_1 > x_2 > x_3$, set

$$F = \{x_1 x_2 + x_2, \quad x_2^2 - 1, \quad x_3^4 - 1, \quad x_1^5 - x_1\}. \tag{8}$$

Then $d_{\mathrm{ff}(F)} = 3$, $\mathsf{sd}_{\mathrm{grevlex}(F)} = 4$, $d_{\mathrm{reg}(F)} = 8$, and the specified FIFO naive-Buchberger run reaches degree $D_{\mathcal{A}}(F) = 9$.

Proof. The nontrivial degree-3 relation is $x_2(x_1 x_2) - x_1(x_2^2) = 0$, giving $d_{\mathrm{ff}} = 3$. The closed degree-4 Macaulay space contains $x_1 + 1 = x_2(x_1 x_2 + x_2) - (x_1 + 1)(x_2^2 - 1)$, hence the whole Gröbner basis $\{x_1 + 1, x_2^2 - 1, x_3^4 - 1\}$, giving $\mathsf{sd} = 4$. The top ideal $(x_1 x_2, x_2^2, x_3^4, x_1^5)$ first fills all forms in degree 8, so $d_{\mathrm{reg}} = 8$. Finally, the FIFO run processes the coprime pair whose leading-monomial LCM is $x_1^5 x_3^4$, of degree 9. Each value is produced by an exact modular row reduction, and SymPy's Gröbner routine independently returns the stated basis. □

The values $3, 8, 4, 9$ are pairwise distinct; in particular $d_{\mathrm{reg}} - d_{\mathrm{ff}} = 5$ and $\mathsf{sd} - d_{\mathrm{ff}} = 1$ *on the same system*. The problem statement's parenthetical identification of d_{reg} with sd is therefore false without extra hypotheses. This is the local baseline against which the Semaev-specific results below are read: whatever we prove for the Weil family, we prove for *named* invariants, never for an engine's log label.

4 The Semaev–Weil pipeline and its expansion boundary

To measure anything on real systems we need the summation polynomials themselves and an exact Weil restriction. Both are implemented over exact prime-field and polynomial-basis arithmetic.

Proposition 4 (the coordinate Weil builder). PROVED Represent $\mathbb{F}_{q^n} = \mathbb{F}_q[\alpha]$ in a polynomial basis, substitute factor-base variables $x_i \in \mathbb{F}_q$, expand $f_{m+1}(x_1, \ldots, x_m, x_R)$ as an element of $\mathbb{F}_{q^n}[x_1, \ldots, x_m]$, and equate its n basis coordinates to zero. The resulting base-field system $S(q, n, m)$ has exactly the base-field solutions in bijection with the extension-field zeros of $f_{m+1}(\cdot, x_R)$.

This is the explicit coordinate construction of Weil restriction used by Petit and Quisquater [4] and Kousidis and Wiemers [6], and matches the formalization of Caminata, Ceria, and Gorla [9]. Every known-target system we build uses the nonsingular curve $E : y^2 = x^3 + \alpha x + 1$ (with α the basis generator) unless a curve is explicitly overridden, and each stored factor-base tuple is verified to vanish in all n Weil coordinates; singular inputs are rejected.

The Semaev polynomials grow fast, and honesty about *which* ones we can handle exactly matters. Figure 1 records the exact sparse expansion statistics.

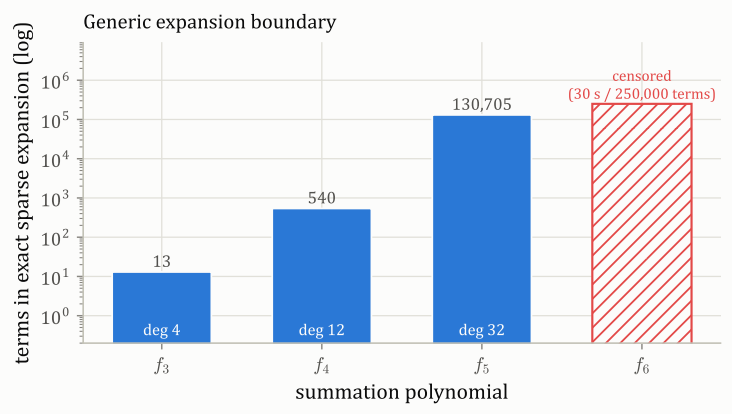

Figure 1: EMPIRICAL: 30 s / 250,000-term ceiling Exact sparse expansion of the generic summation polynomials: f_3 has 13 terms and total degree 4, f_4 has 540 terms and degree 12, f_5 has 130,705 terms and degree 32. Generic f_6 crosses the declared ceiling and is *censored*, not extrapolated; its independent recursive evaluator still passes a six-point zero-sum test over $\mathbb{F}_{101}$. Data: `measure_semaev_stats_20260722.csv`.

The censoring is a hard resource boundary, recorded as such: the generic f_6 expansion exceeded both a 30-second wall clock and a 250,000-term ceiling. Consequently our exact degree measurements live at $m \leq 4$. The sharp mutant classification lives at $m = 2$, while the exact obstruction lives at $m = 3$ and uses the expanded f_4 top pair. The global theorem below needs only Semaev's degree formula, not an expanded f_{m+1}. All arithmetic in the certificates is exact; no numerical approximation enters at any stage.

5 A global unconditional bound

The literal P1.3 question has a short worst-case answer once the field equations and the correct solving-degree theorem are used together. Put

$$F(q,n,m) = S(q,n,m) \cup \{x_1^q - x_1, \ldots, x_m^q - x_m\}. \tag{9}$$

Theorem 5 (global regularity and solving-degree bounds). PROVED For every finite field $\mathbb{F}_q$, every extension degree n, every factor-base size $m \geq 2$, and every degree-compatible monomial order σ,

$$d_{\mathrm{reg}(F(q,n,m))} \leq m(q-1)+1 \tag{10}$$

and

$$\mathsf{sd}_{\sigma(F(q,n,m))} \leq \max(m(q-1)+2, m2^{m-1}). \tag{11}$$

In particular, both bounds are independent of n and invoke no first-fall assumption.

