

Algorithmic List Decoding at Capacity and Optimal Proximity Gaps for Reed–Solomon Codes

Fernando Granha Jeronimo*

September 5, 2026

Abstract

We give a unified hidden-derivative framework for list decoding and mutual correlated agreement of ordinary Reed–Solomon codes over prime fields, on arbitrary prescribed evaluation sets. For every fixed slack $\gamma > 0$, every sufficiently large block length n , every prime $q \geq n$, and every dimension $1 \leq k \leq (1 - \gamma)n$, a deterministic algorithm finds all codewords within relative distance $1 - k/n - \gamma$ in $q^{O_\gamma(1)}$ time. The final list has size $n^{O_\gamma(1)}$, independently of q . Both statements extend to bounded-input-list recovery, with constants depending additionally on the input-list bound.

For every fixed curve degree ℓ , at most $n^{O_{\gamma,\ell}(1)}$ parameters on a curve $f_0 + zf_1 + \dots + z^\ell f_\ell$ admit a nearby codeword whose exact agreement support is not a maximal jointly explained support of the coefficient words. For lines this gives MCA error $n^{O_\gamma(1)}/q$, with no proximity loss.

The interpolation stage reparameterizes and optimizes the hidden-derivative construction of Brakensiek, Chen, Putterman, Zhang, and Zheng; differential root enumeration uses Kopparty’s algorithm. We then prove that a specialization-safe differential equation has a cover by constant-dimensional varieties of polynomial cumulative degree, outside polynomially many parameter values. Intersecting these varieties with equations from the full agreement support yields both the field-size-independent list bound and exact-support MCA.

*University of Illinois, Urbana-Champaign. granha@illinois.edu. arXiv submission Sat, 5 Sep 2026 00:22:16 EST

Contents

1	Introduction	3
1.1	Main results	3
1.2	The common interpolation theorem	4
1.3	From differential equations to exact supports	5
1.4	Context and scope	6
2	Preliminaries	6
2.1	Hasse derivatives	6
2.2	Sparse list recovery and padding	7
2.3	Agreement supports and mutual correlated agreement	7
3	Hidden-derivative interpolation	8
3.1	The interpolation space	8
3.2	Local constraints and root multiplicity	9
3.3	Dimension of the interpolation space	10
3.4	Tail-monomial geometry	11
3.5	The local rank bound	12
3.6	The global interpolation theorem	14
3.7	The coefficient-level interpolation interface	16
4	Uniform parameters and deterministic decoding	16
4.1	Padding at the actual rate	16
4.2	Prime-field differential-equation root finding	17
4.3	Sparse list recovery and its running time	18
5	Symbolic interpolation and solution geometry	19
5.1	A primitive polynomial interpolant over $\mathbb{F}_q[Z]$	19
5.2	Cumulative degree	20
5.3	Effective jet decomposition of the solution locus	21
6	List bounds independent of the field size	26
7	Support-preserving descent and mutual correlated agreement	27
7.1	Descent along the full agreement support	27
7.2	Proof of the MCA theorem	29
8	Consequences and quantitative scope	31
8.1	Coordinate transformations, punctures, and erasures	31
8.2	Fixed interleaving	31
8.3	Fixed-slack certificates for the proximity challenges	31
8.4	Field characteristic and the endpoint	32
8.5	Effectivity and remaining quantitative questions	32
A	Transfer to other root-enumeration settings	35
B	Quantitative derivative order and parameter ledger	35
B.1	Inverting the sparse-incidence condition	35
B.2	Rounding and field-size thresholds	36
B.3	Parameter ledger	37

1 Introduction

Let $D = \{\alpha_1, \dots, \alpha_n\} \subseteq \mathbb{F}_q$ consist of distinct points. The Reed–Solomon code

$$\text{RS}_{\mathbb{F}_q}(D, k) = \{(P(\alpha_1), \dots, P(\alpha_n)) : P \in \mathbb{F}_q[X], \deg P < k\}$$

has rate k/n and minimum distance $n - k + 1$ [RS60, Sin64]. List decoding asks for all codewords near a received word, rather than a unique closest codeword. At rate R , the large-alphabet capacity benchmark is the radius $1 - R$; the fixed-slack objective is efficient decoding at every radius $1 - R - \gamma$ with $\gamma > 0$ fixed. For ordinary Reed–Solomon codes, the classical general algorithmic guarantee is the Johnson radius $1 - \sqrt{R}$, from the interpolation algorithms of Sudan and Guruswami–Sudan [Sud97, GS99].

A second question concerns how nearby codewords behave when the received word varies algebraically. Given coefficient words $f_0, \dots, f_\ell \in \mathbb{F}_q^n$, consider

$$y(z) = \sum_{j=0}^{\ell} z^j f_j.$$

Ordinary correlated agreement seeks one large set of coordinates on which all the f_j are simultaneously explained by codewords. Mutual correlated agreement (MCA) asks for more: outside a small exceptional set of parameters, the *entire exact agreement support of every nearby codeword* must already be jointly explained. This property was introduced in WHIR [WHIR25] and is relevant to the soundness of Reed–Solomon proximity protocols [BCIKS20, ABF26].

We treat these two questions through the same differential interpolant. Root enumeration gives a decoder. A bounded-complexity description of the solution locus gives a list bound independent of the field size and, in the parametric setting, the stronger exact-support MCA conclusion.

1.1 Main results

For lists $S_1, \dots, S_n \subseteq \mathbb{F}_q$, write

$$\mathcal{L}(D, k, \mathbf{S}, A) := \{P \in \mathbb{F}_q[X] : \deg P < k, |\{i : P(\alpha_i) \in S_i\}| \geq A\}.$$

Singleton lists recover ordinary list decoding.

Theorem 1.1 (Capacity decoding and field-size-independent lists). *Fix $\gamma \in (0, 1)$ and an integer $L \geq 1$. There are effective constants $C_{\text{alg}} = C_{\text{alg}}(\gamma, L)$, $C_{\text{list}} = C_{\text{list}}(\gamma, L)$, and $n_0 = n_0(\gamma, L)$ such that the following holds. Let $n \geq n_0$, let $q \geq n$ be prime, let $D \subseteq \mathbb{F}_q$ have n distinct points, and let $1 \leq k \leq (1 - \gamma)n$. For arbitrary lists $|S_i| \leq L$, all polynomials in*

$$\mathcal{L}(D, k, \mathbf{S}, k + \lceil \gamma n \rceil)$$

can be found deterministically using at most $q^{C_{\text{alg}}}$ field operations. Moreover,

$$|\mathcal{L}(D, k, \mathbf{S}, k + \lceil \gamma n \rceil)| \leq n^{C_{\text{list}}}.$$

In particular, every such Reed–Solomon code is list decodable at radius $1 - k/n - \gamma$, with polynomial list size independent of q and deterministic polynomial time whenever $q = n^{O(1)}$.

The constants are uniform in the actual dimension k , not merely in a prescribed constant rate. For every fixed $R \in (0, 1)$ and $\gamma \in (0, 1 - R)$, the theorem therefore gives decoding at radius $1 - R - \gamma$ for every $k \leq Rn$. Linear-size prime fields are allowed. The final list-size estimate is stronger than the $q^{O(r)}$ bound on all differential-equation roots: it counts only roots passing the agreement filter. The geometric argument proving this distinction is in [Section 6](#).

For MCA, put $A_\rho = n - \lfloor \rho n \rfloor$. A support $S \subseteq [n]$ is *jointly explained* by $\mathbf{f} = (f_0, \dots, f_\ell)$ if there are degree-below- k polynomials $P_0, \dots, P_\ell$ such that $P_j(\alpha_i) = f_{j,i}$ for all $i \in S$ and all j . A parameter z is bad if some degree-below- k polynomial P has at least A_ρ agreements with $y(z)$, but its full agreement support is not a maximal jointly explained support. We give the formal definitions in [Section 2.3](#).

Theorem 1.2 (Fixed-slack capacity-radius curve MCA). *Fix $\gamma \in (0, 1)$ and an integer $\ell \geq 1$. There are effective constants*

$$C = C(\gamma, \ell) > 0, \quad n_0 = n_0(\gamma, \ell),$$

such that the following holds. Let $n \geq n_0$, let $q \geq n$ be prime, let $D = \{\alpha_1, \dots, \alpha_n\} \subseteq \mathbb{F}_q$ have n distinct points, and let

$$\mathcal{C} = \text{RS}_{\mathbb{F}_q}(D, k), \quad 1 \leq k \leq (1 - \gamma)n.$$

For arbitrary $f_0, \dots, f_\ell \in \mathbb{F}_q^n$ and every

$$0 \leq \rho \leq 1 - \frac{k}{n} - \gamma,$$

one has

$$\left| \text{Bad}_{\mathcal{C}, \rho}^{(\ell)}(f_0, \dots, f_\ell) \right| \leq n^C.$$

In particular, for lines,

$$\text{err}_{\text{MCA}}(\mathcal{C}, \rho) \leq \frac{n^{C(\gamma, 1)}}{q}.$$

The two main estimates have different field-size implications. The decoder applies already for $q = \Theta(n)$. The MCA estimate becomes nonvacuous only when q exceeds its polynomial exception budget. A constant-degree curve with more than that many nearby points has a jointly explained support of size at least A_ρ and is consequently close to the code at every parameter; see [Corollary 7.3](#).

1.2 The common interpolation theorem

The interpolation stage depends on the total incidence

$$M = \sum_{i=1}^n |S_i|.$$

Fix a multiplicative slack $\vartheta \in (0, 1)$ and a padded degree ceiling K with $A/(K - 1) \geq (1 - \vartheta)^{-1}$. We construct a nonzero differential interpolant of order r whenever

$$M \leq a_\vartheta(K - 1) \frac{r^\vartheta}{\log^4(er)}. \tag{1}$$

Every degree-below- K polynomial with A list hits satisfies

$$Q(X, P, P^{[1]}, \dots, P^{[r]}) \equiv 0.$$

Here $P^{[j]}$ denotes the j th Hasse derivative. The order r is free and can be taken sufficiently large, but constant, at any fixed capacity slack. Degree padding makes $K = \Theta_\gamma(n)$ even when the actual code dimension is much smaller.

The construction follows the hidden-derivative mechanism of Brakensiek, Chen, Putterman, Zhang, and Zheng [BCPZZ26]. The two-cutoff derivative-tail space, the backward-Taylor substitution, and the local-kernel mechanism are theirs. Their presentation fixes the derivative order as a function of the target agreement at the start of its interpolation section [BCPZZ26, Eq. (10)]. We establish the corresponding estimates with that order left free, then optimize the two cutoffs. The resulting dimension-to-rank ratio is

$$\Omega_\vartheta \left((K-1) \frac{r^\vartheta}{\log^4(er)} \right).$$

We also stack constraints over arbitrary point–symbol incidences and count the existing monomial space by weak compositions. These give sparse list recovery and a $q^{O_\vartheta(r)}$ interpolation algorithm. Prime-field differential root enumeration is due to Kopparty [Kop15], in the formulation recorded in [BCPZZ26].

1.3 From differential equations to exact supports

The geometric part uses more information than a black-box list-size bound. We first run interpolation over $\mathbb{F}_q(Z)$ and choose a primitive polynomial kernel vector. This produces one polynomial $Q(Z, X, Y_0, \dots, Y_r)$ that remains nonzero after every specialization $Z = z$ and contains every nearby-polynomial witness in its specialized solution locus.

The key algebraic statement, [Theorem 5.5](#), covers these witnesses outside polynomially many parameter values by varieties of dimension at most $r+1$ and polynomial cumulative degree. At an anchor α , the Hasse–Taylor equations recursively recover all coefficients beyond the initial jet. Their denominators have exponents $O(d)$ and their numerator degrees are polynomial in the message degree d and the coefficient degree of Q . Singular solutions are handled by induction on total derivative-variable degree. Thus the cover controls degree as well as dimension.

For a fixed received word, agreement at k distinct coordinates uniquely determines a polynomial. A candidate cannot lie on a positive-dimensional branch satisfying every equation from its agreement support. Successive support-hyperplane cuts therefore isolate it after at most r dimension drops. Bézout and the number of possible index tuples yield the field-size-independent list bound. With input lists, the available cuts are the M point–symbol equations.

For a curve of received words, we instead follow each witness’s *exact* support. A bad witness reaches a zero-dimensional or vertical component after constantly many proper cuts. Such components contribute only polynomially many parameter values. On a nonvertical branch where all support equations vanish identically, a Vandermonde system expresses the polynomial coefficients as a degree- ℓ polynomial in z . Transcendence of the parameter splits every remaining support equation coefficientwise, giving the coefficient codewords over $\mathbb{F}_q$. Reed–Solomon uniqueness then proves maximality of the full support.

The symbolic-specialization and jet-decomposition setup develops the framework of the unpublished ordinary-proximity companion note [PG26]; all geometric statements used here are proved in this paper, so no result is invoked from that note. The support-preserving descent, and its use for both candidate counting and MCA, make the relationship between the two conclusions explicit.

1.4 Context and scope

Related algebraic codes attain capacity through folding or derivative evaluations [PV05, GR08, GW13, Kop15, KRSW23, GHKS24, CZ25, AHS26]. Earlier work improved list decoding for suitable ordinary Reed–Solomon evaluation sets [RW14, ST23, GLS21, GST23]. Generic and random evaluation sets admit capacity list-size guarantees, including over linear-size fields [BGM24, GZ23, AGL24]; [AGG25] is the merged journal version of [GZ23, AGL24]. Our setting retains the ordinary encoding map and allows every prescribed evaluation set over a prime field. BCPZZ supplies the capacity decoder in the low constant-rate regime [BCPZZ26]; the all-rate conclusion here extends that framework, rather than replacing its interpolation mechanism.

At the Johnson radius, ordinary proximity gaps are studied in [BCIKS20, BCCHKS25], and MCA in [Hab25, BCGM26]. Fixed integer improvements beyond Johnson are obtained in [Jo26]. Goyal and Guruswami prove capacity-approaching proximity gaps and MCA for subspace-design codes and random Reed–Solomon codes over linear-size fields [GG25]. Our evaluation-set guarantee is uniform, at the expense of a much larger field-size budget for small MCA error. Counterexamples near capacity [CS25, KKH26] require care with shrinking slack: our constants depend on a fixed γ , and the theorems do not assert a uniform estimate when γ tends to zero with n .

