Electronic Colloquium on Computational Complexity, Report No. 304 (2026)

Combinatorial limitations of list-decoding Reed–Solomon codes

Omar Alrabiah* Rohan Goyal† Venkatesan Guruswami‡

October 2026

Abstract

For infinitely many rates $R \in (0,1)$, we show that full-length Reed–Solomon codes over fields of low characteristic can contain super-polynomially many codewords in a Hamming ball of radius just exceeding the Johnson radius. Over prime fields, we exhibit full-length Reed–Solomon codes of constant rate R with polynomially many codewords in a Hamming ball of relative radius bounded strictly below $1 - R$. This refutes a recent conjecture that, over prime fields, list sizes below capacity are always bounded by a constant. Together, these results demonstrate that certain restrictions in recent works on explicit Reed–Solomon codes achieving list-decoding capacity, related to the choice of field or evaluation points or to the list-size guarantee, are inherent.

*Department of Electrical Engineering and Computer Sciences, UC Berkeley, Berkeley, CA 94709, USA. Email: oalrabiah@berkeley.edu. Research supported in part by a Saudi Arabian Cultural Mission (SACM) Scholarship, ONR grant N00014-24-1-2491, and V. Guruswami's Simons Investigator Award.

†Massachusetts Institute of Technology, Cambridge, MA, USA. Email: rohan_g@mit.edu. Research supported by Yael Tauman Kalai's NSF Award 6956054.

‡Department of Electrical Engineering and Computer Sciences, Department of Mathematics, and the Simons Institute for the Theory of Computing, UC Berkeley, Berkeley, CA 94709, USA. Email: venkatg@berkeley.edu. Research supported in part by a Simons Investigator Award, a UC Noyce initiative award, DOD Advanced Research Projects Agency grant HR0011262E031, and NSF grant 2211972.

ISSN 1433-8092

1 Introduction

List decoding, introduced by Elias and Wozencraft [Eli57, Woz58], is a decoding paradigm in which a decoder for a code $C \subseteq \Sigma^n$ over a finite alphabet Σ receives a word $y \in \Sigma^n$ and outputs all codewords $c \in C$ satisfying $d_{\mathrm{H}}(c, y) \leqslant \rho n$, where d_{H} denotes Hamming distance and ρ is the prescribed fractional decoding radius. Unlike unique decoding, which seeks a single codeword close to the received word, list decoding remains meaningful beyond half the minimum distance of C, where a received word may be close to multiple codewords. More formally, we call C (ρ, L)-*list-decodable* if $|C \cap B(y, \rho n)| \leqslant L$ for every $y \in \Sigma^n$, where $B(y, r) \coloneqq \{z \in \Sigma^n : d_{\mathrm{H}}(z, y) \leqslant r\}$ denotes the Hamming ball of radius r around y. A central goal in list-decoding is to maximize the decoding radius ρ while keeping the list size L small, ideally by a constant or at most a polynomial in n. For arbitrary codes, a first general answer to this question is provided by the Johnson bound [Joh62] (for simple proofs and extensions, see [GS01]). Specifically, if a code C has relative distance δ, then the list size $|C \cap B(y, \rho n)|$ is at most polynomial in n for every $y \in \Sigma^n$ whenever $\rho < 1 - \sqrt{1-\delta}$, and it is in fact $O(1/\varepsilon)$ when $\rho = 1 - \sqrt{1-\delta} - \varepsilon$. We call $1 - \sqrt{1-\delta}$ the *Johnson radius*.