Proof. PROVED The top ideal of F contains $(x_1^q, \ldots, x_m^q)$. Every monomial of total degree $m(q-1)+1$ has some exponent at least q, by the pigeonhole principle, and is therefore in this monomial ideal. Hence the entire homogeneous component of that degree lies in (F^{top}), proving $d_{\mathrm{reg}(F)} \leq m(q-1)+1$.

CITED Semaev's individual-degree formula gives degree at most 2^{m-1} in each factor-base variable of f_{m+1} [1]; the binary construction uses the same formula [6]. Fixing the target and extracting Weil coordinates are specialisation and base-field linear projection, so neither increases exponents. Thus every g_i has total degree at most $m2^{m-1}$.

CITED Salizzoni's unconditional Proposition 3.10 gives

$$\mathsf{sd}_{\sigma(F)} \leq \max\left(d_{\mathrm{reg}(F)} + 1, \max_{f \in F} \deg(f)\right) \tag{12}$$

[8]. Substitution yields $\max(m(q-1)+2, q, m2^{m-1})$. Since $m(q-1)+2 \geq q$ for $q, m \geq 2$, the middle term is redundant. □

Remark 6 (what the global theorem does not say). PROVED The theorem resolves the existence of an unconditional explicit bound, but it does not validate the cryptanalytic first-fall prediction. The term $m2^{m-1}$ is exponential in m, and $m(q-1)+2$ is linear in the field size rather than its bit length. The remainder of the paper asks how sharply the bound collapses in a structured Semaev family.

6 The underdetermined obstruction

The linear dependence on q in the global theorem is not just a weakness of the pigeonhole proof. Whenever the Weil core has fewer equations than factor-base variables and has a solution, a degree-q obstruction is forced before any Semaev-specific calculation.

Theorem 7 (underdetermined solving-degree lower bound). PROVED Let

$$C = (G_1, \ldots, G_r) \subset \mathbb{F}_{q[x_1,\ldots,x_m]} \tag{13}$$

be a proper Weil core ideal with $r \leq n < m$, and put

$$F = \{G_1, \ldots, G_r, x_1^q - x_1, \ldots, x_m^q - x_m\}. \tag{14}$$

For every degree-compatible monomial order τ,

$$\mathsf{sd}_{\tau(F)} \geq q. \tag{15}$$

Proof. CITED Krull's height theorem says that every minimal prime over an ideal generated by r elements has height at most r [10]. If all field equations belonged to C, then $\mathbb{F}_{q[x_1,\dots,x_m]}/C$ would be a quotient of the finite-dimensional algebra

$$\mathbb{F}_{q[x_1,\dots,x_m]}/(x_1^q - x_1, \dots, x_m^q - x_m). \tag{16}$$

Since C is proper, it would have dimension zero and height m, contrary to $\mathsf{ht}(C) \leq r \leq n < m$. Thus $(F) \supsetneq C$.

PROVED For $d < q$, no field equation can enter the closed space $V_{F,d}$, so every row in that space is generated from the core and $V_{F,d} \subseteq C$. A Groebner basis of the strictly larger ideal (F) cannot be contained in C, because it generates (F). No cutoff below q can therefore contain a Groebner basis. □

Corollary 8 (consequence in the logarithmic-extension regime). PROVED Every solvable system with $m > n$ and $n \asymp \log q$ has solving degree at least $q = \exp(\Theta(n))$. Therefore no polynomial-in-n, first-fall-scale universal theorem can cover all factor-base sizes under the explicit-field-equation convention.

The word *proper* is not a genericity assumption: a verified factor-base root makes the core proper. Thus the lower bound applies precisely to the underdetermined relation systems that a relation search succeeds in solving.

6.1 An exact infinite (m=3) family

We now make the obstruction concrete and simultaneously force first fall to stay constant. Let $q \equiv 3 \bmod 4$, $q \geq 7$, write $\mathbb{F}_{q^2} = \mathbb{F}_{q[u]}/(u^2+1)$, choose $h \in \mathbb{F}_q^\times$ with $h \neq 1, -1$, and define

$$\rho = (h + h^{-1})/2, \quad \eta = (h^{-1} - h)/2, \quad a = -4\eta^2, \quad c = 2\eta^2. \tag{17}$$

Then $\rho^2 - \eta^2 = 1$, and ρ, η, a, c are nonzero because -1 is not a square.

Theorem 9 (exact three-variable Semaev obstruction). PROVED On

$$E : Y^2 = X^3 + aX, \tag{18}$$

take the target

$$R' = (cu, -2\rho\eta^2(1-u)). \tag{19}$$

Its x-coordinate is non-base, the curve is nonsingular, and the $n = 2, m = 3$ Weil system for $f_4(x, y, z, cu)$ has the factor-base root

$$(x, y, z) = (2(1+\rho), -2(1+\rho), 0). \tag{20}$$

For every degree-compatible order τ,

$$d_{\mathrm{ff}} = 14, \quad d_{\mathrm{reg}} = 2q + 1, \quad q \leq \mathsf{sd}_{\tau(F)} \leq 2q + 2. \tag{21}$$

Proof. PROVED Direct substitution gives

$$\left(-2\rho\eta^2(1-u)\right)^2 = (cu)^3 + a(cu), \tag{22}$$

using $u^2 = -1$ and $\rho^2 - \eta^2 = 1$. Thus R' lies on E, and $c \neq 0$ makes its x-coordinate non-base. Put $\zeta = 2(1+\rho)$. The standard f_3 formula gives the two identities

$$f_3(\zeta, -\zeta, 2u) = 0, \quad f_3(0, cu, 2u) = 0. \tag{23}$$

Hence $2u$ is a common auxiliary root in $\mathrm{Res}_{Z(f_3(\zeta,-\zeta,Z),f_3(0,cu,Z))}$, proving $f_4(\zeta, -\zeta, 0, cu) = 0$. Nonsingularity follows from $a \neq 0$.