The result is not a claim of $\text{poly}(n, \log q)$ decoding time for arbitrary large fields, constant output lists, or practical dependence on $1/\gamma$. It does give fixed-slack asymptotic certificates for both the MCA and fixed-interleaving list-size targets in the preliminary Proximity Prize statement [ABF26, Prize26]; it does not determine their largest safe radius. These consequences and limitations are stated in Section 8.

Organization. Section 2 sets notation. Section 3 proves the common interpolation theorem and its specialization-compatible matrix formulation. Section 4 gives the uniform parameter choice and the sparse decoder. Section 5 proves the symbolic construction and the jet theorem. Section 6 establishes the polynomial list bound and completes Theorem 1.1. Section 7 proves exact-support MCA. Section 8 records interleaving, coordinate transformations, and quantitative certificates. The appendices give the root-solver transfer and the more detailed parameter estimates.

2 Preliminaries

Throughout, $\log$ denotes the natural logarithm. A zero polynomial satisfies every displayed upper degree bound. We write $[n] = \{1, \dots, n\}$. For $u, v \in \mathbb{F}_q^n$, their relative Hamming distance is

$$\Delta(u, v) := \frac{1}{n} |\{i \in [n] : u_i \neq v_i\}|.$$

A code $C \subseteq \mathbb{F}_q^n$ is (ρ, L) list decodable if every Hamming ball of relative radius ρ contains at most L codewords. In list recovery, the input is a sequence of sets $S_1, \dots, S_n \subseteq \mathbb{F}_q$, and a codeword is retained when its i th symbol lies in S_i on the prescribed number of coordinates. All polynomial degrees are ordinary univariate degrees unless a weighted degree is displayed explicitly.

2.1 Hasse derivatives

For $P \in F[X]$ over a field F , the j th Hasse derivative $P^{[j]}$ is defined by

$$P(X + T) = \sum_{j \geq 0} P^{[j]}(X) T^j. \quad (2)$$

Replacing X by $X + T$ and T by $-T$ gives the backward identity

$$P(X) = \sum_{j \geq 0} P^{[j]}(X + T)(-T)^j. \quad (3)$$

If $P(\alpha) = y$, then for every $r \geq 1$,

$$P(\alpha + T) = y + \sum_{j=1}^r (-1)^{j+1} T^j P^{[j]}(\alpha + T) + T^{r+1} G_P(T) \quad (4)$$

for some $G_P \in F[T]$.

If $P(\alpha + U) = \sum_{j=0}^d c_j U^j$, then $c_j = P^{[j]}(\alpha)$ and

$$P^{[i]}(\alpha + U) = \sum_{j=i}^d \binom{j}{i} c_j U^{j-i}. \quad (5)$$

When $d < \text{char}(F)$, the binomial coefficients with $0 \leq i \leq j \leq d$ are nonzero.

2.2 Sparse list recovery and padding

Definition 2.1 (Sparse list-recovery instance). A sparse list-recovery instance consists of distinct $\alpha_1, \dots, \alpha_n \in F$, finite sets $S_1, \dots, S_n \subseteq F$ over a field F , an actual degree bound $k - 1$, and an agreement threshold A . Its incidence size is

$$M = \sum_{i=1}^n |S_i|.$$

A polynomial P is valid if $\deg P < k$ and

$$|\{i \in [n] : P(\alpha_i) \in S_i\}| \geq A.$$

Ordinary list decoding is the case $S_i = \{y_i\}$. Empty lists and coordinate-dependent list sizes are allowed.

Lemma 2.2 (Degree padding). *Suppose an algorithm outputs every polynomial of degree below K satisfying a given list-agreement condition. For every $k \leq K$, filtering its output by $\deg P < k$ solves the same problem for degree bound $k - 1$.*

Proof. Every valid degree-below- k polynomial is among the degree-below- K outputs, and the final filter removes only extraneous roots. $\square$

2.3 Agreement supports and mutual correlated agreement

Fix $\mathcal{C} = \text{RS}_{\mathbb{F}_q}(D, k)$ and a radius $\rho \in [0, 1]$ such that $A_\rho := n - \lfloor \rho n \rfloor \geq k$. For $u \in \mathbb{F}_q^n$ and $P \in \mathbb{F}_q[X]$, define

$$\text{Agr}(u, P) := \{i \in [n] : u_i = P(\alpha_i)\}.$$

For coefficient words $\mathbf{f} = (f_0, \dots, f_\ell)$, call a set $S \subseteq [n]$ *$\mathbf{f}$ -correlated* if there are polynomials $P_0, \dots, P_\ell \in \mathbb{F}_q[X]$ of degree below k such that

$$P_j(\alpha_i) = f_{j,i} \quad (i \in S, 0 \leq j \leq \ell).$$

For these coefficient words write $y(z) = \sum_{j=0}^\ell z^j f_j$. Let $\mathcal{A}_\rho(\mathbf{f})$ be the collection of inclusion-maximal $\mathbf{f}$ -correlated sets of cardinality at least $A_\rho = n - \lfloor \rho n \rfloor$.

Definition 2.3 (Bad curve parameters). For $y(z) = \sum_{j=0}^{\ell} z^j f_j$, define

$$\text{Bad}_{\mathcal{C},\rho}^{(\ell)}(\mathbf{f}) := \left\{ z \in \mathbb{F}_q : \begin{array}{l} \text{there exists } P \in \mathbb{F}_q[X], \deg P < k, \text{ with } |\text{Agr}(y(z), P)| \geq A_\rho, \\ \text{and } \text{Agr}(y(z), P) \notin \mathcal{A}_\rho(\mathbf{f}) \end{array} \right\}.$$

For $\ell = 1$, the MCA error is

$$\text{err}_{\text{MCA}}(\mathcal{C}, \rho) := \max_{f_0, f_1 \in \mathbb{F}_q^n} \frac{|\text{Bad}_{\mathcal{C},\rho}^{(1)}(f_0, f_1)|}{q}.$$

In the regime $A_\rho \geq k$, [Lemma 2.4](#) shows that an exact support of size at least A_ρ is correlated if and only if it belongs to $\mathcal{A}_\rho(\mathbf{f})$. For lines, the definition therefore agrees with the usual MCA condition [[WHIR25](#), [GG25](#)]; for curves, we use the analogous exact-support formulation.

Lemma 2.4 (Explained exact supports are maximal). *Let $z \in \mathbb{F}_q$ and let $P \in \mathbb{F}_q[X]$ have degree below k . Put*

$$S = \text{Agr}(y(z), P).$$

If $|S| \geq k$ and S is $\mathbf{f}$ -correlated, then S is inclusion-maximal among $\mathbf{f}$ -correlated sets. In particular, if $|S| \geq A_\rho \geq k$, then $S \in \mathcal{A}_\rho(\mathbf{f})$.

Proof. Choose degree-below- k polynomials $P_0, \dots, P_\ell$ explaining S . Then P and $\sum_{j=0}^{\ell} z^j P_j$ agree at every α_i with $i \in S$. Since $|S| \geq k$, Reed–Solomon uniqueness gives

$$P = \sum_{j=0}^{\ell} z^j P_j.$$

Suppose that a strict superset $T \supsetneq S$ were $\mathbf{f}$ -correlated, witnessed by $Q_0, \dots, Q_\ell$. The polynomials P and $\sum_j z^j Q_j$ agree on S , hence are equal. The latter polynomial agrees with $y(z)$ on all of T , contradicting the definition of S as the *full* agreement support of P . Thus no such T exists. $\square$

3 Hidden-derivative interpolation

All constructions in this section are over an arbitrary coefficient field F . In particular, they apply over $\mathbb{F}_q(Z)$. We prove the parameterized estimates rather than invoking the capacity decoder as a black box.

3.1 The interpolation space

We now define the family from which the interpolating polynomial will be chosen. It is a reparameterization of the two-cutoff interpolation space in [[BCPZZ26](#), Eq. (18)]: the derivative tail obeys both a weighted cutoff, adapted to the backward-Taylor substitution, and an ordinary-degree cutoff. The gap between the two cutoffs is optimized later in [Section 3.6](#), and the ordinary cutoff also permits a sharper monomial enumeration.

Fix integers A, K, r, m with $1 \leq r < K \leq A$ and write

$$u := \frac{A}{K-1}.$$

Choose real numbers

$$1 < c < s < u.$$

For

$$\mathbf{v} = (v_2, \dots, v_r) \in \mathbb{Z}_{\geq 0}^{r-1},$$

define

$$\omega(\mathbf{v}) := \sum_{j=2}^r (j-1)v_j, \quad |\mathbf{v}| := \sum_{j=2}^r v_j, \quad Y^{\mathbf{v}} := \prod_{j=2}^r Y_j^{v_j}.$$

Set

$$W := \left\lfloor \frac{crm}{\log(er)} \right\rfloor \quad (6)$$

and

$$\mathcal{T} := \left\{ \mathbf{v} \in \mathbb{Z}_{\geq 0}^{r-1} : \omega(\mathbf{v}) \leq W, |\mathbf{v}| \leq \lceil sm \rceil \right\}. \quad (7)$$

Finally put

$$B := \left\lceil \frac{mA}{K-1} \right\rceil \quad (8)$$

and let $\mathcal{Q}$ be the span of all monomials

$$X^a Y_0^{b_0} Y_1^{b_1} Y^{\mathbf{v}} \quad (9)$$

with

$$a, b_0, b_1 \in \mathbb{Z}_{\geq 0}, \quad \mathbf{v} \in \mathcal{T}, \quad b_1 \leq m, \quad (10)$$

$$b_0 + b_1 + |\mathbf{v}| \leq B, \quad (11)$$

$$a + (K-1)(b_0 + b_1 + |\mathbf{v}|) < mA. \quad (12)$$

Lemma 3.1 (Degree properties). *Every $Q \in \mathcal{Q}$ satisfies $\deg_{Y_j} Q \leq B$ for every j . Moreover,*

$$\deg_{(1, K-1, K-2, \dots, K-r-1)} Q < mA.$$

For every P with $\deg P < K$,

$$\deg_X Q(X, P, P^{[1]}, \dots, P^{[r]}) < mA.$$

Proof. The individual-degree statement follows from Equation (11). The actual differential-equation weights are no larger than the conservative weight $K-1$ used for every Y_j in Equation (12). Finally, $\deg P^{[j]} \leq K-1$ for all j , so Equation (12) also bounds the degree after specialization. $\square$

3.2 Local constraints and root multiplicity

The decoder knows only the value $P(\alpha)$, not the Hasse derivatives of P at α . The following substitution, constraints, and multiplicity argument are parameterized versions of the hidden-derivative construction of Brakensiek, Chen, Putterman, Zhang, and Zheng [BCPZZ26, Lemma 3.1].

Fix a point-symbol pair $(\alpha, y) \in F^2$. In Q , make the formal substitution

$$X = \alpha + T, \quad Y_0 = y + \sum_{j=1}^r (-1)^{j+1} T^j Y_j + TE. \quad (13)$$

Write the result uniquely as

$$Q_{\alpha, y}(T, E, Y_1, \dots, Y_r) = \sum_{b, \mathbf{e}} q_{b, \mathbf{e}}(T) E^b Y_1^{e_1} \dots Y_r^{e_r}. \quad (14)$$

For every b with $rb < m$, impose

$$q_{b,\mathbf{e}}(T) \equiv 0 \pmod{T^{m-rb}} \quad \text{for every } \mathbf{e}. \quad (15)$$

These are homogeneous linear constraints on the coefficients of Q .

Lemma 3.2 (One agreement gives multiplicity m). *If $P(\alpha) = y$ and Q obeys Equation (15) at (α, y) , then*

$$Q(\alpha + T, P(\alpha + T), P^{[1]}(\alpha + T), \dots, P^{[r]}(\alpha + T)) \equiv 0 \pmod{T^m}.$$

Proof. By Equation (4),

$$E_P(T) := \frac{P(\alpha + T) - y - \sum_{j=1}^r (-1)^{j+1} T^j P^{[j]}(\alpha + T)}{T}$$

is divisible by T^r . Substitute $Y_j = P^{[j]}(\alpha + T)$ and $E = E_P(T)$ into Equation (14). If $rb < m$, the two factors $q_{b,\mathbf{e}}(T)$ and $E_P(T)^b$ contribute divisibility T^{m-rb} and T^{rb} , respectively. If $rb \geq m$, the second factor alone is divisible by T^m . Thus every summand is divisible by T^m . $\square$

3.3 Dimension of the interpolation space

The first side of the dimension–rank comparison is a lower bound on the number of admissible interpolation monomials. The following box-counting estimate is a parameterized form of [BCPZZ26, Lemma 3.2]: the ordinary-degree buffer $s < u$ leaves a three-dimensional box in the exponents of X, Y_0, Y_1 for every derivative-tail monomial.

Lemma 3.3 (Dimension lower bound). *Fix $u_0 > 1$ and $1 < s < u_0$, and put*

$$\Delta := u_0 - s, \quad \overline{\Delta} := \min\{1, \Delta\}.$$

Whenever

$$u = \frac{A}{K-1} \geq u_0, \quad \overline{\Delta}m \geq 2,$$

we have

$$\dim \mathcal{Q} \geq \frac{\overline{\Delta}^3}{8192} |\mathcal{T}| (K-1)m^3. \quad (16)$$

In particular, for fixed constants $u_0 > s > 1$ this gives $\dim \mathcal{Q} \geq a_0 |\mathcal{T}| (K-1)m^3$ for all sufficiently large m , with $a_0 = \Omega(\min\{1, u_0 - s\}^3)$.