A canonical family of codes in this context is Reed–Solomon codes [RS60], whose optimal distance makes them especially well suited to the study of list-decoding. A Reed–Solomon code of dimension k over a finite field $\mathbb{F}$ encodes each polynomial in $\mathbb{F}[X]$ of degree less than k by its values at n distinct evaluation points in $\mathbb{F}$. It has rate $R = k/n$ and relative distance $\delta = (n-k+1)/n = 1 - R + 1/n$, which meets the Singleton bound [Sin64]. Consequently, since $1 - \delta = R - 1/n$, its Johnson radius equals $1 - \sqrt{R - 1/n}$, which, as a function of the rate R, is $1 - \sqrt{R}$ up to an additive $O(1/n)$ term. Thus, this optimal distance translates into a strong list-decoding guarantee, and this is made particularly compelling by the existence of *efficient* algorithms that achieve it. This began with classical algorithms [Pet60, Ber68, Mas69, WB86] that decode Reed–Solomon codewords in polynomial time up to half their minimum distance and was later extended to the list-decoding algorithm of Guruswami and Sudan [GS99], building on Sudan's earlier algorithm [Sud97], that goes up to the Johnson radius for *arbitrary* Reed–Solomon codes.

In general, however, super-polynomial list sizes can occur just beyond the Johnson radius. A folklore random coding argument shows that there are (not necessarily linear) codes C of relative distance δ and words y for which $|C \cap B(y, \rho n)|$ is super-polynomial in n, with ρ only slightly exceeding $1 - \sqrt{1-\delta}$ [GRS00, Section 4.3]. Moreover, this phenomenon can occur even for binary *linear* codes [Gur02, GS03].[1]

These limitations raise the question of how far beyond the Johnson radius Reed–Solomon codes can be efficiently list-decoded. The ultimate limit is the *list-decoding capacity* $1 - R$, beyond which no code of rate R can have sub-exponential list sizes. Indeed, if $|\Sigma| \geqslant n$, say, then for every $\varepsilon > 0$ the product $|C| \cdot |B(y, (1 - R + \varepsilon)n)|$ exceeds $|\Sigma|^n$ by an exponential factor, and hence $|C \cap B(y, (1 - R + \varepsilon)n)|$ is exponential in n on average over a uniformly random center $y \in \Sigma^n$. On the other hand, random codes of rate R over large alphabets achieve the capacity, being $(1 - R - \varepsilon, O(1/\varepsilon))$-list-decodable [ZP81, Eli91].

For Reed–Solomon codes, however, it remained conceivable that *every* such code could be list-decoded beyond the Johnson radius, and in fact up to the capacity $1 - R$, with polynomially bounded lists. More precisely, one could hope that for every $\varepsilon > 0$, every Reed–Solomon code of rate R is $(1 - R - \varepsilon, L)$-list-decodable with L polynomial in n. Some evidence for this possibility comes from Reed–Solomon codes with *random* (or generic) evaluation points over large fields, which exhibit behavior

[1] For binary codes, the Johnson radius is $(1 - \sqrt{1-2\delta})/2$, and more generally, for alphabet size q, it is $(1 - 1/q)(1 - \sqrt{1 - q\delta/(q-1)})$.

similar to that of random linear codes. Starting with the work of Rudra and Wootters [RW14] in the high-noise regime, and later that of Shangguan and Tamo [ST23], a sequence of works established list-decodability of such codes beyond the Johnson radius [ST23, GLS+21, FKS22, GST23], eventually reaching capacity with constant list size [BGM23, GZ23, AGL24, AGG+25]. However, these results apply to random evaluation points and provide no guarantees for a particular Reed–Solomon code, such as the *full-length* code over a given field, whose evaluation points are all the elements of the field and whose length n is therefore the field size. For arbitrary evaluation points, the recent work of Brakensiek, Chen, Putterman, Zhang and Zheng [BCP+26] establishes capacity-approaching list-decoding over sufficiently large prime fields, as we discuss below.

The contrasting possibility—that the Johnson radius is the true limit for some Reed–Solomon codes—has been explored in several earlier works. This began with the work of Justesen and Høholdt [JH01], which studied the list sizes of MDS codes (codes meeting the Singleton bound, such as Reed–Solomon codes) around the Johnson radius, proving upper bounds on the number of codewords and exhibiting received words with polynomially many nearby codewords. In a related direction, Guruswami and Rudra [GR06] considered the notion of list recovery, a generalization of list decoding in which each coordinate of the received word is replaced by a small set of allowed symbols, and showed that Reed–Solomon codes cannot be list-recovered beyond the natural analogue of the Johnson radius with polynomially bounded lists. Their construction uses polynomials over an extension field that take values in a subfield, an ingredient that also appears in our proof of Theorem 1.1.