PROVED Splitting the resultant in the basis $(1, u)$ gives two core coordinates of degrees $12, 11$ with top parts

$$H_0 = x^4y^4z^4, \quad H_1 = -4cx^3y^3z^3(xy + xz + yz). \tag{24}$$

Their gcd is $x^3y^3z^3$, while the primitive pair $xyz, xy + xz + yz$ is coprime. The first polynomial-ring syzygy is therefore

$$(xy + xz + yz)H_0 + xyz/(4c)H_1 = 0 \tag{25}$$

in degree 14. Below that degree every product has variable exponents at most six, so reduction modulo (x^q, y^q, z^q) creates no earlier relation for $q \geq 7$. The degree-14 relation precedes both the degree-23 Koszul relation and the function-ring trivial relations. Hence $d_{\mathrm{ff}} = 14$.

PROVED In the full top ideal

$$J = (H_0, H_1, x^q, y^q, z^q), \tag{26}$$

the monomial $x^2y^{q-1}z^{q-1}$ survives in degree $2q$, so $d_{\mathrm{reg}} > 2q$. At degree $2q+1$, every monomial not already covered by a field monomial or H_0 is one of the three permutations of $x^3y^{q-1}z^{q-1}$. Multiplying H_1 by $y^{q-5}z^{q-5}$ produces the first boundary monomial modulo two terms divisible by H_0; symmetry handles the other two. Thus $J_{2q+1} = R_{2q+1}$ and $d_{\mathrm{reg}} = 2q + 1$.

PROVED The preceding underdetermined theorem gives $\mathsf{sd}_{\tau(F)} \geq q$. CITED Salizzoni's Proposition 3.10 [8] gives

$$\mathsf{sd}_{\tau(F)} \leq \max\big(d_{\mathrm{reg}} + 1, q, 12\big) = 2q + 2. \tag{27}$$

□

Remark 10 (an unbounded genuine-Semaev gap). PROVED The prime-power sequence $q = 3^{2r+1}$ is unbounded and lies in $q \equiv 3 \bmod 4$. Along this family,

$$\mathsf{sd}_{\tau(F)} - d_{\mathrm{ff}} \geq q - 14 \to \infty. \tag{28}$$

Thus a constant first fall and a growing solving degree coexist inside nonsingular Semaev–Weil systems with on-curve non-base targets, not merely in an abstract invariant-gap example.

Remark 11 (exact certificate). EMPIRICAL: $q in {7,11,19}$ and four stored solvable rows `certify_underdetermined_obstruction_20260723.json` records the symbolic resultant and top-part identities, exact roots, first fall 14, nonzero field-equation normal forms, and the audit of every completed stored underdetermined known-root row.

7 The quadratic family: first fall and regularity, exactly

We now fix $n = m = 2$ and prove the two exact invariants. Write $\mathbb{F}_{q^2} = \mathbb{F}_q[u]/(u^2 + m_1 u + m_0)$ with $u^2 + m_1 u + m_0$ irreducible, and let $T = t_0 + t_1 u$ with $t_1 \neq 0$ (the target x-coordinate is non-base). For short-Weierstrass coefficients $A, B \in \mathbb{F}_{q^2}$, let $G_0, G_1 \in \mathbb{F}_q[x, y]$ be the two Weil coordinates of $f_3(x, y, T)$, and set

$$F = \{G_0, G_1, x^q - x, y^q - y\}, \quad C = (G_0, G_1). \tag{29}$$

The whole analysis is driven by the shape of the top parts.

Proposition 12 (the quadratic top shape). PROVED The top parts of the two f_3 coordinates are

$$G_0^{\text{top}} = x^2 y^2, \quad G_1^{\text{top}} = c\, xy(x + y), \quad c \neq 0. \tag{30}$$

Proof. Semaev's third polynomial for $E : y^2 = x^3 + Ax + B$ is

$$f_3(X_1, X_2, X_3) = (X_1 - X_2)^2 X_3^2 - 2((X_1 + X_2)(X_1 X_2 + A) + 2B)X_3 + (X_1 X_2 - A)^2 - 4B(X_1 + X_2). \tag{31}$$

Taking the terms of highest factor-base degree in $x = X_1, y = X_2$ and splitting the two extension coordinates of the coefficient of $X_3 = T$ leaves $x^2 y^2$ in the coordinate along 1 and $c\, xy(x + y)$ in the coordinate along u, with c a nonzero $\mathbb{F}_q$-multiple of t_1; irreducibility of the modulus and $t_1 \neq 0$ give $c \neq 0$. □

Theorem 13 (first fall degree of the quadratic family). PROVED For every odd prime power $q \geq 5$ and non-base target, $d_{\text{ff}(G_0, G_1)} = 5$.

Proof. At degree 5 the relation

$$(x + y)G_0^{\text{top}} - c^{-1} xy\, G_1^{\text{top}} = 0 \tag{32}$$

holds identically, since both terms equal $x^2 y^2 (x + y)$. It is nontrivial: the first Koszul syzygy has degree $\deg G_0^{\text{top}} + \deg G_1^{\text{top}} = 7$, and the quotient-trivial syzygies $\left(G_i^{\text{top}}\right)^{q-1} e_i$ occur in degree $(q - 1) \cdot \deg G_i^{\text{top}} \geq 8$. No relation exists in degree 3 (a single generator cannot syzygy alone). A putative degree-4 relation $A' G_0^{\text{top}} + (B' x + C' y) G_1^{\text{top}} = 0$ expands to $A' x^2 y^2 + cB'(x^3 y + x^2 y^2) + cC'(x^2 y^2 + xy^3)$; the coefficients of the distinct monomials $x^3 y$ and xy^3 force $B' = C' = 0$, then $A' = 0$. Hence the first nontrivial relation is in degree 5. □

Theorem 14 (degree of regularity of the quadratic family). PROVED For every odd prime power $q \geq 5$ and non-base target, $d_{\text{reg}(F)} = q$.