Proof. Set

$$\tau := \frac{\overline{\Delta}}{16}.$$

Every $\mathbf{v} \in \mathcal{T}$ satisfies

$$um - |\mathbf{v}| \geq u_0m - sm - 1 = \Delta m - 1.$$

Choose arbitrary integers

$$0 \leq b_0, b_1 \leq \lfloor \tau m \rfloor.$$

Since $b_0 + b_1 \leq 2\tau m$ and $\overline{\Delta}m \geq 2$,

$$\begin{aligned} um - |\mathbf{v}| - b_0 - b_1 &\geq \Delta m - 1 - 2\tau m \\ &\geq 4\tau m. \end{aligned} \quad (17)$$

Therefore every integer

$$0 \leq a < 4\tau(K-1)m$$

satisfies Equation (12). Since $a \geq 0$, that strict inequality also implies

$$b_0 + b_1 + |\mathbf{v}| < \frac{mA}{K-1} \leq B,$$

so Equation (11) holds; and $b_1 \leq m$ because $\tau \leq 1/16$.

Each b_i interval contains at least $\tau m/2$ integers, while the a interval contains at least $2\tau(K-1)m$ integers. Hence each $\mathbf{v} \in \mathcal{T}$ contributes at least

$$\frac{\tau m}{2} \cdot \frac{\tau m}{2} \cdot 2\tau(K-1)m = \frac{\tau^3}{2}(K-1)m^3 = \frac{\bar{\Delta}^3}{8192}(K-1)m^3$$

monomials, proving Equation (16). $\square$

3.4 Tail-monomial geometry

The local rank estimate depends on how much the set of derivative-tail monomials grows when its weighted cutoff is enlarged by m . The simplex–cube comparison and centroid–Markov argument below parameterize [BCPZZ26, Corollary 3.8 and the proof of Lemma 3.3].

For $z \geq 0$, define

$$\Lambda(z) := \left| \{ \mathbf{v} \in \mathbb{Z}_{\geq 0}^{r-1} : \omega(\mathbf{v}) \leq z \} \right|. \quad (18)$$

Let

$$\mathbf{S}_z := \left\{ x \in \mathbb{R}_{\geq 0}^{r-1} : \sum_{j=1}^{r-1} jx_j \leq z \right\}.$$

A change of variables from the standard simplex gives

$$\text{Vol}(\mathbf{S}_z) = \frac{z^{r-1}}{((r-1)!)^2}. \quad (19)$$

The usual half-open unit-cube comparison gives

$$\frac{z^{r-1}}{((r-1)!)^2} \leq \Lambda(z) \leq \frac{(z + r(r-1)/2)^{r-1}}{((r-1)!)^2}. \quad (20)$$

Indeed, flooring coordinates maps $\mathbf{S}_z$ into the union of cubes based at counted lattice points, and every such cube lies in $\mathbf{S}_{z+r(r-1)/2}$.

Lemma 3.4 (Uniform parameterized growth bound). *Let $J \subset (1, \infty)$ be compact. There are constants $C_J > 0$ and r_J such that, for every $r \geq r_J$, every $c \in J$, and every $s > c$, upon setting $m = r^3$ we have*

$$\Lambda(W + m) \leq \frac{C_J}{1 - c/s} |\mathcal{T}| r^{1/c}. \quad (21)$$

Proof. Let X be uniform on $\mathbf{S}_W$. The centroid of this simplex gives

$$\mathbb{E}|X|_1 = \frac{W}{r} \sum_{j=1}^{r-1} \frac{1}{j} \leq \frac{W \log(er)}{r} \leq cm.$$

Markov's inequality yields

$$\Pr[|X|_1 > sm] \leq \frac{c}{s}.$$

Taking coordinatewise floors maps the remaining subset of S_W into cubes based at points of $\mathcal{T}$, and the cubes are disjoint. Hence

$$|\mathcal{T}| \geq \left(1 - \frac{c}{s}\right) \frac{W^{r-1}}{((r-1)!)^2}. \quad (22)$$

Using the upper bound in Equation (20) and dividing by Equation (22),

$$\frac{\Lambda(W+m)}{|\mathcal{T}|} \leq \frac{1}{1-c/s} \left(1 + \frac{m+r(r-1)/2}{W}\right)^{r-1}. \quad (23)$$

Since $m = r^3$ and

$$W = \frac{cr^4}{\log(er)} + O(1),$$

uniformly for $c \in J$, after increasing r_J if necessary we have

$$(r-1) \frac{m+r(r-1)/2}{W} \leq \frac{1}{c} \log r + C'_J$$

for a constant C'_J depending only on J . Apply $\log(1+x) \leq x$ in Equation (23) and exponentiate, absorbing $e^{C'_J}$ into C_J . $\square$

3.5 The local rank bound

We next bound the number of independent equations imposed by one point–symbol incidence. The factorization through Γ , the kernel spaces, and the rank–nullity argument below are parameterized versions of [BCPZZ26, Lemmas 3.10–3.12]. The key is not to count all truncated coefficients directly: after a triangular change of variables, a large explicit subspace maps to zero.

Fix (α, y) . Let $\Phi_{\alpha, y}$ be the linear map that records exactly the coefficients prohibited by Equation (15). First substitute

$$X = \alpha + T, \quad Y_0 = y + TU \quad (24)$$

and reduce modulo T^m . We regard $\mathcal{V}$ and all $\mathcal{K}_\rho$ below as subspaces of $F[T, U, Y_1, \dots, Y_r]/(T^m)$; displayed generators denote residue classes, with the same convention after rewriting U in terms of E . The image lies in

$$\mathcal{V} := \text{span} \left\{ T^\rho U^a Y_1^b Y^\mathbf{v} : \begin{array}{l} 0 \leq \rho < m, \ 0 \leq a \leq \rho, \ 0 \leq b \leq m, \\ \omega(\mathbf{v}) \leq W + \rho \end{array} \right\}. \quad (25)$$

Now rewrite

$$E = U - \sum_{j=1}^r (-1)^{j+1} T^{j-1} Y_j. \quad (26)$$

Let Γ record, after this rewrite, all coefficients of monomials

$$T^i E^b Y_1^{e_1} Y^\mathbf{v} \quad \text{with } i + rb < m.$$

Then $\Phi_{\alpha, y}$ factors through Γ , so

$$\text{rank } \Phi_{\alpha, y} \leq \text{rank } \Gamma. \quad (27)$$

For $0 \leq \rho < m$, set

$$h_\rho := \left\lceil \frac{m - \rho}{r} \right\rceil. \quad (28)$$

If $\rho - h_\rho < 0$, let $\mathcal{K}_\rho = 0$. Otherwise, let $\mathcal{K}_\rho$ be spanned by

$$T^\rho E^{h_\rho} U^a Y_1^b Y^\mathbf{v} \quad (29)$$

with

$$0 \leq a \leq \rho - h_\rho, \quad 0 \leq b \leq m - h_\rho, \quad \omega(\mathbf{v}) \leq W + \rho.$$

Lemma 3.5 (Kernel spaces). *For every ρ , $\mathcal{K}_\rho \subseteq \mathcal{V} \cap \ker \Gamma$. The spaces $\mathcal{K}_0, \dots, \mathcal{K}_{m-1}$ are linearly independent, and*

$$\dim \ker \Gamma \geq \sum_{\rho=0}^{m-1} \max \{0, (\rho - h_\rho + 1)(m - h_\rho + 1)\Lambda(W + \rho)\}. \quad (30)$$

Proof. Expand E^{h_ρ} by Equation (26). If a term selects e_j copies of Y_j for $j \geq 2$, it gains both T -degree and ω -weight

$$L := \sum_{j=2}^r (j-1)e_j.$$

The resulting monomial has T -degree $\rho + L$, U -degree at most $h_\rho + a \leq \rho \leq \rho + L$, Y_1 -degree at most $h_\rho + b \leq m$, and ω -weight at most $W + \rho + L$. Every surviving term modulo T^m therefore belongs to $\mathcal{V}$.

After rewriting U in terms of $E, Y_1, \dots, Y_r$, every term in Equation (29) remains divisible by $T^\rho E^{h_\rho}$. Since $\rho + rh_\rho \geq m$, no resulting monomial is recorded by Γ . Thus $\mathcal{K}_\rho \subseteq \ker \Gamma$.

For fixed ρ , the displayed vectors are independent: their coefficient at the lowest T -degree is the common nonzero factor $(U - Y_1)^{h_\rho}$ times distinct monomials in $U, Y_1, Y_2, \dots, Y_r$. Spaces with different ρ are independent by considering the smallest nonzero T -degree in a putative relation. Counting the allowed exponents gives Equation (30). $\square$

Lemma 3.6 (Local rank). *Fix $1 < c < s$, set $m = r^3$, and define $W, \mathcal{T}$ as above. For all sufficiently large r ,*

$$\text{rank } \Phi_{\alpha, y} \leq C(c, s) |\mathcal{T}| m^3 r^{-(1-1/c)}. \quad (31)$$

The bound is uniform in (α, y) .

Proof. At fixed T -degree ρ , the space $\mathcal{V}$ has dimension

$$(\rho + 1)(m + 1)\Lambda(W + \rho).$$

By Lemma 3.5 and rank-nullity,

$$\text{rank } \Gamma \leq \sum_{\rho=0}^{m-1} B_\rho \Lambda(W + \rho), \quad (32)$$

where

$$B_\rho := (\rho + 1)(m + 1) - \max \{0, (\rho - h_\rho + 1)(m - h_\rho + 1)\}.$$

A direct expansion, including the case in which the maximum is zero, gives

$$B_\rho \leq h_\rho(\rho + m + 2), \quad h_\rho \leq \frac{m - \rho}{r} + 1.$$

Because $m = r^3$,

$$\begin{aligned} \sum_{\rho=0}^{m-1} B_{\rho} &\leq \sum_{\rho=0}^{m-1} \left(\frac{m-\rho}{r} + 1 \right) (\rho + m + 2) \\ &\leq 6 \frac{m^3}{r} \end{aligned}$$

for all sufficiently large r . Apply [Lemma 3.4](#) with any compact interval $J \subset (1, \infty)$ containing c , and use monotonicity of Λ together with [Equations \(27\) and \(32\)](#):

$$\text{rank } \Phi_{\alpha,y} \leq 6 \frac{m^3}{r} \Lambda(W + m) \leq C(c, s) |\mathcal{T}| m^3 r^{1/c-1}.$$

□

3.6 The global interpolation theorem

We now compare the dimension of $\mathcal{Q}$ with the sum of the local ranks. The first proposition records the derivative-order dependence established above by reparameterizing the dimension and rank arguments of [\[BCPZZ26\]](#) and records a fixed-shape version that makes the basic mechanism transparent. The second lets the shape approach the full degree slack and is the form used by the decoder.

We first give a clean fixed-shape formulation. Fix $\vartheta, \lambda \in (0, 1)$ and define

$$c := \frac{1}{1 - \lambda\vartheta}, \quad s := \frac{1}{2} \left(\frac{1}{1 - \lambda\vartheta} + \frac{1}{1 - \vartheta} \right). \quad (33)$$

Then

$$1 < c < s < \frac{1}{1 - \vartheta}, \quad 1 - \frac{1}{c} = \lambda\vartheta.$$

Proposition 3.7 (Fixed-shape sparse interpolant). *Fix $\vartheta, \lambda \in (0, 1)$. There are effective constants r_0 and $a_{\vartheta,\lambda} > 0$ such that the following holds. Suppose*

$$\frac{A}{K-1} \geq \frac{1}{1 - \vartheta}, \quad r \geq r_0, \quad m = r^3.$$

For a list-recovery instance of total incidence M , if

$$M \leq a_{\vartheta,\lambda} (K-1) r^{\lambda\vartheta}, \quad (34)$$

then there is a nonzero $Q \in \mathcal{Q}$ satisfying the local constraints at every incidence

$$(\alpha_i, y), \quad y \in S_i.$$

Every degree-below- K polynomial hitting at least A lists satisfies

$$Q(X, P, P^{[1]}, \dots, P^{[r]}) \equiv 0. \quad (35)$$

Proof. Apply [Lemma 3.3](#) with $u_0 = 1/(1 - \vartheta)$ and the value of s in [Equation \(33\)](#), increasing r_0 so that $\min\{1, u_0 - s\} r^3 \geq 2$. It gives

$$\dim \mathcal{Q} \geq a_0 |\mathcal{T}| (K-1) m^3.$$

By [Lemma 3.6](#), one incidence has rank at most

$$C_0 |\mathcal{T}| m^3 r^{-\lambda\vartheta}.$$

The stacked map over all M incidences has rank at most the sum of these ranks. Taking $a_{\vartheta,\lambda} < a_0/C_0$ leaves a nonzero vector in its kernel.

Let P hit the lists on a set I with $|I| \geq A$. For every $i \in I$, apply [Lemma 3.2](#) with $y = P(\alpha_i) \in S_i$. The specialization in [Equation \(35\)](#) has A distinct roots, each of multiplicity at least m . By [Lemma 3.1](#), its degree is below mA , so it is identically zero. $\square$

3.6.1 Using the full slack

We now track the constants while allowing the shape to depend mildly on r .

Proposition 3.8 (Optimized sparse interpolant). *Fix $\vartheta \in (0, 1)$. There are effective constants r_0 and $a_\vartheta > 0$ such that, for integers $2 \leq K \leq A \leq n$ and $1 \leq r < K$, whenever*

$$\frac{A}{K-1} \geq u_0 := \frac{1}{1-\vartheta}, \quad r \geq r_0, \quad m = r^3,$$

and

$$M \leq a_\vartheta (K-1) \frac{r^\vartheta}{\log^4(er)}, \tag{36}$$

there is a nonzero interpolant satisfying every incidence constraint, and every degree-below- K polynomial with at least A list hits satisfies its differential equation.

Proof. Put $L = \log(er)$ and, for sufficiently large r , choose

$$\delta := \frac{1}{L}, \quad c := u_0 - 2\delta, \quad s := u_0 - \delta. \tag{37}$$

Increasing $r_0(\vartheta)$ ensures $1 < c < s < u_0$, that

$$c \in J_\vartheta := \left[\frac{1+u_0}{2}, u_0 \right],$$

and that $\delta m = r^3 / \log(er) \geq 2$.