Complementing these combinatorial investigations, several works have established computational barriers to decoding Reed–Solomon codes. In particular, maximum-likelihood decoding is NP-hard in general [GV05], and in certain parameter regimes, list-decoding beyond the Johnson radius is at least as hard as computing discrete logarithms in finite fields [CW07]. These hardness results, however, do not rule out polynomially bounded list sizes.

An earlier precursor to our work, more directly addressing the existence of large lists beyond the Johnson radius, is the work of Ben-Sasson, Kopparty and Radhakrishnan [BSKR10], who used subspace polynomials to construct received words with super-polynomially many nearby codewords in full-length Reed–Solomon codes beyond the Johnson radius. Their construction, however, yields super-polynomial list sizes only when the code rate tends to zero, a regime in which both the Johnson radius and the list-decoding capacity approach 1. At any fixed positive rate, the list sizes obtained by their construction are only polynomial in the block length.

Extension field RS codes that are not list-decodable just past the Johnson radius. Our first result shows that the Johnson radius is essentially a barrier to list decoding with polynomially bounded lists for certain full-length Reed–Solomon codes of constant rate over extension fields. Specifically, for rates $R = q^{-2}$ and $R = (1 - q^{-1})^2$, where q is a prime power, we construct received words with super-polynomially many nearby codewords at a relative distance arbitrarily close to the Johnson radius $1 - \sqrt{R}$ from above. In particular, there is a received word y such that for every fixed $\varepsilon > 0$, these codes have super-polynomially many codewords in the Hamming ball $B\Big(y, (1 - \sqrt{R} + \varepsilon)n\Big)$. Unlike the earlier constructions based on subspace polynomials, our lower bounds hold at constant rate, where the Johnson radius and the list-decoding capacity $1 - R$ are separated by a constant. Our result also addresses a question left open by the recent work of Brakensiek, Chen, Putterman, Zhang, and Zheng [BCP+26], who established capacity-approaching list-decodability for arbitrary evaluation points over sufficiently large *prime* fields, leaving open whether analogous guarantees hold over general finite fields. We show that such guarantees cannot hold in general over extension fields of fixed characteristic.

Theorem 1.1 (Not all RS codes are list-decodable beyond Johnson radius)**.** *Let q be any prime power, and let R be either q^{-2} or $(1-q^{-1})^2$. For every integer $t \geqslant 1$, let $n = q^{4t}$. Then there is an explicit received word $y \in \mathbb{F}_{q^{4t}}^n$ such that the full-length Reed–Solomon code over $\mathbb{F}_{q^{4t}}$ of rate R has $n^{\Omega_q(\log n)}$ codewords at relative distance $1 - \sqrt{R} + O_q(n^{-1/4})$ from y.*

Together with the Johnson bound, Theorem 1.1 (proved in Section 3) shows that the Johnson radius is essentially the exact threshold for polynomially bounded lists in these full-length Reed–Solomon codes. For q ranging over prime powers, this phenomenon occurs at two infinite families of constant rates, $R = q^{-2}$ and $R = (1-q^{-1})^2$, which approach 0 and 1, respectively, as q grows. At each of these rates, one can be $o(1)$ close to the Johnson radius and still get super-polynomially large lists. Whether the same phenomenon occurs at every fixed rate $R \in (0,1)$ remains open.