Proof. The top ideal of F is $J = (x^2 y^2, xy(x + y), x^q, y^q)$ (the last two from the field equations). The monomial x^{q-1} is divisible by none of the generators of degree $\leq q - 1$ — those are $x^2 y^2$ and $xy(x + y)$, each requiring both variables — so $J_{q-1} \neq R_{q-1}$. In degree q: the pure powers $x^q, y^q \in J$; every mixed monomial $x^a y^{q-a}$ with $2 \leq a \leq q - 2$ is divisible by $x^2 y^2$. The two boundary monomials are reached through $xy(x + y)$: since $x^{q-3} \cdot xy(x + y) = x^{q-1} y + x^{q-2} y^2$ and the second term is divisible by $x^2 y^2$, we get $x^{q-1} y \in J$ modulo covered monomials, and symmetrically $xy^{q-1} \in J$. Thus $J_q = R_q$ while $J_{q-1} \neq R_{q-1}$, so $d_{\text{reg}(F)} = q$. □

Two facts deserve emphasis. First, d_{reg} depends on the input *top parts*, not on the ideal alone: it is the field-equation top parts x^q, y^q that drive d_{reg} up to q, exactly as Caminata and Gorla warn [7]. Second, $d_{\text{ff}} = 5$ is *constant* in q, so the pair $\left(d_{\text{ff}}, d_{\text{reg}}\right) = (5, q)$ already exhibits an unbounded

gap — but d_{reg} is an over-estimate of the true solving cost, and the interesting question is where sd actually lands.

8 The solving-degree bounds

The heart of P1.3 is a solving-degree bound that does not assume first fall is a good proxy. We give an unconditional *upper* bound and a conditional matching *lower* bound.

8.1 An unconditional upper bound via a mutant family

The strategy is to replace the two degree-q field equations by low-degree remainders modulo a *universal* Gröbner basis of the core C, staying inside the original closed degree-q Macaulay space the whole time.

Lemma 15 (the universal core basis). PROVED Write $s = x + y, p = xy$. In these symmetric variables the two core coordinates normalize by invertible row operations to

$$H_0 = p^2 + bp + cs^2 + ds + e, \quad H_1 = ps + fp + gs^2 + hs + i. \tag{33}$$

Over the localized ring $\mathbb{Z}[b, c, d, e, f, g, h, i]\left[(c + g^2)^{-1}\right]$ the grevlex ($x > y$) Gröbner basis of (H_0, H_1) has exactly four elements, of total degrees $4, 4, 3, 3$ and leading monomials xy^3, y^4, x^3, x^2y. The only nonconstant denominator arising in the computation is $c + g^2$, and for the Semaev specialization

$$c + g^2 = (m_1^2 - 4m_0)t_1^2/4 \neq 0. \tag{34}$$

Proof. The exact certificate `certify_quadratic_family.py` checks every one of the six Buchberger pairs over the localized ring, records explicit basis representations, and finds maximum denominator power 3 in $(c + g^2)$. The nonvanishing of $c + g^2$ uses irreducibility of the odd-characteristic quadratic modulus (so its discriminant $m_1^2 - 4m_0 \neq 0$) and $t_1 \neq 0$; a quartic top-part minor of determinant -1 certifies the rank claim after every valid finite-field specialization. The results are stored in `certify_quadratic_family_20260723.json`. □

Theorem 16 (unconditional solving-degree upper bound). PROVED For every odd prime power $q \geq 5$ and non-base target, $\mathsf{sd}_{\mathrm{grevlex}(F)} \leq q$.

Proof. By the lemma the four core-basis elements have degree ≤ 4 and lie in the closed degree-5 core space $V_{\{G_0,G_1\},5}$: three appear in the initial degree-5 Macaulay span and the fourth is obtained by multiplying lower-degree rows inside the closed space. Divide $x^q - x$ and $y^q - y$ by this basis; the leading monomials xy^3, y^4, x^3, x^2y leave remainders r_x, r_y supported on standard monomials of degree ≤ 3. Polynomial division is degree-compatible and the basis is already in $V_{F,q}$, so $r_x, r_y \in V_{F,q}$. The mutant family

$$F' = \{\text{four core-basis elements}, r_x, r_y\} \tag{35}$$

generates (F), has maximum input degree ≤ 4, and has degree of regularity ≤ 4 because its top ideal already contains leading monomials covering every degree-4 monomial. Salizzoni's Proposition 3.10 [8],

$$\mathsf{sd}_{\sigma(F')} \leq \max\left\{d_{\mathrm{reg}(F')} + 1, \max_{f \in F'} \deg f\right\}, \tag{36}$$

gives $\mathsf{sd}(F') \le 5$. Since $F' \subseteq V_{F,q}$ and $q \ge 5$, closed-space stability yields $V_{F',5} \subseteq V_{F,q}$, so a grevlex basis of $(F') = (F)$ lies in $V_{F,q}$, i.e. $\mathsf{sd}_{\mathrm{grevlex}(F)} \le q$. □

8.2 Extension-uniform refinement at factor-base size two

The quadratic-extension proof is not confined to $n = 2$. Its mechanism extends to every non-base target once the degree of the target over the base field is split into two cases.

Theorem 17 (all-extension factor-base-size-two bound). PROVED Let q be odd, let E be a nonsingular short-Weierstrass curve over $\mathbb{F}_{q^n}$, and let the target coordinate $T \in \mathbb{F}_{q^n}$ with $T \notin \mathbb{F}_q$. For the $m = 2$ Weil system with field equations,

$$\mathsf{sd}_{\mathrm{grevlex}(F)} \le \max(q, 5). \tag{37}$$

In particular $\mathsf{sd}_{\mathrm{grevlex}(F)} \le q$ for every $q \ge 5$, independently of n.

Proof. PROVED Put $p = xy$ and $s = x + y$. The f_3 formula is

$$p^2 - 2Tps + T^2 s^2 + (-2A - 4T^2)p + (-2AT - 4B)s + A^2 - 4BT. \tag{38}$$

If $\left[\mathbb{F}_{q(T)} : \mathbb{F}_q\right] \ge 3$, then $1, T, T^2$ are independent. Row operations on the Weil coordinates isolate three equations with top parts

$$p^2, \quad -2ps, \quad x^2 + \mu xy + y^2 \tag{39}$$

for some $\mu \in \mathbb{F}_q$; all complementary coordinates have degree at most two. For $\mu \ne 1$, their top ideal has grevlex basis

$$y^4, \quad xy^2 + y^3/(\mu - 1), \quad x^2 + \mu xy + y^2. \tag{40}$$

For $\mu = 1$, it has basis $y^3, x^2 + xy + y^2$. In both branches its degree of regularity is 4, and every standard monomial has degree at most 3.