Apply [Lemma 3.3](#) with gap $u_0 - s = \delta$ to obtain

$$\dim \mathcal{Q} \geq c_\vartheta \delta^3 |\mathcal{T}| (K-1) m^3. \tag{38}$$

Apply the uniform form of [Lemma 3.4](#) with the compact interval J_ϑ . Since

$$\frac{1}{1-c/s} = \frac{s}{s-c} = O_\vartheta(\delta^{-1}),$$

we obtain

$$\Lambda(W+m) \leq C_\vartheta \delta^{-1} |\mathcal{T}| r^{1/c}.$$

Moreover,

$$\vartheta - \left(1 - \frac{1}{c}\right) = \frac{1}{c} - \frac{1}{u_0} = \frac{2\delta}{cu_0}.$$

Since $\delta \log r = O(1)$,

$$r^{1/c-1} = O_\vartheta(r^{-\vartheta}).$$

Combining this uniform estimate with the bound $\text{rank } \Phi_{\alpha,y} \leq 6m^3\Lambda(W+m)/r$ established in the proof of [Lemma 3.6](#) gives

$$\text{rank } \Phi_{\alpha,y} \leq C_{\vartheta} \delta^{-1} |\mathcal{T}| m^3 r^{-\vartheta}. \quad (39)$$

The total rank over all incidences is smaller than [Equation \(38\)](#) whenever

$$M \leq c'_{\vartheta}(K-1)\delta^4 r^{\vartheta},$$

which is [Equation \(36\)](#). The multiplicity argument is unchanged. $\square$

3.7 The coefficient-level interpolation interface

For symbolic applications we need the linear system itself, not just the existence of an interpolant for each received word.

Corollary 3.9 (Specialization-compatible interpolation). *Fix $\vartheta \in (0, 1)$, and let r_0, a_{ϑ} be the constants of [Proposition 3.8](#). Let F be any field, let $\alpha_1, \dots, \alpha_n \in F$ be distinct, and let $S_i \subseteq F$ be finite sets of total incidence M . Suppose*

$$\begin{aligned} 2 \leq K \leq A \leq n, \quad r_0 \leq r < K, \quad m = r^3, \\ \frac{A}{K-1} \geq \frac{1}{1-\vartheta}, \quad M \leq a_{\vartheta}(K-1) \frac{r^{\vartheta}}{\log^4(er)}. \end{aligned}$$

Put $B = \lceil mA/(K-1) \rceil$. There is a homogeneous interpolation matrix, in the fixed monomial basis of [Equations \(9\) to \(12\)](#), with a nonzero kernel. Every nonzero kernel vector gives a polynomial Q satisfying

$$\deg_Y^{\text{tot}} Q \leq B, \quad \deg_{(1, K-1, \dots, K-1)} Q < mA. \quad (40)$$

Every degree-below- K polynomial with at least A list hits satisfies

$$Q(X, P, P^{[1]}, \dots, P^{[r]}) \equiv 0. \quad (41)$$

For fixed r, B , the matrix has $O_{r,B}(n)$ columns and $O_{r,B}(M)$ rows. Each entry in the block for (α_i, y) is a polynomial of degree at most B in y . All these assertions about a kernel vector and its local constraints remain valid under extension of the coefficient field.

Proof. The matrix records exactly the coefficient constraints in [Equation \(15\)](#). The nonzero kernel is supplied by [Proposition 3.8](#). The fixed basis enforces [Equation \(40\)](#) for every vector, and the multiplicity argument in [Lemma 3.2](#) proves [Equation \(41\)](#) for every kernel vector.

For fixed r, B , there are constantly many possible Y -monomials and fewer than $mA = O_r(n)$ choices of the X -exponent. In a local block, both the truncated T -degree and every exponent in the substituted derivative variables and E are bounded in terms of r, B . Thus each incidence contributes only constantly many rows. In the substitution for Y_0 , the received symbol occurs to degree at most its original exponent, which is at most B . These are identities over the coefficient field, so extension of scalars preserves the local equations and the degree-multiplicity implication. $\square$

4 Uniform parameters and deterministic decoding

4.1 Padding at the actual rate

The following choice is shared by the algorithmic and geometric arguments. It makes the constants independent of the actual rate k/n .

Lemma 4.1 (Uniform fixed-slack parameters). *Fix $\gamma \in (0, 1)$ and an integer $L \geq 1$. For all sufficiently large n , and every pair of integers*

$$1 \leq k \leq (1 - \gamma)n, \quad k + \lceil \gamma n \rceil \leq A \leq n,$$

one can choose $r = r(\gamma, L)$ and $m = r^3$, independently of n, k, A , so that, with

$$\vartheta := \frac{\gamma}{2}, \quad K := \lceil (1 - \vartheta)A \rceil, \quad (42)$$

all hypotheses of [Corollary 3.9](#) hold for every instance with total incidence $M \leq Ln$. Moreover,

$$K - k \geq \frac{\gamma n}{2}, \quad B = \left\lceil \frac{mA}{K - 1} \right\rceil \leq B_{\gamma, L} \quad (43)$$

for an effective constant $B_{\gamma, L}$. For every prime $q \geq n$, after increasing the same lower threshold for n , one also has

$$r < K \leq q, \quad B < q, \quad r^3 A < q^2.$$

Proof. Choose an integer $r \geq r_0(\vartheta)$ sufficiently large that

$$1 \leq \frac{a_\vartheta(1 - \vartheta)\gamma}{3L} \frac{r^\vartheta}{\log^4(er)}. \quad (44)$$

Such an effective choice exists because $r^\vartheta / \log^4(er)$ tends to infinity. Since $A \geq k + \gamma n$ and $k + \gamma n \leq n$,

$$K - k \geq (1 - \vartheta)(k + \gamma n) - k = \gamma n - \vartheta(k + \gamma n) \geq \gamma n/2. \quad (45)$$

For sufficiently large n , $2 \leq K \leq A$ and $r < K$. Also

$$K - 1 < (1 - \vartheta)A, \quad K - 1 \geq \frac{(1 - \vartheta)\gamma n}{2}.$$

These inequalities give the required ratio and, with [Equation \(44\)](#), the incidence budget for $M \leq Ln$. For large n , the stronger estimate $K - 1 \geq (1 - \vartheta)A/2$ gives $B \leq \lceil 2m/(1 - \vartheta) \rceil$. Finally B and m are fixed: taking $n > B$ and $n > m$ gives $B < q$ and $mA \leq mn < n^2 \leq q^2$. $\square$

4.2 Prime-field differential-equation root finding

We use the prime-field formulation in [\[BCPZZ26, Theorem 2.1\]](#), which restates Kopparty's differential-equation root solver [\[Kop15, Theorem 4.3\]](#).

Theorem 4.2 (Kopparty; prime-field form from BCPZZ). *Let q be prime and $q \geq K > r$. Suppose*

$$0 \neq Q \in \mathbb{F}_q[X, Y_0, \dots, Y_r]$$

satisfies $\deg_{Y_j} Q < q$ for all j and

$$\deg_{(1, K-1, K-2, \dots, K-r-1)} Q < q^2.$$

Then all $P \in \mathbb{F}_q[X]$ with $\deg P < K$ satisfying

$$Q(X, P, P^{[1]}, \dots, P^{[r]}) \equiv 0$$

can be found in $q^{O(r+1)}$ time. Their number is at most q^{4r+6} .

Remark 4.3 (The number of algebraic roots versus the final list). The root bound in [Theorem 4.2](#) includes every degree-bounded solution of the differential equation, whether or not it has the required agreement. In [Section 6](#) we bound the much smaller set that passes the agreement test. From Kopparty's bound $t(r+1)q^{2r\lfloor d/q \rfloor + 4r+4}$ with $d = K - 1 < q$, $t < q$, and $r+1 \leq q$, one obtains the displayed q^{4r+6} estimate [\[Kop15, Theorem 4.3\]](#).

4.3 Sparse list recovery and its running time

The interpolation theorem becomes an algorithm once it is combined with Kopparty's prime-field root-enumeration theorem. We state the sparse-incidence form, from which ordinary list decoding and bounded-list recovery follow immediately.

Theorem 4.4 (Prime-field sparse list recovery). *Fix $\vartheta \in (0, 1)$. There are effective constants $r_0, a_\vartheta > 0$ with the following property.*

Let q be prime, let $\alpha_1, \dots, \alpha_n \in \mathbb{F}_q$ be distinct, and let $S_i \subseteq \mathbb{F}_q$ have total incidence M . Let A, k, K be integers with $1 \leq A \leq n$, $1 \leq k \leq K$, and $K \geq 2$, and suppose

$$\frac{A}{K-1} \geq \frac{1}{1-\vartheta}, \quad (46)$$

$$r_0 \leq r < K, \quad M \leq a_\vartheta(K-1) \frac{r^\vartheta}{\log^4(er)}, \quad (47)$$

$$B := \left\lceil \frac{r^3 A}{K-1} \right\rceil < q, \quad r^3 A < q^2. \quad (48)$$

Then a deterministic algorithm outputs every $P \in \mathbb{F}_q[X]$ with $\deg P < k$ and at least A list hits. It uses

$$q^{O_\vartheta(r)} \quad (49)$$

field operations, and the output list has size at most q^{4r+6} .

Proof. Construct $\mathcal{Q}$ using the optimized shape Equation (37). Form the homogeneous local constraints for every incidence and use Gaussian elimination to find the nonzero interpolant promised by Proposition 3.8. By Lemma 3.1 and Equation (48), its individual Y_j -degrees are below q and its differential weighted degree is below q^2 . Since distinct evaluation points imply $n \leq q$ and Equation (46) implies $K \leq A \leq n$, we also have $q \geq K > r$. Apply Theorem 4.2, then filter by degree $k-1$ and agreement.

It remains to bound interpolation time. Since $s = O_\vartheta(1)$ and $m = r^3$,

$$|\mathcal{T}| \leq \binom{\lceil sm \rceil + r - 1}{r-1} = r^{O_\vartheta(r)}. \quad (50)$$

Condition $B < q$ and $B \geq r^3$ imply $q > r$. Thus Equation (50) is $q^{O_\vartheta(r)}$. There are at most q choices for each of b_0, b_1 , and fewer than q^2 choices for a , so $\mathcal{Q}$ has $q^{O_\vartheta(r)}$ monomials.

The coefficient records in one local map have

$$0 \leq i < m, \quad 0 \leq b < m/r, \quad e_1 < 2m, \quad \omega(\mathbf{v}) \leq W + m.$$

Indeed, before the U -rewrite, a term of T -degree ρ has Y_1 -degree at most m and U -degree at most $\rho < m$, so rewriting U can increase the Y_1 -degree only to $m + \rho < 2m$. Its initial tail weight is at most $W + \rho$, and each added Y_j with $j \geq 2$ increases both the T -degree and the ω -weight by $j-1$. Thus a final term of T -degree $i < m$ has tail weight at most $W + i < W + m$. Their number is $r^{O_\vartheta(r)} = q^{O_\vartheta(r)}$. There are at most $M \leq nq \leq q^2$ incidences. Each matrix entry can be computed by truncated polynomial arithmetic in $q^{O_\vartheta(r)}$ operations. Hence the whole matrix has $q^{O_\vartheta(r)}$ rows and columns and can be formed and row-reduced in the same asymptotic form. Root finding and final verification also fit Equation (49). $\square$

Remark 4.5 (Where the runtime improvement comes from). The two-cutoff derivative-tail space already appears in [BCPZZ26]. For the runtime bound we count its admissible tails directly as weak compositions under $|\mathbf{v}| = O(r^3)$, obtaining only $r^{O(r)}$ possibilities. This is a sharper enumeration of the existing interpolation space; no new linear-algebra primitive is required.

Corollary 4.6 (Algorithmic part of Theorem 1.1). *Under the hypotheses of Theorem 1.1, the desired list is computable in $q^{O_{\gamma,L}(1)}$ field operations. Before agreement filtering, the differential root solver produces at most q^{4r+6} candidates, where $r = r(\gamma, L)$ is from Lemma 4.1.*

Proof. Set $A = k + \lceil \gamma n \rceil$. The bound on k ensures $A \leq n$. Apply Lemma 4.1, use $M \leq Ln$, and invoke Theorem 4.4. Every desired polynomial has degree below K and is preserved by the final degree and agreement filters. $\square$

For fixed R, γ, L and $k \leq Rn$, requiring $\lceil (R + \gamma)n \rceil$ list hits instead only restricts the output further. The constants above depend on γ, L alone. A more quantitative derivative-order choice in terms of a multiplicative slack and a target agreement is given in Section B.

5 Symbolic interpolation and solution geometry

We now replace the finite-field enumeration of roots by a geometric description that is useful both for counting actual list candidates and for following their supports along curves. The symbolic construction is used for MCA; a parameter-free corollary of the same geometric theorem will control individual lists.

5.1 A primitive polynomial interpolant over $\mathbb{F}_q[Z]$

For the curve in Theorem 1.2, put $A = n - \lfloor \rho n \rfloor$ and use Lemma 4.1 with $L = 1$. Write $B_\gamma = B_{\gamma,1}$. Define symbolic received symbols

$$y_i(Z) := \sum_{j=0}^{\ell} f_{j,i} Z^j \in \mathbb{F}_q[Z]. \quad (51)$$

Apply Corollary 3.9 over $\mathbb{F}_q(Z)$. We need a version whose coefficients are polynomial in Z and that remains nonzero under every specialization.