Thus, for a Reed–Solomon code of rate R over a field of small characteristic to be $(1-\sqrt{R}+\varepsilon, L)$-list-decodable, for a fixed $\varepsilon > 0$ and with L polynomial in n, one has to place restrictions on its set of evaluation points. Indeed, the fields $\mathbb{F}_{q^{4t}}$ in Theorem 1.1 all have the characteristic of the fixed base field $\mathbb{F}_q$, and the codes in the theorem use every element of these fields as an evaluation point. In a companion paper [AGG26], we show a positive result in this regard: for a careful choice of *explicit* evaluation points in an extension field, one can list-decode up to capacity, and in fact achieve a list size that is optimal as a function of the gap to capacity.

Prime field RS codes. For prime fields, as discussed earlier, a striking recent result of Brakensiek, Chen, Putterman, Zhang, and Zheng [BCP+26] established that Reed–Solomon codes over sufficiently large prime fields can be list-decoded up to capacity, that is, up to a relative radius approaching $1-R$, for *every* choice of evaluation points. More precisely, for every constant rate R and every $\varepsilon > 0$, provided the prime is at least a suitable constant multiple (depending on R and ε) of the code length, every Reed–Solomon code of rate R over the prime field is $(1-R-\varepsilon, L)$-list-decodable with L polynomial in the field size, and the list can be found in time polynomial in the field size [BCP+26, Corollary 5.1]. The formulation in Harsha, Kumar and Saptharishi [HKS26, Theorem 1.1] (and also the immediate follow-up [Jer26] to [BCP+26]) requires only $p \geqslant n$ over a prime field $\mathbb{F}_p$, and therefore covers *every* prime-field Reed–Solomon code of constant rate $R < 1$, including the full-length code (they also make the list size polynomial in the block length as opposed to field size).

The result of [BCP+26], however, yields a polynomial list-size bound with a large exponent that depends doubly exponentially on $1/\varepsilon$. It has been conjectured [CGH+26, Conjecture 1] that, over prime fields, list-decoding capacity can in fact be achieved with a constant list size $L = L(R, \varepsilon)$. In the opposite direction, Krachun, Kazanin, and Haböck [KKH26, Theorem 1] constructed arbitrarily large polynomial lists for Reed–Solomon codes over prime fields whose evaluation points form a multiplicative subgroup, but only at a vanishing gap of order $1/\log n$ below capacity.

Our second result refutes this conjecture definitively by exhibiting lists of polynomial size for full-length Reed–Solomon codes at a constant gap below capacity. Specifically, for every integer $m \geqslant 2$ with $m \equiv 2 \pmod 3$, it gives full-length Reed–Solomon codes over prime fields of rate $R \approx 2/(3m)$ with at least $\mathrm{poly}(n)$ codewords in a Hamming ball of relative radius about $1 - 1/m$, which is about $1/(3m)$ below the capacity $1-R$.

Theorem 1.2 (Linear-sized lists below capacity over prime fields)**.** *Let $m \geqslant 2$ be an integer such that $m \equiv 2 \pmod 3$. Then, there exist infinitely many primes p such that the full-length Reed–Solomon code over $\mathbb{F}_p$ of length $n = p$ and dimension $\frac{2(p+m-1)}{3m}$ has an explicit received word $y \in \mathbb{F}_p^n$ at Hamming distance exactly $p - \frac{p-1}{m}$ from at least n codewords.*

We prove Theorem 1.2 in Section 4. There is no technical dependence between Theorems 1.1 and 1.2, so one can read Section 4 independently from Section 3.

Setting $m = 2$ in Theorem 1.2 gives us the following corollary.

Corollary 1.3 (Linear lists below capacity over prime fields)**.** *For infinitely many primes p, the full-length Reed–Solomon code over $\mathbb{F}_p$ of length $n = p$ and dimension $(p+1)/3$ has an explicit received word $y \in \mathbb{F}_p^n$ at Hamming distance exactly $(p+1)/2$ from at least n codewords.*

Via a simple list-amplification technique described in the overview below, one can boost the list size in Theorem 1.2 to obtain any polynomial list size, at the expense of a larger decoding radius. This is the content of the following result.