Salizzoni's proposition therefore places a core Gröbner basis in the closed degree-5 space. Division of the field equations leaves remainders of degree at most 3. Repeating the preceding mutant argument puts a Gröbner basis of the full ideal in $V_{F,q}$ when $q \ge 5$. At $q = 3$, retaining the degree-3 field equations in the normalized family gives solving degree at most 5 directly.

If $\left[\mathbb{F}_{q(T)} : \mathbb{F}_q\right] = 2$, the preceding quadratic-modulus lemma applies on $\mathrm{span}_{\mathbb{F}_q}\{1, T\}$; complementary Weil coordinates again have degree at most two and can only enlarge the replacement top ideal. These two cases exhaust every non-base target. □

Remark 18 (cubic-extension certificate). EMPIRICAL: $q in {3,5,7,11}$, exact known roots `certify_cubic_extension_family_20260723.json` records the invertible $(1, T, T^2)$ coordinate changes, both top-ideal branches, core regularity 4, degree-at-most-2 field remainders in the tested systems, and original solving degree 4.

The global theorem is the literal P1.3 deliverable; this sharper result shows how Semaev structure improves it from roughly $2q$ to q when $m = 2$, with *no* appeal to the first-fall heuristic. We tried the more obvious route first — bounding solving degree by the Castelnuovo–Mumford regularity of the homogenized input, per Caminata–Gorla [11] — and it fails: the representative $q = 5$ system is *not* t-saturated, its saturation adding the low-degree elements $x + y - t$ and $y^2 - ty$. Remark 4.6 of [11] is precisely this warning, and it is why the mutant-family route is necessary.

8.3 A conditional matching lower bound

Theorem 19 (conditional lower bound and exact equality). CONDITIONAL: (F) ⊋ C If at least one field equation lies outside the core ideal C, then $\mathsf{sd}_{\mathrm{grevlex}(F)} \geq q$, and combined with the upper bound, $\mathsf{sd}_{\mathrm{grevlex}(F)} = q$.

Proof. For $d < q$ the degree-q field equations cannot enter the closed space, so $V_{F,d} = V_{\{G_0,G_1\},d} \subseteq C$. If this space contained a Gröbner basis of (F), then $(F) \subseteq C$, contradicting $(F) \supsetneq C$. Hence no cutoff below q suffices, and $\mathsf{sd}(F) \geq q$. □

So the entire equality $\mathsf{sd} = q$ hinges on whether the field equations are *redundant* over the core. Because C is symmetric in x, y, either both field equations belong to C or neither does, and the redundancy question has a clean algebraic characterization.

Proposition 20 (the redundancy criterion). PROVED Let $A_C = \mathbb{F}_q[x,y]/C$. The universal core basis has standard monomials $1, y, y^2, y^3, x, xy, xy^2, x^2$, so $\dim_{\mathbb{F}_q} A_C = 8$. The following are

(1) $x^q - x, y^q - y \in C$;
(2) both field-equation normal forms by the core basis are zero;
(3) the q-Frobenius endomorphism of A_C is the identity;
(4) $A_C \cong \mathbb{F}_q^8$;

equivalent: (5) the core has eight distinct algebraic-closure zeros, all in $\mathbb{F}_q^2$.

Nonredundancy — the hypothesis of the equality theorem — is exactly the failure of (1)–(5). One might hope it is *automatic* for genuine on-curve Semaev systems. It is not, and that is the subject of the next section.

9 Refuting automatic field-equation nonredundancy

Session four's decisive finding is a negative one, and we present it as such: the tempting conjecture that a nonsingular curve with an on-curve non-base target always yields nonredundant field equations is *false*, with an infinite explicit counterexample family.

Theorem 21 (an infinite redundant Semaev family). PROVED Let $q \equiv 3 \bmod 4$, $q \geq 7$, and $\mathbb{F}_{q^2} = \mathbb{F}_q[u]/(u^2+1)$. Choose $h \in \mathbb{F}_q^\times \setminus \{1, -1\}$ and set

$$\rho = (h + h^{-1})/2, \quad \sigma = (h^{-1} - h)/2, \quad a = -4\sigma^2. \tag{41}$$

Then $E : Y^2 = X^3 + aX$ is nonsingular, the point $R = (2u, 2\rho(1-u))$ lies on E with non-base x-coordinate, and the two coordinates of $f_3(x, y, 2u)$ generate the same ideal as

$$H_0 = (xy - a)^2 - 4(x - y)^2, \quad H_1 = (x + y)(xy + a). \tag{42}$$

Both field equations $x^q - x, y^q - y$ are redundant: they lie in $C = (H_0, H_1)$.

Proof. Since -1 is a nonsquare (as $q \equiv 3 \bmod 4$) and $\rho^2 - \sigma^2 = 1$, one has $\rho \neq 0$ and, by the restriction on h, $\sigma \neq 0$, so $a \neq 0$ and E is nonsingular. Both sides of the curve equation at R equal $-8\rho^2 u$. The branch $x + y = 0$ of C gives the four points $(z, -z)$ with $z \in \{\pm 2(1+\rho), \pm 2(1-\rho)\}$; the branch $xy = -a = 4\sigma^2$ gives two ordered roots of sum $4\sigma\rho$ (discriminant $16\sigma^4$), their swap, and both negatives. These eight points are distinct and lie in $\mathbb{F}_q^2$; a collision between branches would make -1 a square. The universal basis gives quotient dimension 8 (its sole specialization factor

is $(m_1^2 - 4m_0)t_1^2/4 = -4 \neq 0$ here), so eight distinct zeros force $A_C \cong \mathbb{F}_q^8$; by the redundancy criterion the field equations belong to C. □