Lemma 5.1 (Polynomial kernel vector). *Let $M(Z) \in F[Z]^{u \times v}$ have entries of degree at most E , and suppose $\text{rank}_{F(Z)} M < v$. Then $\ker_{F[Z]} M$ contains a nonzero vector $c(Z)$ whose coordinates have degree at most $E \min\{u, v - 1\}$. The coordinates may be chosen primitive, meaning that their greatest common divisor in $F[Z]$ is 1.*

Proof. Let $s = \text{rank}_{F(Z)} M$. If $s = 0$, take a standard basis vector. Otherwise choose a nonzero $s \times s$ minor and one additional column. The signed $s \times s$ cofactors of the resulting $s \times (s + 1)$ submatrix give a nonzero relation among the selected columns on the s selected rows. Those rows are linearly independent and hence form a basis of the row space over $F(Z)$, so the same relation annihilates every row of M . Thus the cofactor vector, extended by zero on the other columns, lies in $\ker_{F[Z]} M$. Every cofactor has degree at most sE . Divide all coordinates by their common polynomial factor. Because $F[Z]$ is a domain, the divided vector remains in the kernel. $\square$

Proposition 5.2 (Symbolic differential interpolant). *Under the hypotheses and notation of Theorem 1.2 and Lemma 4.1, there are constants $r = r(\gamma)$, $B = B(\gamma)$, and $c = c(\gamma, \ell)$, and a polynomial*

$$Q(Z, X, Y_0, \dots, Y_r) \in \mathbb{F}_q[Z, X, Y_0, \dots, Y_r]$$

with the following properties:

(a) *Q is primitive as a polynomial in Z , i.e., the gcd in $\mathbb{F}_q[Z]$ of its coefficients in $X, Y_0, \dots, Y_r$ is 1;*

(b)

$$\deg_Z Q \leq cn, \quad \deg_X Q \leq cn, \quad \deg_Y^{\text{tot}} Q \leq B;$$

(c) *for every $z \in \overline{\mathbb{F}_q}$, the specialization $Q_z := Q(z, X, Y_0, \dots, Y_r)$ is nonzero;*

(d) *for every $z \in \mathbb{F}_q$ and every $P \in \mathbb{F}_q[X]$ of degree below k that agrees with $(y_i(z))_{i=1}^n$ on at least A coordinates,*

$$Q(z, X, P, P^{[1]}, \dots, P^{[r]}) \equiv 0. \quad (52)$$

Proof. Use the interpolation matrix in Corollary 3.9, replacing each received symbol by Equation (51). Since the matrix entries have degree at most B in y_i , they have Z -degree at most ℓB . The matrix has $O_\gamma(n)$ rows and columns. By Lemma 5.1, it has a nonzero polynomial kernel vector of Z -degree $O_{\gamma, \ell}(n)$. Interpret that vector as the coefficient vector of Q in the hidden-derivative monomial basis, and divide its content in $\mathbb{F}_q[Z]$. The divided vector remains in the kernel, so the matrix formulation in Corollary 3.9 guarantees all local interpolation constraints for this particular primitive choice.

The X - and Y -degree bounds follow from Equation (40) and $A \leq n$. Primitivity implies that no $z \in \overline{\mathbb{F}_q}$ can annihilate every coefficient of Q : otherwise the minimal polynomial of z over $\mathbb{F}_q$ would divide their gcd. This proves (c).

All interpolation constraints are polynomial identities in Z . They therefore remain valid after specializing $Z = z$. The coupled monomial bound in Equation (40) and the multiplicity argument in Lemma 3.2 then gives Equation (52) for every nearby P . $\square$

5.2 Cumulative degree

All algebraic varieties in the proof are considered over an algebraic closure. The degree of an affine irreducible variety means the degree of its projective closure. If V is an affine algebraic set with irreducible components $V_1, \dots, V_t$, define its cumulative degree by

$$\text{cdeg}(V) := \sum_{j=1}^t \deg(V_j).$$

We use two standard consequences of affine/projective Bézout; see, for example, [Hei83, Har92].

Lemma 5.3 (Effective intersections). *Let $V \subseteq \mathbb{A}^N$ have dimension at most s and cumulative degree Δ . If $W \subseteq V$ is cut out inside V by an arbitrary collection of polynomials of degree at most $E \geq 1$, then*

$$\text{cdeg}(W) \leq \Delta E^s.$$

If $U = W \cap \{H \neq 0\}$ is a principal-open subset of W , then $\overline{U}$ is a union of irreducible components of W , so the same bound holds for $\text{cdeg}(\overline{U})$.

Proof. By Noetherianity, finitely many of the equations cut out W set-theoretically inside V . Decompose V into irreducible components and organize the successive intersections as a component tree, retaining an equation on a branch only when it does not vanish identically on the current component. Every retained intersection strictly decreases dimension, so a branch has length at most s ; at each retained step, affine/projective Bézout multiplies the sum of the degrees of the children by at most E . Components on which later equations vanish identically are carried forward without a degree increase. Padding shorter branches by the factor $E \geq 1$ gives total leaf degree at most ΔE^s , and every irreducible component of W is one of these leaves. $\square$

Lemma 5.4 (Graph of a bounded-degree rational map). *Let $U \subseteq \mathbb{A}^m$ be constructible, with $\dim \bar{U} \leq s$ and $\text{cdeg}(\bar{U}) \leq \Delta$. Suppose a rational map $\phi : U \rightarrow \mathbb{A}^N$ has all coordinates of the form*

$$\phi_j = \frac{N_j}{H e_j},$$

where H is nonzero on U , e_j, L are nonnegative integers with $e_j \leq L$, and

$$\deg H, \deg N_j, L \deg H \leq E.$$

Then the Zariski closure of the graph of ϕ has dimension at most s and cumulative degree at most

$$\Delta(2E + 2)^s.$$

In particular, when s is fixed and E, N are polynomially bounded in a parameter D , the graph has degree $D^{O_s(1)}$.

Proof. Put $G = H^L$. On the open set $H \neq 0$, the graph is the image of the graph map

$$\Psi(u) := [G(u) : u_1 G(u) : \cdots : u_m G(u) : N_1(u) H(u)^{L-e_1} : \cdots : N_N(u) H(u)^{L-e_N}].$$

After passing to the projective closure of each irreducible component of $\bar{U}$ and homogenizing the displayed coordinates to a common degree, Ψ is a rational projective map defined by forms of degree at most $2E + 2$. The source coordinates occur in the image, so Ψ is generically one-to-one on every component meeting U . The standard degree bound for a rational image [Har92] therefore gives, for a component X of dimension $t \leq s$,

$$\deg \overline{\Psi(X \cap U)} \leq \deg(X)(2E + 2)^t.$$

Indeed, intersecting the image with a generic codimension- t linear space and pulling back gives t members of this degree- $(2E + 2)$ linear system on X ; after discarding components supported in the base locus, projective Bézout bounds the resulting moving zero-cycle by the right-hand side. Summing over the irreducible components of $\bar{U}$ yields the stronger bound

$$\text{cdeg}(\overline{\Gamma_\phi}) \leq \Delta(2E + 2)^s,$$

as asserted. The same generically injective parametrization gives $\dim \overline{\Gamma_\phi} \leq s$. $\square$

5.3 Effective jet decomposition of the solution locus

This section proves the algebraic statement that converts one symbolic differential equation into a bounded-complexity family of polynomial solutions. The nonsingular Taylor lifting and the singular reduction by a highest-variable partial derivative follow Kopparty [Kop15, Section 4.2, Theorem 4.4

and the proof of Theorem 4.3]. Here we add polynomial numerator and denominator degree bounds, parameter-specialization control, and a bounded-cumulative-degree geometric cover.

Let F be algebraically closed of characteristic p , let $d < p$, and write

$$P_{\mathbf{p}}(X) = \sum_{j=0}^d p_j X^j$$

for the polynomial corresponding to $\mathbf{p} = (p_0, \dots, p_d) \in F^{d+1}$. For

$$Q \in F[Z, X, Y_0, \dots, Y_r],$$

define

$$\text{Sol}_d(Q) := \left\{ (z, \mathbf{p}) \in \mathbb{A}^{d+2} : Q(z, X, P_{\mathbf{p}}, P_{\mathbf{p}}^{[1]}, \dots, P_{\mathbf{p}}^{[r]}) \equiv 0 \right\}. \quad (53)$$

A polynomial in $F[Z, X, Y_0, \dots, Y_r]$ is Z -*primitive* if the gcd of its coefficients as a polynomial in $X, Y_0, \dots, Y_r$ is 1 in $F[Z]$.

Theorem 5.5 (Parametric jet decomposition). *Fix integers $r, B \geq 0$. There is an effective constant $C_0 = C_0(r, B)$ with the following property. Let F be algebraically closed of characteristic p , let $0 \leq d < p$, and let*

$$0 \neq Q \in F[Z, X, Y_0, \dots, Y_r]$$

be Z -primitive and satisfy

$$\deg_Z Q, \deg_X Q \leq D, \quad \deg_Y^{\text{tot}} Q \leq B < p, \quad D \geq 2. \quad (54)$$

Then there are a finite set $E_Q \subseteq F$ and affine algebraic sets

$$V_1, \dots, V_t \subseteq \mathbb{A}^{d+2}$$

such that

$$|E_Q| + \sum_{j=1}^t \text{cdeg}(V_j) \leq (D + d + 2)^{C_0}, \quad (55)$$

$$\dim V_j \leq r + 1 \quad \text{for every } j, \quad (56)$$

and every $(z, \mathbf{p}) \in \text{Sol}_d(Q)$ with $z \notin E_Q$ belongs to $\bigcup_j V_j$.

The exceptional set is needed because, after differentiating Q with respect to its highest derivative variable, all coefficients of that derivative may vanish at finitely many parameter values. In our proximity application we select at most one polynomial above each z , so those fibers contribute only $|E_Q|$ selected points.

5.3.1 Triangular Hasse–Taylor lifting

We first give the quantitative local lifting statement. Suppose Q depends on Y_s but on no Y_j with $j > s$. Fix $\alpha \in F$ and write

$$P(\alpha + U) = \sum_{j=0}^d c_j U^j.$$

Set

$$H_{\alpha}(Z, c_0, \dots, c_s) := \frac{\partial Q}{\partial Y_s}(Z, \alpha, c_0, \dots, c_s). \quad (57)$$

For $t \geq 0$, let $F_{\alpha,t}$ be the coefficient of U^t in

$$Q\left(Z, \alpha + U, P(\alpha + U), P^{[1]}(\alpha + U), \dots, P^{[s]}(\alpha + U)\right). \quad (58)$$

Lemma 5.6 (Triangular coefficient equation). *For $1 \leq t \leq d - s$,*

$$F_{\alpha,t} = \binom{s+t}{s} H_{\alpha}(Z, c_0, \dots, c_s) c_{s+t} + G_{\alpha,t}(Z, c_0, \dots, c_{s+t-1}) \quad (59)$$

for a polynomial $G_{\alpha,t}$. In particular, because $d < p$, the coefficient $\binom{s+t}{s}$ is nonzero in F .

Proof. Perturb c_{s+t} while fixing all earlier Taylor coefficients. By Equation (5), the induced perturbation of $P^{[s]}$ begins with

$$\binom{s+t}{s} c_{s+t} U^t,$$

whereas the perturbation of $P^{[i]}$ for $i < s$ begins in degree $s + t - i > t$. In the coefficient of U^t in Equation (58), only the term linear in the perturbation of Y_s can occur; two such perturbations have order at least $2t > t$. Its coefficient is the constant term of $\partial Q / \partial Y_s$ after substitution, namely H_{α} . This proves Equation (59). Since $s + t \leq d < p$, the displayed binomial coefficient is nonzero. $\square$

Lemma 5.7 (Polynomial degree of the lifted jet). *Assume Equation (54), and suppose the total Y -degree is at most B . On the open set $H_{\alpha} \neq 0$, the equations*

$$F_{\alpha,t} = 0, \quad 1 \leq t \leq d - s,$$

recursively determine

$$c_{s+t} = \frac{N_t(Z, c_0, \dots, c_s)}{H_{\alpha}(Z, c_0, \dots, c_s)^{e_t}}. \quad (60)$$

There is a constant C_B depending only on B such that

$$e_t \leq 2t - 1, \quad \deg N_t \leq C_B(D + B)t^2. \quad (61)$$

After these substitutions, every remaining coefficient equation $F_{\alpha,t} = 0$ has a numerator of degree at most

$$E_0 := C_B(D + B)(d + 2)^2. \quad (62)$$

Proof. The recursive existence follows from Lemma 5.6. We prove the denominator bound and the stronger numerator estimate $\deg N_t \leq 4(D + B)t^2$ by induction on t . Consider a monomial contributing to the coefficient of U^t in Equation (58). It contains at most B Taylor coefficients. If c_j with $j > s$ occurs through $P^{[i]}$, its U -order is $j - i \geq j - s$. Hence, if the occurrences above the initial jet are $c_{s+h_1}, \dots, c_{s+h_v}$, then

$$h_1 + \dots + h_v \leq t, \quad v \leq B. \quad (63)$$

In the remainder $G_{\alpha,t}$ from Equation (59), either $h_1 + \dots + h_v \leq t - 1$, or equality holds and $v \geq 2$: the only term with $v = 1$ and $h_1 = t$ is the linear term in c_{s+t} already separated in Equation (59). Using the inductive bound $e_h \leq 2h - 1$, every monomial of $G_{\alpha,t}$ therefore has denominator exponent at most

$$\sum_{j=1}^v (2h_j - 1) \leq 2t - 2.$$

After putting $G_{\alpha,t}$ over the common denominator H_{α}^{2t-2} , solving Equation (59) for c_{s+t} gives $e_t \leq 2t - 1$.

For the numerator degree, the same separation gives

$$\sum_{j=1}^v h_j^2 \leq t^2 - 2t + 2$$

whenever $t \geq 2$: under a fixed sum, the sum of squares is maximized by concentrating all but one unit in a single part, and the one-part case of total weight t is absent from $G_{\alpha,t}$. By induction, the numerator of a substituted monomial therefore has degree at most

$$D + B + 4(D + B)(t^2 - 2t + 2).$$

Passing to the common denominator H_{α}^{2t-2} adds at most $(2t-2)(D+B)$, since $\deg H_{\alpha} \leq D+B$. For $t \geq 2$, the inequality $1 + 4(t^2 - 2t + 2) + (2t-2) \leq 4t^2$ closes the induction and gives

$$\deg N_t \leq 4(D+B)t^2.$$

The case $t = 1$ follows directly from Equation (59). This proves Equation (61).