Theorem 1.4 (Arbitrary polynomial-lists)**.** *For any integer $\ell \geqslant 2$, there are infinitely many primes p such that the full-length Reed–Solomon code over $\mathbb{F}_p$ of length $n = p$ and rate $R = \Omega(1/\ell)$ is not $(1 - R - \Omega(1/\ell^2), \binom{n}{\ell}/2)$-list-decodable.*

Organization. Section 2 provides an overview of the ideas behind the proofs of both cases. In Section 3, we prove the limitations of list-decoding at the Johnson bound for small characteristic fields (Theorem 1.1). In Section 4, we prove the limitations over prime fields (Theorem 1.2 and Theorem 1.4). There is no technical dependence between Theorems 1.1 and 1.2 (with the latter being simpler), and so they can be read independently.

Concurrent work. In independent recent works, Dao, Kominers, Thaler and Zheng [DKTZ26] and Zhu [Zhu26] also prove a lower bound for list decoding full-length Reed–Solomon codes of rate q^{-2} whenever q is a power of two, with list size $n^{\Omega_q(\log n)}$ at relative radius $1 - q^{-1} + o(1)$. Their results thus include the low-rate conclusion of Theorem 1.1 when q is a power of two. Neither of these works has any result concerning limitations of list decoding prime field Reed–Solomon codes, and in particular do not include the analogs of Theorems 1.2 and 1.4.

2 Proof overview

To demonstrate a list-size lower bound of L at relative radius ρ, we need to exhibit a received word with L distinct codewords within relative Hamming distance ρ. Concretely, let $\mathbb{F}$ be a finite field, set $n \coloneqq |\mathbb{F}|$, and let $C \subseteq \mathbb{F}^n$ be the full-length Reed–Solomon code of rate $R \in (0,1)$, evaluated at all elements of $\mathbb{F}$. By interpolation, any received word $y \in \mathbb{F}^n$ can be written as $y = (g(\alpha))_{\alpha \in \mathbb{F}}$ for a polynomial $g \in \mathbb{F}[X]$ of degree less than n. Each codeword $c_i \in C$ is the evaluation $c_i = (f_i(\alpha))_{\alpha \in \mathbb{F}}$ of a message $f_i \in \mathbb{F}[X]$ of degree less than Rn. Thus c_i agrees with y at a position $\alpha \in \mathbb{F}$ precisely when $g(\alpha) - f_i(\alpha) = 0$. Defining the *error polynomial* $p_i \coloneqq g - f_i$, we can therefore reformulate the problem as finding distinct polynomials $p_1, \ldots, p_L \in \mathbb{F}[X]$ satisfying the following two properties.

(i) Each p_i has at least $(1-\rho)n$ distinct roots in $\mathbb{F}$.

(ii) The polynomials share all coefficients of degree at least Rn; equivalently, $\deg(p_i - p_j) < Rn$ for every i, j.

Indeed, the first property expresses the required agreements, and the second follows from $p_i - p_j = f_j - f_i$. Conversely, given such polynomials, let g be their common high-degree part. Then $f_i \coloneqq g - p_i$ are distinct messages of degree less than Rn, whose evaluations agree with the evaluation of g at the roots of p_i. Since evaluation is injective on polynomials of degree less than n, this gives L distinct codewords within distance ρn of a common received word.

The difficulty is to satisfy both properties simultaneously. On the one hand, we can easily satisfy property (ii) by taking a common monomial X^D, with $D \geqslant Rn$, and adding a few terms of degree

less than Rn. However, this offers no control over the number of roots in $\mathbb{F}$. On the other hand, we can choose arbitrary sets $A_1, \ldots, A_L \subseteq \mathbb{F}$ of size at least $(1-\rho)n$ and take $p_i \coloneqq \prod_{a \in A_i}(X-a)$. These polynomials automatically satisfy property (i), but ensuring that their high-degree coefficients agree is much more difficult.