Corollary 22 (the smallest concrete counterexample). PROVED Take $q = 7$, $h = 2$, so $\rho = 3, \sigma = 1, a = 3$. Over $\mathbb{F}_{49} = \mathbb{F}_7[u]/(u^2 + 1)$ use $E : Y^2 = X^3 + 3X$ and $R = (2u, 6 + u)$. Then both field-equation normal forms vanish and

$$\left(d_{\mathrm{ff}}, d_{\mathrm{reg}}, \mathsf{sd}_{\mathrm{grevlex}}\right) = (5, 7, 5). \tag{43}$$

Proof. The core generators are $G_0 = x^2y^2 + 3x^2 + 2xy + 3y^2 + 2$ and $G_1 = 3x^2y + 3xy^2 + 2x + 2y$, with reduced grevlex basis $\{xy^3 - 3x^2 + xy - 2, y^4 - 3y^2 + 2, x^3 + x + y^3 + y, x^2y + xy^2 + 3x + 3y\}$. Exact division gives zero normal forms for both $x^7 - x$ and $y^7 - y$. The closed degree-4 space has rank 4 and omits two basis elements; the degree-5 space contains all four. Hence $\mathsf{sd} = 5$, strictly below $d_{\mathrm{reg}} = 7$. The certificate `certify_quadratic_field_equations.py` checks the symbolic family over $\mathbb{Z}[1/2, h, h^{-1}, u]/(u^2 + 1)$ and the concrete normal forms, quotient multiplication matrices, and closed spaces. □

This is a counterexample *inside the actual on-curve Semaev family*, not merely inside an abstract family with the same top-degree shape. Its eight core zeros, split cleanly across the two branches, are shown in the right panel of Figure 2. The left panel is the exhaustive census that both locates these six redundant $q = 7$ systems and confirms their absence at $q = 5, 9$.

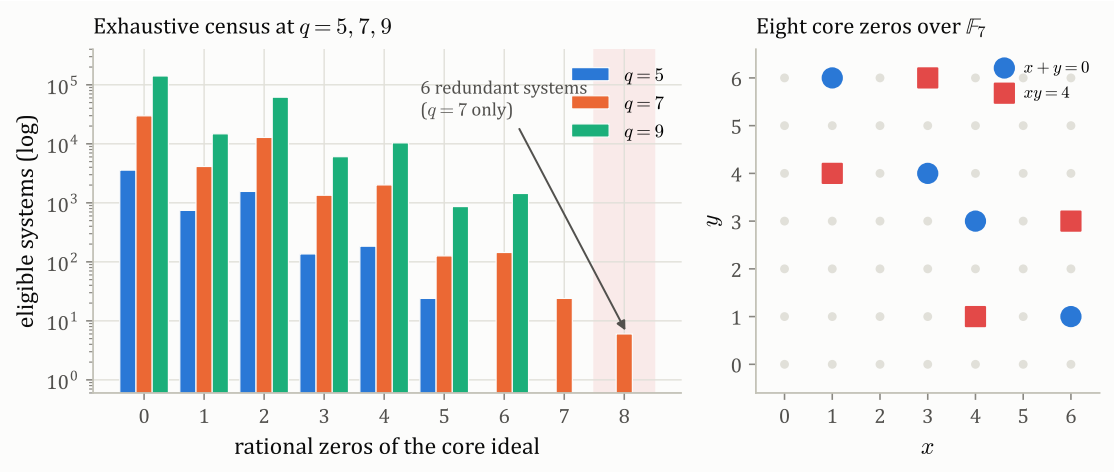

Figure 2: EMPIRICAL: exhaustive q=5,7,9 *Left:* histogram of the number of rational core-ideal zeros over all eligible nonsingular curve/non-base-target systems; redundancy requires the maximum count of eight, achieved only by six systems at $q = 7$. *Right:* the eight base-field core zeros of the $q = 7$ counterexample, four on the branch $x + y = 0$ and four on $xy = 4$. Data: `search_quadratic_redundancy_20260723.json`, `certify_quadratic_field_equations_20260723.json`.

Consequently the unconditional statement is $\mathsf{sd} \leq q$, and the equality $\mathsf{sd} = q$ genuinely requires the nonredundancy hypothesis — which cannot be dropped. We flag this exactly as the research log does: a former six-prime solving-degree *conjecture* survives only as a *conditional* theorem.

10 Empirical validation

Every proved value is anchored by exact measurement, and the honest ranges, censored rows, and search counts are reported without smoothing.

10.1 The measured degree table

Figure 3 plots the two families that matter, and Table 1 tabulates the underlying rows. All values come from exact closed Macaulay spaces with SymPy-verified Gröbner-basis containment; a dash is a *censored* value, never an estimate.

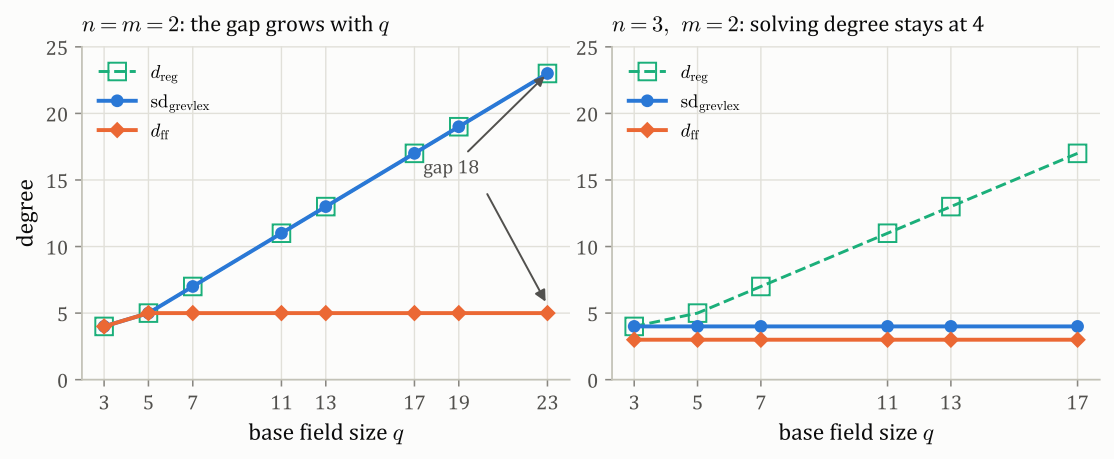

Figure 3: EMPIRICAL: known-target rows, q up to 23 *Left:* $n = m = 2$. First fall stays at 5 while $\mathsf{sd} = d_{\mathrm{reg}} = q$, so the solving-minus-first-fall gap grows to 18 at $q = 23$. *Right:* $n = 3, m = 2$. Here sd stays at 4 while d_{reg} climbs with q — a live demonstration that d_{reg} and sd are different columns. Data: `first_fall_vs_solving_20260722.csv`.