The same order-budget argument applies to every residual coefficient of Equation (58). There are no Taylor coefficients beyond c_d , at most B noninitial coefficients occur in one monomial, and their total excess above s is at most Bd . Thus a common denominator uses only $O_B(d)$ powers of H_{α} , while

$$\sum_j h_j^2 \leq \left(\sum_j h_j \right)^2 \leq B^2 d^2.$$

The product of the substituted numerators and the denominator clearing therefore have degree $O_B((D+B)(d+2)^2)$, which is Equation (62) after increasing C_B . $\square$

5.3.2 Proof of the jet-decomposition theorem

Proof of Theorem 5.5. We induct on the total Y -degree of Q . If $d < r$, the ambient space $\mathbb{A}^{d+2}$ itself has dimension $d+2 \leq r+1$, so the theorem is immediate with one degree-one set and no exceptions. We may therefore assume $d \geq r$.

If Q is independent of every Y_j , then $Q(z, X) \equiv 0$ has no solution for any z : Z -primitivity rules out a specialization at which all X -coefficients vanish. This is the base case.

Otherwise, let $s \leq r$ be maximal such that Q depends on Y_s , and put

$$H := \frac{\partial Q}{\partial Y_s}.$$

Because $\deg_{Y_s} Q \leq B < p$ whenever the theorem is used below, H is nonzero. (More generally, the assumption needed here is $\deg_{Y_s} Q < p$.) Write

$$H = c(Z)\tilde{H}$$

where $c(Z) \in F[Z]$ is the content and $\tilde{H}$ is Z -primitive. Add the roots of c to the exceptional set. There are at most D of them.

Every nonexceptional solution (z, P) is of one of two types.

Singular type. If

$$H(z, X, P, P^{[1]}, \dots, P^{[s]}) \equiv 0,$$

then $(z, P) \in \text{Sol}_d(\tilde{H})$. The total Y -degree has decreased by one, while all Z - and X -degrees remain at most D . The inductive hypothesis supplies the required cover for all singular solutions outside another set of at most $(D + d + 2)^{C_0(r, B-1)}$ parameter values.

Nonsingular type. Suppose instead that the substituted polynomial $H(z, X, P, \dots, P^{[s]})$ is nonzero. Its X -degree is at most

$$D + (B - 1)d. \quad (64)$$

Choose a fixed set

$$\Omega \subseteq F, \quad |\Omega| = D + (B - 1)d + 1.$$

Then some $\alpha \in \Omega$ satisfies

$$H_\alpha(z, P(\alpha), P^{[1]}(\alpha), \dots, P^{[s]}(\alpha)) \neq 0.$$

Fix this α . In Taylor coordinates $c_j = P^{[j]}(\alpha)$, [Lemmas 5.6](#) and [5.7](#) express every $c_{s+1}, \dots, c_d$ as a rational function of the base variables

$$u = (z, c_0, \dots, c_s)$$

with numerator degree at most $E_0 = O_B((D + B)(d + 2)^2)$ and a common denominator H_α^L satisfying $\deg H_\alpha, L \deg H_\alpha \leq E_0$.

The base variables must satisfy

$$Q(z, \alpha, c_0, \dots, c_s) = 0, \quad (65)$$

and the numerators of all residual coefficient equations. Let U_α be the corresponding constructible set with $H_\alpha \neq 0$. If U_α is nonempty, then H_α is not the zero polynomial. Consequently the polynomial

$$Q_\alpha(Z, c_0, \dots, c_s) := Q(Z, \alpha, c_0, \dots, c_s)$$

is nonzero, since $\partial Q_\alpha / \partial c_s = H_\alpha$. As $\overline{U_\alpha} \subseteq Z(Q_\alpha) \subseteq \mathbb{A}^{s+2}$, we have

$$\dim \overline{U_\alpha} \leq s + 1 \leq r + 1. \quad (66)$$

Let W_α be the closed set defined by the base equation and the cleared residual equations. Then $U_\alpha = W_\alpha \cap \{H_\alpha \neq 0\}$, so $\overline{U_\alpha}$ is the union of the irreducible components of W_α not contained in $Z(H_\alpha)$. By [Lemma 5.3](#) and [Equation \(62\)](#),

$$\text{cdeg}(\overline{U_\alpha}) \leq (D + d + 2)^{O_{r, B}(1)}. \quad (67)$$

The rational Taylor-coefficient map from U_α to $(z, c_0, \dots, c_d)$ satisfies the hypotheses of [Lemma 5.4](#). Its graph closure therefore has dimension at most $s + 1$ and cumulative degree $(D + d + 2)^{O_{r, B}(1)}$. The graph is identified with its $(z, c_0, \dots, c_d)$ coordinates, since these already contain the base variables. The change from Taylor coefficients at α to monomial coefficients is invertible and linear, so it preserves dimension and degree. We obtain one admissible algebraic set for each $\alpha \in \Omega$.

There are only $O_B(D + d)$ choices of α , and the singular induction has depth at most B . Increasing one effective exponent $C_0(r, B)$ absorbs all exceptional parameter values, all graph degrees, and all recursive contributions, proving [Equations \(55\)](#) and [\(56\)](#). $\square$

Remark 5.8 (Why the large-characteristic hypothesis is essential). If $d \geq p$, even the equation $Y_1 = 0$ has every polynomial in X^p as a solution, so the solution locus has dimension growing with d/p . The condition $d < p$ eliminates exactly this Frobenius freedom. In the prime-field Reed–Solomon application, $d = k - 1 < n \leq q = p$.

6 List bounds independent of the field size

The root solver bounds the number of all polynomial solutions of $Q = 0$ by a power of q . Agreement supplies additional linear equations, allowing a bound in terms of n instead. This section records the consequence of combining interpolation with the geometric decomposition.

Corollary 6.1 (A parameter-free solution cover). *Fix $r, B \geq 0$. There is an effective $C_0 = C_0(r, B)$ such that the following holds. Let F be algebraically closed of characteristic p , let $d < p$, let $B < p$, and let $D \geq 2$. For a nonzero*

$$Q(X, Y_0, \dots, Y_r) \in F[X, Y_0, \dots, Y_r], \quad \deg_X Q \leq D, \quad \deg_Y^{\text{tot}} Q \leq B,$$

the coefficient vectors of all degree-at-most- d solutions of

$$Q(X, P, P^{[1]}, \dots, P^{[r]}) \equiv 0$$

are contained in a union of affine algebraic sets $W_1, \dots, W_t \subseteq \mathbb{A}^{d+1}$ with

$$\dim W_j \leq r, \quad \sum_j \text{cdeg}(W_j) \leq (D + d + 2)^{C_0}.$$

Proof. Introduce an indeterminate Z and regard Q as independent of Z . It is Z -primitive. Apply [Theorem 5.5](#), and decompose its covering sets into irreducible components. Choose $z_0 \in F$ outside the exceptional set and outside the finitely many constant Z -values of vertical components. Such a choice exists because F is infinite.

Intersect every nonvertical component with $Z = z_0$. This is a proper hyperplane intersection, so its dimension is at most r and its cumulative degree is at most the degree of the component. Vertical components have empty intersection with this slice. Identifying the slice with $\mathbb{A}^{d+1}$ yields the stated degree and dimension bounds. Every solution P belongs to this cover because (z_0, P) solves the parameter-independent equation and z_0 is nonexceptional. This is an existence argument for a cover; the choice of z_0 is not an additional step of the decoding algorithm. $\square$

Lemma 6.2 (Counting points isolated by their support equations). *Let F be algebraically closed, and let $V_1, \dots, V_t \subseteq \mathbb{A}^N$ have dimension at most s and total cumulative degree at most Δ . Let $h_1, \dots, h_M$ have degree at most $E \geq 1$, with $M \geq 1$. Suppose $T \subseteq \bigcup_j V_j$ is finite and every $x \in T$ is assigned a set $S_x \subseteq [M]$ such that*

$$\bigcap_{i \in S_x} Z(h_i) = \{x\}.$$

Then

$$|T| \leq \Delta \sum_{a=0}^s (ME)^a.$$

Proof. Assign each point to an irreducible component of the cover that contains it. At a positive-dimensional component W through x , not every assigned equation can vanish identically: otherwise W would be contained in their singleton intersection. Choose an assigned equation that does not vanish identically and pass to an irreducible component of its intersection with W containing x . Dimension drops at every step, so a zero-dimensional component is reached after at most s cuts.

For a fixed ordered tuple of a equation indices, Bézout bounds the total degree of the resulting proper-intersection components by ΔE^a . A zero-dimensional component contributes at most its degree many points. Summing over the at most M^a tuples of length a , and then over $0 \leq a \leq s$, gives the bound. Repetitions or overlaps can only overcount points. $\square$

Theorem 6.3 (A sparse list bound from a differential interpolant). *Fix $r, B \geq 0$, and let $\mathbb{F}_q$ be a finite field of characteristic $p > \max\{k-1, B\}$. Let $D = \{\alpha_1, \dots, \alpha_n\} \subseteq \mathbb{F}_q$ have n distinct points, let $S_i \subseteq \mathbb{F}_q$ have total incidence M , and let $A \geq k \geq 1$. Suppose every $P \in \mathcal{L}(D, k, \mathbf{S}, A)$ satisfies*

$$Q(X, P, P^{[1]}, \dots, P^{[r]}) \equiv 0$$

for a nonzero polynomial Q with $\deg_X Q \leq D_0$, $\deg_Y^{\text{tot}} Q \leq B$, and $D_0 \geq 2$. Then

$$|\mathcal{L}(D, k, \mathbf{S}, A)| \leq (D_0 + k + 1)^{C_0(r, B)} \sum_{a=0}^r M^a. \quad (68)$$

If $M = 0$, the list is empty.

Proof. Apply [Corollary 6.1](#) over $\overline{\mathbb{F}_q}$ with $d = k - 1$. The candidate coefficient vectors lie in a cover of dimension at most r and cumulative degree at most $(D_0 + k + 1)^{C_0(r, B)}$.

For every incidence (i, b) with $b \in S_i$, define the hyperplane

$$h_{i,b}(\mathbf{p}) = \sum_{a=0}^{k-1} p_a \alpha_i^a - b.$$

To a candidate P assign all pairs $(i, P(\alpha_i))$ at its list-hit coordinates. There are at least $A \geq k$ distinct such coordinates. Any k of their evaluation equations form an invertible Vandermonde system, so their common zero set, and hence that of all assigned equations, is exactly the coefficient vector of P . Apply [Lemma 6.2](#) with $E = 1$ and $s = r$. This proves [Equation \(68\)](#). $\square$

Proof of Theorem 1.1. The algorithmic assertion is [Corollary 4.6](#). For the list bound, take $A = k + \lceil \gamma n \rceil$ and choose the parameters of [Lemma 4.1](#). By [Corollary 3.9](#), there is a nonzero differential interpolant containing every candidate, with

$$\deg_X Q < mA = O_{\gamma, L}(n), \quad \deg_Y^{\text{tot}} Q \leq B_{\gamma, L}.$$

For sufficiently large n , the characteristic $p = q \geq n$ exceeds both $k - 1$ and $B_{\gamma, L}$. Use [Theorem 6.3](#) with $D_0 = \max\{2, mA\}$ and $M \leq Ln$. Since $r, B_{\gamma, L}, L$ are fixed, its right-hand side is $n^{O_{\gamma, L}(1)}$. Increasing an effective exponent and the length threshold absorbs the fixed multiplicative constants.

For singleton lists, relative distance at most $1 - k/n - \gamma$ is equivalent to at least

$$n - \lfloor (1 - k/n - \gamma)n \rfloor = k + \lceil \gamma n \rceil$$

agreements. This proves the decoding-radius formulation as well. $\square$

Remark 6.4 (What the list bound does not give). The estimate is uniform in the field size; it is not a constant list-size bound. Nor does it by itself turn Kopparty's root enumeration into a $\text{poly}(n, \log q)$ algorithm. The geometric cover is used for counting, whereas the stated decoder may enumerate $q^{O(r)}$ differential-equation roots before filtering.

7 Support-preserving descent and mutual correlated agreement

7.1 Descent along the full agreement support

The point-isolation argument has a parametric counterpart. We follow the complete support assigned to each witness and stop either on a vertical component or on a branch that explains that support identically. This is the step needed for MCA rather than ordinary correlated agreement.

Lemma 7.1 (Support-preserving descent). *Let F be algebraically closed, let $\pi : \mathbb{A}^N \rightarrow \mathbb{A}^1$ be one coordinate function, and let $V_1, \dots, V_t \subseteq \mathbb{A}^N$ be affine algebraic sets satisfying*

$$\dim V_j \leq s, \quad \sum_{j=1}^t \text{cdeg}(V_j) \leq \Delta.$$

Let $h_1, \dots, h_n \in F[x_1, \dots, x_N]$ have degree at most $L \geq 1$. Let $T \subseteq \bigcup_j V_j$ be finite, and assign to each $x \in T$ a set $S_x \subseteq [n]$ such that $h_i(x) = 0$ for every $i \in S_x$.

Call x branch-explained if there is a positive-dimensional irreducible subvariety $W \subseteq V_j$ through x for some j such that $\pi|_W$ is nonconstant and

$$h_i|_W \equiv 0 \quad \text{for every } i \in S_x.$$

Then

$$|\{\pi(x) : x \in T \text{ is not branch-explained}\}| \leq \Delta \sum_{a=0}^s (nL)^a. \quad (69)$$

Proof. Decompose all V_j into irreducible components and assign each point of T to one component containing it. Starting from the assigned component W_0 , process a point x as follows.

If W_a is zero-dimensional, stop. If π is constant on W_a , stop. If every h_i with $i \in S_x$ vanishes identically on W_a , then x is branch-explained and the process stops. Otherwise choose an index $i_{a+1} \in S_x$ for which $h_{i_{a+1}}$ is not identically zero on W_a , and let W_{a+1} be an irreducible component of

$$W_a \cap Z(h_{i_{a+1}})$$

containing x . Because $h_{i_{a+1}}(x) = 0$ but does not vanish identically on the irreducible variety W_a , every such component has strictly smaller dimension. Thus an un-explained point reaches a zero-dimensional or π -vertical terminal component after at most s cuts.