Indeed, a root polynomial of degree $(1-\rho)n$ has about $(1-\rho-R)n$ high-degree coefficients, with roughly $n^{(1-\rho-R)n}$ possible coefficient tuples. For a radius ρ bounded a constant below the capacity $1-R$, this number far exceeds the at most 2^n subsets of $\mathbb{F}$, so direct pigeonholing does not guarantee a large family with a common high-degree part. The counting argument of Justesen and Høholdt [JH01], as reformulated in [BSKR10], follows this approach, but applies only at radii close to capacity.

This brings us to a natural question about polynomials over finite fields: how does the sparsity of a polynomial relate to the number of roots it has? Our constructions exploit this connection through structured choices of the agreement sets A_i, allowing us to obtain many roots while arranging the required cancellation of high-degree terms.

In this overview, we reverse the order of the main proofs, beginning with the simpler construction over prime fields before turning to extension fields.

2.1 Prime fields: choosing and moving the agreement sets

Our prime-field construction starts with a set whose root polynomial is especially sparse: a multiplicative subgroup $H \subseteq \mathbb{F}_p^\times$ of size t, with root polynomial $X^t - 1$. We obtain many agreement sets A_i by moving H under low-degree maps. The key observation is that the multiplicative symmetry of H forces a long gap below the leading term even after its roots have been moved. Specifically, if $f(0) = 0$ and $1 \leqslant \deg(f) = d < t$, then

$$P_f(X) \coloneqq \prod_{u \in H}(X - f(u)), \qquad \deg(P_f - X^t) \leqslant t - \lceil t/d \rceil \,.$$

Thus, low-degree maps preserve a common high-degree part, while maps that are injective on H preserve the number of distinct roots. This separates the two requirements on our error polynomials (Lemma 4.1).

For primes $p \equiv 2 \pmod 3$, a convenient family is given by the shifted cubes $f_a(X) = (X+a)^3 - a^3$, indexed by $a \in \mathbb{F}_p$. These maps are permutations of $\mathbb{F}_p$, so each agreement set $A_a = f_a(H)$ has size t. Choosing a proper subgroup with $t > 3$ and $t \equiv 2 \pmod 3$ also makes these sets pairwise distinct: a single moment of A_a recovers a. Consequently, the p error polynomials P_{f_a} all have t roots and share the top part X^t, with the remaining terms of degree at most about $2t/3$. Taking t to be a fixed positive fraction of p gives linear-sized lists at a constant gap below capacity, proving Theorem 1.2. For example, taking H to be the squares gives rate about $1/3$ and relative distance about $1/2$.

To obtain larger lists, we multiply ℓ of these error polynomials. Their root sets become unions of ℓ moved copies of H, and the products retain a common top part $X^{\ell t}$ with a gap of about $t/3$ below it. Choosing H sufficiently small keeps the average overlap between the copies low, so many unions contain nearly ℓt points. Now, we show that sufficiently many moments show that different choices of factors give distinct products. This yields lists of size $\Omega_\ell(n^\ell)$ at rate $\Theta(1/\ell)$ and a gap $\Omega(1/\ell^2)$ below capacity, as in Theorem 1.4. The details are in Section 4.

2.2 Extension fields: subspaces and the BKR construction

Over $\mathbb{F}_{q^m}$, we can instead exploit its vector space structure over $\mathbb{F}_q$. The construction of Ben-Sasson, Kopparty and Radhakrishnan [BSKR10] chooses the agreement sets A_i to be $\mathbb{F}_q$-linear subspaces. If A has dimension r, its *subspace polynomial* is linearized:

$$p_A(X) := \prod_{a \in A} (X - a) = X^{q^r} + \sum_{j=0}^{r-1} c_j X^{q^j}.$$

The q^r roots give the agreements, and the restriction to powers of q leaves very few high-degree coefficients to control.