Table 1: Known-target subset of `first_fall_vs_solving_20260722.csv`. The $n = m = 2$ block realizes the exact theorem; the $n = 3, m = 2$ block shows $\mathsf{sd} = 4 < d_{\mathrm{reg}} = q$; the last rows reach the resource boundary ($q = 5, m = 4$ is censored after the regularity stage at 60 s).

q	n	m	d_{ff}	d_{reg}	sd	$\mathsf{sd} - d_{\mathrm{ff}}$	root
3	2	2	4	4	4	0	✓
5	2	2	5	5	5	0	✓
7	2	2	5	7	7	2	✓
11	2	2	5	11	11	6	✓
13	2	2	5	13	13	8	✓
17	2	2	5	17	17	12	✓
19	2	2	5	19	19	14	✓
23	2	2	5	23	23	18	✓
3	3	2	3	4	4	1	✓
5	3	2	3	5	4	1	✓
7	3	2	3	7	4	1	✓
11	3	2	3	11	4	1	✓
13	3	2	3	13	4	1	✓
17	3	2	3	17	4	1	✓
5	2	3	12	12	12	0	✓
5	3	3	11	12	12	1	✓
3	2	4	8	8	8	0	✓
5	2	4	16	16	—	—	✓

Two independent separations appear in one table. In the $n = m = 2$ block, $\mathsf{sd} - d_{\mathrm{ff}}$ grows as $q - 5$; in the $n = 3, m = 2$ block, d_{reg} grows to q while sd is pinned at 4. The first refutes "first fall approximates solving"; the second refutes "regularity equals solving." Both are exactly the confusions P1.3 targets.

10.2 Curve/target variation and exhaustive searches

Beyond the single known target, we varied curves and targets extensively. Table 2 collects the two kinds of evidence: a structured verified-root sample, and *exhaustive* enumeration at small q.

Table 2: Validation searches. The 397-case structured sample (`quadratic_family_summary_20260722.csv`) fixed a non-base coefficient of A and so *missed* the base-defined counterexample family — a selection bias the exhaustive $q = 7$ enumeration (`search_quadratic_redundancy_20260723.json`) exposed. The abstract trial (`search_quadratic_counterexamples_20260722.csv`) hits $c + g^2 = 0$, the very denominator pole excluded by the Semaev modulus.

Search	q	Eligible	Redundant	Outcome
Structured verified-root sample	5	171	0	all $(5, q, q)$
(fixed non-base A_1)	7	190	0	all $(5, q, q)$
	11	36	0	all $(5, q, q)$
Exhaustive curve/target	5	6,228	0	no redundant core
	7	50,376	6	six redundant systems
	9	236,160	0	no redundant core
Abstract top-shape trials	5	566	—	tuple $(3, 1, 4, 0, 1, 2, 0, 3)$: $\mathsf{sd} = 6$

Three lessons are recorded. First, the exhaustive $q = 7$ search finds *all six* redundant systems and matches the infinite-family construction; the structured sampler found none because it fixed a nonzero extension coordinate of A, excluding the base-defined curves $Y^2 = X^3 + aX$ where redundancy occurs. Second, at $q = 9$ (the smallest non-prime odd prime power in scope) an exhaustive search over 236,160 eligible on-curve targets finds no redundant core, consistent with the family's $q \equiv 3 \bmod 4$ hypothesis. Third, the abstract counterexample $(3, 1, 4, 0, 1, 2, 0, 3)$ with $\mathsf{sd} = 6$ shows the top shape *alone* does not force $\mathsf{sd} \le q$: the nonvanishing of $c + g^2$ is essential, and it fails for that abstract tuple while holding for every genuine Semaev system.

11 Relation to prior bounds, obstruction, and limitations

The result sits precisely against the literature it draws on, and its boundaries are sharp.

Against the first-fall heuristic. Petit and Quisquater [4] assume $d_{\mathrm{reg}} \approx d_{\mathrm{ff}}$ for binary Weil systems; for our odd-characteristic quadratic family $d_{\mathrm{reg}} = q$ while $d_{\mathrm{ff}} = 5$, so the proxy is off by $q - 5$. More decisively, the $m = 3$ family has $d_{\mathrm{ff}} = 14$ and $\mathsf{sd} \ge q$, so the same invariant gap is unbounded at the first unresolved $m > 2$ boundary. This does not claim that every binary square core is hard; it proves that first fall cannot support a *universal* solving-degree theorem. Hodges, Petit, and Schlather [5] anticipated the logical gap by labelling closeness a heuristic; we make the failure quantitative.

Against general invariant-gap examples. Caminata and Gorla [7] already prove families with arbitrarily large gaps in either direction, and their Example 4.2 has $d_{\mathrm{ff}} = 3$, $\mathsf{sd} = q - 1$, $d_{\mathrm{reg}} = 2q - 2$ even after field equations. Our contribution is *not* the existence of a gap in the abstract; it is an

exact *nonsingular Semaev/Weil family* with on-curve non-base targets, verified roots, fixed first fall, exact regularity, and a solving-degree interval linear in q.

Against the solving-degree bounds we use. Caminata, Ceria, and Gorla [9] give general Weil-restriction solving-degree bounds via homogenized source regularity; Salizzoni [8] gives the closed-space bound we invoke. The field-equation monomial ideal converts Salizzoni's theorem into the explicit global function $\max(m(q-1)+2, m2^{m-1})$ without source-regularity assumptions. The underdetermined theorem proves that its exponent in q is optimal whenever $n < m$: there $q \le \mathsf{sd} \le O(mq + m2^m)$. A finer theorem may improve constants or square-core behavior, but cannot restore a universal first-fall-scale bound.