Fix an ordered index tuple $(i_1, \dots, i_a) \in [n]^a$. Organize the successive intersections with $Z(h_{i_1}), \dots, Z(h_{i_a})$ as a tree of irreducible components, retaining only proper intersections along each branch. Bézout's theorem bounds the sum of the degrees at depth a by ΔL^a . Each zero-dimensional terminal component contributes at most its degree many values of π . Each positive-dimensional vertical irreducible component contributes exactly one value of π , and the number of such components is at most the same cumulative-degree bound. Hence all terminal components reached by this fixed tuple contribute at most ΔL^a parameter values. There are n^a ordered tuples of length a . Summing over $0 \leq a \leq s$ proves Equation (69). $\square$

For $\mathbf{p} = (p_0, \dots, p_{k-1})$, write

$$P_{\mathbf{p}}(X) = \sum_{a=0}^{k-1} p_a X^a.$$

For the coefficient words in Theorem 1.2, define

$$h_i(z, \mathbf{p}) := P_{\mathbf{p}}(\alpha_i) - \sum_{j=0}^{\ell} z^j f_{j,i}. \quad (70)$$

These hypersurfaces have total degree at most ℓ .

Lemma 7.2 (A support-identical branch explains the full support). *Let $W \subseteq \mathbb{A}^{k+1}$, with coordinates $(z, \mathbf{p})$, be a positive-dimensional irreducible variety over $\overline{\mathbb{F}_q}$. Assume that $z|_W$ is nonconstant. Let $S \subseteq [n]$ have $|S| \geq k$, and suppose*

$$h_i|_W \equiv 0 \quad \text{for every } i \in S.$$

Then there are $P_0, \dots, P_\ell \in \mathbb{F}_q[X]$, each of degree below k , such that

$$P_j(\alpha_i) = f_{j,i} \quad (i \in S, 0 \leq j \leq \ell).$$

Moreover, at every point $(z_0, \mathbf{p}_0) \in W$, one has

$$P_{\mathbf{p}_0} = \sum_{j=0}^{\ell} z_0^j P_j.$$

Proof. Choose k indices $i_1, \dots, i_k \in S$. In the function field $\overline{\mathbb{F}_q}(W)$, their equations give

$$\begin{pmatrix} 1 & \alpha_{i_1} & \cdots & \alpha_{i_1}^{k-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_{i_k} & \cdots & \alpha_{i_k}^{k-1} \end{pmatrix} \mathbf{p} = \begin{pmatrix} \sum_{j=0}^{\ell} z^j f_{j,i_1} \\ \vdots \\ \sum_{j=0}^{\ell} z^j f_{j,i_k} \end{pmatrix}.$$

The Vandermonde matrix is invertible over $\mathbb{F}_q$, so

$$\mathbf{p} = \mathbf{p}^{(0)} + z\mathbf{p}^{(1)} + \cdots + z^\ell \mathbf{p}^{(\ell)} \quad (71)$$

for vectors $\mathbf{p}^{(j)} \in \mathbb{F}_q^k$. Let P_j be the polynomial with coefficient vector $\mathbf{p}^{(j)}$.

Because the base field $\overline{\mathbb{F}_q}$ is algebraically closed and z is nonconstant on the irreducible variety W , the element $z \in \overline{\mathbb{F}_q}(W)$ is transcendental over $\overline{\mathbb{F}_q}$. For any $i \in S$, substituting Equation (71) into the identity $h_i = 0$ yields

$$\sum_{j=0}^{\ell} z^j (P_j(\alpha_i) - f_{j,i}) = 0.$$

Transcendence forces every coefficient to vanish, proving the first claim. The identity in Equation (71) holds in the regular coordinate functions on W , so it also gives the asserted polynomial identity at every point of W . $\square$

7.2 Proof of the MCA theorem

Proof of Theorem 1.2. Set

$$e = \lfloor \rho n \rfloor, \quad A = n - e.$$

The radius hypothesis gives

$$A \geq k + \lceil \gamma n \rceil \geq k. \quad (72)$$

For each bad parameter $z \in \text{Bad}_{C,\rho}^{(\ell)}(\mathbf{f})$, choose one witnessing polynomial P_z of degree below k , and put

$$S_z := \text{Agr}(y(z), P_z).$$

Thus $|S_z| \geq A$, and S_z is not a maximal $\mathbf{f}$ -correlated set. Let $x_z = (z, \mathbf{p}_z) \in \mathbb{A}^{k+1}$ be the coefficient point of P_z . We select only one point above each bad parameter.

Construct the primitive symbolic differential interpolant Q from [Proposition 5.2](#). Every x_z belongs to $\text{Sol}_{k-1}(Q)$. Write $B_\gamma = B_{\gamma,1}$ from [Lemma 4.1](#), and enlarge n_0 so that $n > B_\gamma$ and $n \geq 2$, and apply [Theorem 5.5](#) over $\overline{\mathbb{F}}_q$ with $d = k - 1$ and

$$D_0 := \max\{2, \deg_Z Q, \deg_X Q\} = O_{\gamma,\ell}(n).$$

Indeed, $d = k - 1 < q$, while $B \leq B_\gamma < n \leq q$. Moreover, Z -primitivity is preserved after extending scalars to $\overline{\mathbb{F}}_q$: a common linear factor over the algebraic closure would force its minimal polynomial over $\mathbb{F}_q$ to divide every coefficient of Q . Thus all hypotheses of [Theorem 5.5](#) hold. We obtain an exceptional set E_Q and varieties $V_1, \dots, V_t \subseteq \mathbb{A}^{k+1}$ satisfying

$$|E_Q| + \sum_{j=1}^t \text{cdeg}(V_j) \leq n^{C_1}, \quad \dim V_j \leq s := r + 1, \quad (73)$$

for an effective $C_1 = C_1(\gamma, \ell)$, and every x_z with $z \notin E_Q$ lies in $\bigcup_j V_j$.

Apply [Lemma 7.1](#) to the selected points with $z \notin E_Q$, using the support assignment $x_z \mapsto S_z$ and the hypersurfaces in [Equation \(70\)](#). Suppose that one selected point x_z were branch-explained. Then there would be a positive-dimensional nonvertical irreducible W through x_z on which every h_i , $i \in S_z$, vanishes identically. By [Equation \(72\)](#) and [Lemma 7.2](#), the entire exact support S_z would be $\mathbf{f}$ -correlated. By [Lemma 2.4](#), it would then be maximal, contradicting the choice of P_z as an MCA witness. Consequently every selected bad point outside E_Q is not branch-explained.

Since the h_i have degree at most ℓ , [Lemma 7.1](#) and [Equation \(73\)](#) give

$$|\text{Bad}_{\mathcal{C},\rho}^{(\ell)}(\mathbf{f}) \setminus E_Q| \leq n^{C_1} \sum_{a=0}^{r+1} (\ell n)^a.$$

There are at most $|E_Q| \leq n^{C_1}$ additional bad parameters in the exceptional set. Because r and ℓ are fixed, increasing an effective exponent gives

$$|\text{Bad}_{\mathcal{C},\rho}^{(\ell)}(\mathbf{f})| \leq n^{C(\gamma,\ell)}.$$

The bound is uniform in the coefficient words. Taking $\ell = 1$, maximizing over f_0, f_1 , and dividing by q proves the MCA error estimate. $\square$

Corollary 7.3 (Ordinary correlated proximity gaps). *Under the hypotheses of [Theorem 1.2](#), if more than $n^{C(\gamma,\ell)}$ values $z \in \mathbb{F}_q$ satisfy*

$$\Delta\left(\sum_{j=0}^{\ell} z^j f_j, \mathcal{C}\right) \leq \rho,$$

then there are degree-below- k polynomials $P_0, \dots, P_\ell$ agreeing jointly with $f_0, \dots, f_\ell$ on at least A_ρ coordinates. Consequently, $\Delta(y(z), \mathcal{C}) \leq \rho$ for every $z \in \mathbb{F}_q$.

Proof. Choose a nearby polynomial at every good parameter. Since there are more good parameters than bad ones, at least one good parameter is not MCA-bad. The exact support of its nearby polynomial belongs to $\mathcal{A}_\rho(\mathbf{f})$ and therefore is jointly explained by $P_0, \dots, P_\ell$ on at least A_ρ coordinates. For every parameter z , the polynomial $\sum_j z^j P_j$ agrees with $y(z)$ on that same support, proving the last assertion. $\square$

8 Consequences and quantitative scope

8.1 Coordinate transformations, punctures, and erasures

Corollary 8.1 (Coordinate-affine generalized RS codes). *Let $v_i \in \mathbb{F}_q^\times$ and $b_i \in \mathbb{F}_q$. All preceding algorithms apply to codewords*

$$(v_i P(\alpha_i) + b_i)_{i=1}^n.$$

For list recovery, replace S_i by

$$S'_i := \{(z - b_i)/v_i : z \in S_i\}.$$

This preserves both incidence size and agreement.

Puncturing is already allowed because the evaluation set is arbitrary. Erased coordinates may simply be omitted; the theorem is then applied to the remaining evaluation set, with its new length n' , and with the desired absolute number of nonerased agreements.

When $b_i = 0$, the same transformation preserves the exact agreement supports relevant to MCA: dividing each curve coefficient $f_{j,i}$ by v_i carries joint explanations and maximality bijectively to those for ordinary Reed–Solomon codes. Arbitrary translations are allowed above only for list decoding and list recovery.

8.2 Fixed interleaving

For an integer $h \geq 1$, let $\mathcal{C}^{\equiv h}$ consist of h rows from $\mathcal{C}$, viewed as a length- n code over $\mathbb{F}_q^h$. Distance counts columns on which the entire h -tuple differs. Write $\Lambda_h(\mathcal{C}, \rho)$ for the maximum number of such codewords in a radius- ρ ball.

Corollary 8.2 (Polynomial lists for fixed interleaving). *Under the singleton-list hypotheses of Theorem 1.1, for every integer $h \geq 1$,*

$$\Lambda_h(\mathcal{C}, 1 - k/n - \gamma) \leq n^{hC_{\text{list}}(\gamma, 1)}.$$

For fixed γ, h , the interleaved list can be enumerated deterministically in $q^{O_{\gamma, h}(1)}$ field operations.

Proof. Fix a received $h \times n$ array. Every valid interleaved codeword has the requisite agreement in every row separately. Its row polynomials therefore belong to the h scalar lists from Theorem 1.1, each of size at most $n^{C_{\text{list}}(\gamma, 1)}$. The product of these lists contains every valid interleaved codeword. Enumerate that product and test common-column agreement. The product bound proves the size estimate, and $q \geq n$ gives the stated running time for fixed h . $\square$

8.3 Fixed-slack certificates for the proximity challenges

The preliminary Grand MCA and Grand List Decoding challenges consider smooth evaluation domains at rates

$$R \in \{1/2, 1/4, 1/8, 1/16\},$$

a target ε^* such as 2^{-128} , and, for list decoding, a fixed interleaving order [ABF26, Prize26]. Smoothness is not needed by our theorems.

Corollary 8.3 (Simultaneous asymptotic certificates). *Fix $R \in (0, 1)$, $\gamma \in (0, 1 - R)$, an integer $h \geq 1$, and $\lambda > 0$. Let $k = Rn$ be an integer and let $\mathcal{C} = \text{RS}_{\mathbb{F}_q}(D, k)$ for any n distinct points in a prime field. For all sufficiently large n , define*

$$C_* := \max\{C(\gamma, 1), hC_{\text{list}}(\gamma, 1)\},$$

where $C(\gamma, 1)$ is the MCA exponent in [Theorem 1.2](#). If

$$q > 2^\lambda n^{C_*},$$

then, at $\rho = 1 - R - \gamma$,

$$\text{err}_{\text{MCA}}(\mathcal{C}, \rho) < 2^{-\lambda}, \quad \Lambda_h(\mathcal{C}, \rho) < 2^{-\lambda} q.$$

Proof. The first estimate is [Theorem 1.2](#). The second follows from [Corollary 8.2](#); the common field-size assumption dominates both polynomial budgets. $\square$

At the four designated rates and $\lambda = 128$, the certified radii are

Rate	Fixed-slack certified radius
1/2	1/2 - γ
1/4	3/4 - γ
1/8	7/8 - γ
1/16	15/16 - γ

These are lower-bound certificates for the safe radius, not a determination of the largest safe radius. In particular, the interleaved-list certificate uses the geometric $n^{O(1)}$ bound; it would not follow from the root solver's $q^{O(1)}$ bound alone.

8.4 Field characteristic and the endpoint

The interpolation construction is characteristic-free. The deterministic decoder invokes the prime-field version of Kopparty's root solver. The geometric list and MCA arguments extend to a finite field of characteristic

$$p > \max\{k - 1, B_{\gamma, L}\}$$

for the list bound, or with $L = 1$ for MCA, provided the evaluation points are distinct. Interpolation over that field and its rational-function extension is already supplied by [Corollary 3.9](#). The two characteristic requirements have different purposes: $p > k - 1$ prevents Frobenius freedom in Hasse–Taylor lifting, and $p > B_{\gamma, L}$ prevents the highest-variable partial derivative of the interpolant from vanishing identically.

None of the theorems permits replacing fixed γ by an n -dependent slack without tracking the constants and the length threshold. The results in [\[CS25, KKH26\]](#) show that the literal up-to-capacity MCA formulation requires qualification; in particular, the prime-field smooth-domain constructions in [\[KKH26\]](#) occur in a shrinking near-capacity window. The fixed-slack statements here do not address that window or the exact integer-error boundary.

8.5 Effectivity and remaining quantitative questions

The parameters are effective: the order r is chosen by [Equation \(44\)](#), $B_{\gamma, L}$ is bounded in [Lemma 4.1](#), and the geometric exponent follows from the degree recurrence in [Lemma 5.7](#) and constant-dimensional intersections. The support-isolation and support-descent arguments add only constantly many powers of the incidence size or block length.

The resulting constants are not optimized. No competitive numerical exponent or useful certificate for a prescribed small block length is claimed. Both the field-size inequality and the sufficiently-large-length threshold must be checked for a concrete application. The decoder is polynomial in q , not in $\log q$, and the list bound is polynomial in n , not constant. Improving the gap dependence, obtaining small-field MCA bounds, and converting the bounded-complexity geometry into a faster output-sensitive decoder remain separate quantitative questions.