Limitations, stated without hedging. The global theorem covers every q, n, m. The extension-uniform $\max(q, 5)$ refinement covers odd-characteristic $m = 2$, while the exact three-invariant classification holds only for $n = m = 2$. Automatic field-equation nonredundancy is *false*, so the equality half of that classification is conditional. The $m = 3$ obstruction is also in odd characteristic and gives an interval $q \le \mathsf{sd} \le 2q + 2$, not an exact solving degree. It settles the universal question but does not classify square or overdetermined cores $n \ge m > 2$. The $q = 5, m = 4$ cases were censored after the exact first-fall and regularity stages ($d_{\mathrm{ff}} = d_{\mathrm{reg}} = 16$) but before Gröbner-basis containment at a 60-second ceiling.

12 Conclusion

P1.3 asked for an unconditional, explicit degree bound on Weil-restricted Semaev systems that does not lean on the first-fall heuristic. The global answer is

$$d_{\mathrm{reg}} \le m(q-1)+1, \quad \mathsf{sd} \le \max(m(q-1)+2, m2^{m-1}), \tag{44}$$

for every q, n, m and every degree-compatible order. It follows from the field-equation top ideal, Semaev's degree formula, and Salizzoni's theorem — a proof, not a heuristic, and independent of n.

The linear q term is not removable from a universal theorem. Every proper underdetermined core $n < m$ has $\mathsf{sd} \ge q$. In an explicit infinite $n = 2, m = 3$ family,

$$d_{\mathrm{ff}} = 14, \quad d_{\mathrm{reg}} = 2q + 1, \quad q \le \mathsf{sd} \le 2q + 2. \tag{45}$$

The first-fall/solving gap is therefore unbounded inside genuine Semaev–Weil systems. In the regime $n \asymp \log q$, any solvable choice $m > n$ already forces a degree lower bound exponential in n.

Structure makes the answer much sharper at $m = 2$: for every odd-characteristic extension and non-base target, $\mathsf{sd} \le \max(q, 5)$. At $n = 2$ we additionally prove $d_{\mathrm{ff}} = 5$ and $d_{\mathrm{reg}} = q$ exactly. When the field equations enlarge the core, the solving-minus-first-fall gap is $q - 5$, reaching 18 at $q = 23$. When they do not, the equality fails: an infinite on-curve family for every $q \equiv 3 \bmod 4$, a concrete $q = 7$ certificate, and exhaustive search prove that automatic nonredundancy is false.

P1.3 is therefore closed in both senses relevant to the question: an unconditional explicit upper bound exists, and the stronger hope that a first-fall-scale bound might hold universally is false. Sharpening constants or classifying square cores can refine the picture, but cannot change either conclusion.

Reproducibility

All computations are exact over prime fields and polynomial-basis extensions using Python 3.13.4 and SymPy 1.14.0; Sage, Singular, msolve, and Macaulay2 were unavailable in the working environment, and the closed-Macaulay solving-degree routine is a hand-built exact implementation. The measurement scripts are `measure_toy_degrees.py` (the four-degree separation), `sparse_weil.py` and `measure_semaev_stats.py` (Semaev expansion and Weil restriction), `measure_weil_degrees.py` (the canonical degree table), `measure_quadratic_variants.py` and `summarize_quadratic_variants.py` (curve/target variation), `certify_quadratic_family.py` (the localized-ring core certificate), `certify_quadratic_field_equations.py` (the infinite counterexample family and the $q = 7$ certificate), `certify_cubic_extension_family.py` (the extension-uniform $m = 2$ mechanism), `certify_global_field_bound.py` (the all-parameter monomial and stored-matrix audit), `certify_underdetermined_obstruction.py` (the height obstruction, symbolic $m = 3$ family, and $q = 7, 11, 19$ specializations), and `search_quadratic_redundancy.py` and `search_quadratic_counterexamples.py` (the exhaustive and abstract searches). Each degree row records the field model, curve, target, root check, engine/version, monomial order, resource ceilings, elapsed time, and last completed pipeline stage; censored rows are preserved as such and never extrapolated. Every mathematical claim above carries one of the epistemic tags PROVED, CITED, CONDITIONAL: hypothesis, or EMPIRICAL: range as used in the research log; untagged sentences are exposition, not claims.

References

[1] I. Semaev, "Summation polynomials and the discrete logarithm problem on elliptic curves." 2004.

[2] P. Gaudry, "Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem," *Journal of Symbolic Computation*, vol. 44, no. 12, pp. 1690–1702, 2009.

[3] C. Diem, "On the discrete logarithm problem in elliptic curves," *Compositio Mathematica*, vol. 147, no. 1, pp. 75–104, 2011.

[4] C. Petit and J.-J. Quisquater, "On polynomial systems arising from a Weil descent," in *ASIACRYPT 2012*, in LNCS, vol. 7658. 2012, pp. 451–466.

[5] T. J. Hodges, C. Petit, and J. Schlather, "First fall degree and Weil descent," *Finite Fields and Their Applications*, vol. 30, pp. 155–177, 2014.

[6] S. Kousidis and A. Wiemers, "On the first fall degree of summation polynomials," *Journal of Mathematical Cryptology*, vol. 13, no. 3–4, pp. 229–237, 2019.

[7] A. Caminata and E. Gorla, "Solving degree, last fall degree, and related invariants," *Journal of Symbolic Computation*, vol. 114, pp. 322–335, 2023.

[8] F. Salizzoni, "An upper bound for the solving degree in terms of the degree of regularity." 2023.

[9] A. Caminata, M. Ceria, and E. Gorla, "The complexity of solving Weil restriction systems," *Journal of Algebra*, vol. 621, pp. 116–133, 2023.

[10] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, vol. 150. in Graduate Texts in Mathematics, vol. 150. Springer, 1995.

[11] A. Caminata and E. Gorla, "Solving multivariate polynomial systems and an invariant from commutative algebra," in *PQCrypto 2021*, in LNCS, vol. 12542. 2021, pp. 3–36.