AI Disclosure

The interactions with ChatGPT 5.6 Pro were crucial in obtaining the main results of this paper. ChatGPT 5.6 and 6 Pro were also used as an editorial assistant. The authors take full responsibility for the results and have verified all claims, proofs, and references.

References

- [ABF26] G. Arnon, D. Boneh, and G. Fenzi. Open problems in list decoding and correlated agreement. Cryptology ePrint Archive, Paper 2026/680, 2026. <https://eprint.iacr.org/2026/680>.
- [AGG25] O. Alrabiah, Z. Guo, V. Guruswami, R. Li, and Z. Zhang. Random Reed–Solomon codes achieve list-decoding capacity with linear-sized alphabets. *Advances in Combinatorics*, 2025:8, pages 1–39, 2025.
- [AGL24] O. Alrabiah, V. Guruswami, and R. Li. Randomly punctured Reed–Solomon codes achieve list-decoding capacity over linear-sized fields. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 1458–1469, 2024.
- [AHS26] V. Ashvinkumar, M. Habib, and S. Srivastava. Algorithmic improvements to list decoding of folded Reed–Solomon codes. In *Proceedings of the 2026 Annual ACM–SIAM Symposium on Discrete Algorithms*, pages 880–898, 2026.
- [BCCHKS25] E. Ben-Sasson, D. Carmon, U. Haböck, S. Kopparty, and S. Saraf. On proximity gaps of Reed–Solomon codes. In *Proceedings of the 58th Annual ACM Symposium on Theory of Computing (STOC)*, pages 1157–1167, 2026. <https://doi.org/10.1145/3798129.3800827>.
- [BCGM26] S. Bordage, A. Chiesa, Z. Guan, and I. Manzur. All polynomial generators preserve distance with mutual correlated agreement. In *41st Computational Complexity Conference (CCC 2026)*, volume 383 of *LIPICs*, pages 24:1–24:18, 2026. <https://doi.org/10.4230/LIPICs.CCC.2026.24>.
- [BCIKS20] E. Ben-Sasson, D. Carmon, Y. Ishai, S. Kopparty, and S. Saraf. Proximity gaps for Reed–Solomon codes. *Journal of the ACM*, 70(5):31:1–31:57, 2023. Preliminary version in FOCS 2020.
- [BCPZZ26] J. Brakensiek, Y. Chen, A. Putterman, Z. Zhang, and K. Z. Zheng. Algorithmic list decoding of Reed–Solomon codes up to capacity in the low-rate regime. *Electronic Colloquium on Computational Complexity*, Report TR26-164, 2026. <https://eccc.weizmann.ac.il/report/2026/164/>.
- [BGM24] J. Brakensiek, S. Gopi, and V. Makam. Generic Reed–Solomon codes achieve list-decoding capacity. *SIAM Journal on Computing*, pages STOC23-118–STOC23-154, 2024. <https://doi.org/10.1137/23M1598064>.
- [CS25] E. Crites and A. Stewart. On Reed–Solomon proximity gaps conjectures. In *Advances in Cryptology–CRYPTO 2026, Part IV*, pages 128–156. Springer, 2026. <https://eprint.iacr.org/2025/2046>.
- [CZ25] Y. Chen and Z. Zhang. Explicit folded Reed–Solomon and multiplicity codes achieve relaxed generalized Singleton bounds. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, pages 1–12, 2025.
- [GG25] R. Goyal and V. Guruswami. Optimal proximity gaps for subspace-design codes and (random) Reed–Solomon codes. In *Proceedings of the 58th Annual ACM Symposium on Theory of Computing (STOC)*, pages 1558–1568, 2026. <https://eccc.weizmann.ac.il/report/2025/166/>.

- [GHKS24] R. Goyal, P. Harsha, M. Kumar, and A. Shankar. Fast list decoding of univariate multiplicity and folded Reed–Solomon codes. In *Proceedings of the 65th Annual IEEE Symposium on Foundations of Computer Science*, pages 328–343, 2024.
- [GLS21] Z. Guo, R. Li, C. Shangguan, I. Tamo, and M. Wootters. Improved list-decodability and list-recoverability of Reed–Solomon codes via tree packings. In *Proceedings of the 62nd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2021)*, pages 708–719, 2022. <https://doi.org/10.1109/FOCS52979.2021.00074>.
- [GR08] V. Guruswami and A. Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Transactions on Information Theory*, 54(1):135–150, 2008.
- [GS99] V. Guruswami and M. Sudan. Improved decoding of Reed–Solomon and algebraic-geometric codes. *IEEE Transactions on Information Theory*, 45(6):1757–1767, 1999.
- [GST23] E. Goldberg, C. Shangguan, and I. Tamo. List-decoding and list-recovery of Reed–Solomon codes beyond the Johnson radius for every rate. *IEEE Transactions on Information Theory*, 69(4):2261–2268, 2023.
- [GW13] V. Guruswami and C. Wang. Linear-algebraic list decoding for variants of Reed–Solomon codes. *IEEE Transactions on Information Theory*, 59(6):3257–3268, 2013.
- [GZ23] Z. Guo and Z. Zhang. Randomly punctured Reed–Solomon codes achieve the list decoding capacity over polynomial-size alphabets. In *Proceedings of the 64th Annual IEEE Symposium on Foundations of Computer Science*, pages 164–176, 2023.
- [Hab25] U. Haböck. A note on mutual correlated agreement for Reed–Solomon codes. Cryptology ePrint Archive, Paper 2025/2110, 2025.
- [Har92] J. Harris. *Algebraic Geometry: A First Course*. Graduate Texts in Mathematics, volume 133. Springer, 1992.
- [Hei83] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoretical Computer Science*, 24(3):239–277, 1983.
- [Jo26] S. Jo. Reed–Solomon mutual correlated agreement beyond the Johnson radius. Cryptology ePrint Archive, Paper 2026/1432, 2026. <https://eprint.iacr.org/2026/1432>.
- [KKH26] D. Krachun, S. Kazanin, and U. Haböck. Failure of proximity gaps close to capacity. Cryptology ePrint Archive, Paper 2026/782, 2026. <https://eprint.iacr.org/2026/782>.
- [KRSW23] S. Kopparty, N. Ron-Zewi, S. Saraf, and M. Wootters. Improved list decoding of folded Reed–Solomon and multiplicity codes. *SIAM Journal on Computing*, 52(3):794–840, 2023.
- [Kop15] S. Kopparty. List-decoding multiplicity codes. *Theory of Computing*, 11(5):149–182, 2015. <https://doi.org/10.4086/toc.2015.v011a005>.
- [PG26] F. Granha Jeronimo and L. Liu. From hidden-derivative interpolation to optimal-radius proximity gaps for Reed–Solomon codes. Unpublished companion manuscript, 2026.
- [PV05] F. Parvaresh and A. Vardy. Correcting errors beyond the Guruswami–Sudan radius in polynomial time. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science*, pages 285–294, 2005.
- [Prize26] Ethereum Foundation. The Proximity Prize: 1M Reed–Solomon challenge. <https://proximityprize.org/>, accessed September 4, 2026.
- [RS60] I. S. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.
- [RW14] A. Rudra and M. Wootters. Every list-decodable code for high noise has abundant near-optimal rate puncturings. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 764–773, 2014.

- [ST23] C. Shangguan and I. Tamo. Generalized Singleton bound and list-decoding Reed–Solomon codes beyond the Johnson radius. *SIAM Journal on Computing*, 52(3):684–717, 2023.
- [Sin64] R. C. Singleton. Maximum distance q -nary codes. *IEEE Transactions on Information Theory*, 10(2):116–118, 1964.
- [Sud97] M. Sudan. Decoding of Reed–Solomon codes beyond the error-correction bound. *Journal of Complexity*, 13(1):180–193, 1997. <https://doi.org/10.1006/jcom.1997.0439>.
- [WHIR25] G. Arnon, A. Chiesa, G. Fenzi, and E. Yogev. WHIR: Reed–Solomon proximity testing with super-fast verification. In *Advances in Cryptology–EUROCRYPT 2025, Part IV*, volume 15604 of *Lecture Notes in Computer Science*, pages 214–243. Springer, 2025.

A Transfer to other root-enumeration settings

Theorem A.1 (Root-solver transfer). *Let $K > r \geq 1$ and $1 \leq k \leq K$. Suppose a field $\mathbb{F}$ has an algorithm that enumerates all degree-below- K solutions of*

$$Q(X, P, P^{[1]}, \dots, P^{[r]}) \equiv 0$$

for every nonzero Q with individual Y -degree at most B and

$$\deg_{(1, K-1, K-2, \dots, K-r-1)} Q < D,$$

in time T_{root} and with at most L_{root} outputs. Under Equations (46) and (47), sparse list recovery over $\mathbb{F}$ with actual degree bound $k-1$ is solvable using

$$r^{O_{\vartheta}(r)} \text{poly}(n, M, B) + T_{\text{root}} + L_{\text{root}} \text{poly}(n, K, M)$$

field operations, with output list at most L_{root} , provided $D \geq r^3 A$ and the assumed root solver applies to the interpolant constructed in Proposition 3.8.

Proof. The interpolation construction, dimension estimate, local rank bound, and multiplicity argument are field-independent. Construct a nonzero interpolant, invoke the assumed root solver, and filter its output by the actual degree bound and list agreement. The last summand explicitly accounts for verification of all returned roots; the transfer does not assume that this cost is already included in T_{root} . $\square$

B Quantitative derivative order and parameter ledger

B.1 Inverting the sparse-incidence condition

The uniform fixed-slack statement is convenient for the main theorems. The following more detailed form retains the dependence on a target agreement ε and a multiplicative slack ϑ .

Corollary B.1 (Bounded-list recovery at every constant agreement). *Fix $\vartheta \in (0, 1)$, $\varepsilon \in (0, 1)$, and $L \geq 1$. Let*

$$A = \lceil \varepsilon n \rceil, \quad K = \lceil (1 - \vartheta)A \rceil,$$

and suppose $k \leq K$. For all sufficiently large n , there is an effective choice

$$r = O_{\vartheta} \left(\left(1 + \frac{L}{\varepsilon} \right)^{1/\vartheta} \log^{5/\vartheta} \left(e + \frac{L}{\varepsilon} \right) \right) \quad (74)$$

for which every instance with $|S_i| \leq L$ is list recoverable up to A hits by the algorithm of Theorem 4.4. Over every prime $q \geq n$ satisfying the degree conditions, the time is $q^{O_{\vartheta}(r)}$ and the list size is at most q^{4r+6} .

Proof. Because $K - 1 < (1 - \vartheta)A$,

$$\frac{A}{K - 1} > \frac{1}{1 - \vartheta}.$$

Also $M \leq Ln$ and $K - 1 = \Omega_{\vartheta}(\varepsilon n)$. Thus

$$\frac{M}{K - 1} = O_{\vartheta}\left(\frac{L}{\varepsilon}\right).$$

Let $x = 1 + L/\varepsilon$. For a sufficiently large hidden constant in [Equation \(74\)](#),

$$\frac{r^{\vartheta}}{\log^4(er)} \geq C_{\vartheta}x,$$

so [Equation \(47\)](#) holds. Since r is fixed once $\vartheta, \varepsilon, L$ are fixed, the remaining inequalities $r < K$, $B < q$, and $r^3 A < q^2$ hold for all sufficiently large n whenever $q \geq n$. $\square$

In particular, at rate at most $(1 - \vartheta)\varepsilon$, singleton lists need only

$$r = O_{\vartheta}\left((1 + 1/\varepsilon)^{1/\vartheta} \log^{5/\vartheta}(e + 1/\varepsilon)\right).$$

The interpolation and root-enumeration stages both take $q^{O_{\vartheta}(r)}$ operations in their stated prime-field parameter range. This is a fixed-parameter polynomial-time bound; it is not polynomial dependence on $1/\vartheta$ or on the additive capacity gap.

B.2 Rounding and field-size thresholds

At the actual capacity-minus- γ radius, set $A = k + \lceil \gamma n \rceil$ and $K = \lceil (1 - \gamma/2)A \rceil$. The upper bound $k \leq (1 - \gamma)n$ implies $A \leq n$, while [Lemma 4.1](#) gives $K \geq k$ and $K - 1 < (1 - \gamma/2)A$. The same lemma applies at smaller radii by increasing A up to n .

After γ, L are fixed, $r, m, B_{\gamma, L}$ are constants and $K = \Theta_{\gamma}(n)$. Thus $r < K$, $B < q$, and $r^3 A < q^2$ hold for sufficiently large n whenever $q \geq n$. The stricter field-size budget in [Corollary 8.3](#) serves a different purpose: it makes a polynomial number of exceptional parameters, or a polynomial list size, small relative to q .

B.3 Parameter ledger

Parameter	Choice	Role
γ	Fixed additive slack	Gives $A - k \geq \gamma n$ and a rate-uniform interpolation budget.
L	Input-list bound	Implies $M \leq Ln$; constants for recovery depend on L .
ℓ	Curve degree	Bounds the degree of evaluation hypersurfaces in MCA.
A	Required number of hits	Supplies root multiplicity at least mA .
K	$\lceil (1 - \vartheta)A \rceil$	Padded degree ceiling, at least the actual dimension k .
ϑ	$\gamma/2$ for uniform padding	Fixed multiplicative degree margin.
r, m	r from Equation (44); $m = r^3$	Differential order and local multiplicity.
c, s	$(1 - \vartheta)^{-1} - 2/\log(er)$ and $(1 - \vartheta)^{-1} - 1/\log(er)$	Weighted and ordinary tail cutoffs.
W	$\lfloor crm/\log(er) \rfloor$	Weighted derivative-tail budget.
B	$\lceil mA/(K - 1) \rceil$	Total derivative-variable degree bound.
D_0	$O(n)$ at fixed parameters	Coefficient-degree scale in the jet theorem.
E_Q	Finite exceptional set	Values lost under derivative-content specialization.
Δ	Polynomial in n	Total cumulative degree of the solution cover.
S_P, S_z	Full list-hit or exact agreement support	Determines all cuts; no agreement subset is substituted for an MCA witness's support.