A useful illustration is offered by hyperplanes. Let $\mathrm{Tr} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ be the field trace. Every $\mathbb{F}_q$-linear functional on $\mathbb{F}_{q^m}$ is uniquely of the form $x \mapsto \mathrm{Tr}(\lambda x)$. Thus every hyperplane is the kernel of such a functional with $\lambda \neq 0$, and its monic root polynomial is $p_A = \lambda^{-n/q} \mathrm{Tr}(\lambda X)$, where $n = q^m$. Its leading term is $X^{n/q}$ and its next possible term has degree n/q^2. Hence all $(n-1)/(q-1)$ hyperplanes already give error polynomials with a common top part for code dimension $n/q^2 + 1$, each with n/q roots. This gives a linear-sized list at a radius approaching the Johnson radius for rate q^{-2}.

Allowing subspaces of other dimensions gives the more general BKR construction. Its counting argument yields super-polynomial lists when the rate tends to zero, but only polynomial lists at constant rate. To obtain super-polynomial lists at constant rate, we need a much larger family of agreement sets while retaining control of the high-degree coefficients.

2.3 From subspaces to quadratic agreement sets for super-polynomial lists

For fixed q, a subspace containing a constant fraction of $\mathbb{F}_{q^m}$ has bounded codimension, leaving only polynomially many choices. A natural next step is to replace linear equations by quadratic ones. Their zero sets can still contain about n/q points, where $n = q^m$, but there are $q^{\Theta(m^2)}$ quadratic forms. This offers enough agreement sets for a super-polynomial list at constant rate, provided we can obtain error polynomials with a common high-degree part.

Here we encounter an additional issue. Although quadratic in the $\mathbb{F}_q$-coordinates, Q has much larger degree as a univariate polynomial. Unlike a subspace polynomial, it can have repeated roots, so its degree need not equal the size of its zero set. It turns out that understanding these extra multiplicities will also help us align the high-degree coefficients.

The link comes from the bilinear form $B_Q(x, y) = Q(x+y) - Q(x) - Q(y)$. For each fixed y, this is a linear functional of x, so the trace representation used in the hyperplane example lets us write $B_Q(x, y) = \mathrm{Tr}(xL_Q(y))$ for a unique coefficient $L_Q(y)$. Bilinearity makes $y \mapsto L_Q(y)$ an $\mathbb{F}_q$-linear map, represented by a linearized polynomial of degree less than n. The construction below will ensure $\deg(Q) < 2n/q$. Under this condition, we have the key identity

$$Q^q - Q \equiv (X^n - X)L_Q. \tag{1}$$

The factor $X^n - X$ is natural: since Q is $\mathbb{F}_q$-valued, $Q^q - Q$ vanishes at every field element. The identity says more by identifying the quotient with L_Q. For suitable Q, this factor accounts for the extra root multiplicities, and removing part of it will give the desired common high-degree part. We therefore seek a large family in which these multiplicities can be controlled.

The hyperplane example suggests how to build such a family. There we composed the trace with the linear maps $x \mapsto \lambda x$. We now compose a fixed quadratic form H with a richer collection of linear

maps P, giving $Q(x) = H(P(x))$. Its zero set is the preimage under P of the zero set of H. This preserves the quadratic structure while allowing many agreement sets. Taking P to be a low-degree linearized polynomial also controls the univariate exponents.

A convenient choice of H comes from the field structure itself. For $m = 4t$, take the norm $x \mapsto x \cdot x^{q^{2t}}$ from $\mathbb{F}_{q^{4t}}$ to $\mathbb{F}_{q^{2t}}$, followed by the trace from $\mathbb{F}_{q^{2t}}$ to $\mathbb{F}_q$. The norm multiplies two $\mathbb{F}_q$-linear maps, and the trace makes the resulting quadratic form $\mathbb{F}_q$-valued. We want every root of L_Q to be a zero of Q. To arrange this, we first choose a t-dimensional subspace U on which H vanishes. On $U^\perp$, with orthogonality defined by the bilinear form of H, we have $H(x + u) = H(x)$ for every $x \in U^\perp$ and $u \in U$. This suggests choosing P to have image $U^\perp$. Then Q is unchanged by translation along $P^{-1}(U)$ and vanishes on this subspace. In fact, $\ker L_Q = P^{-1}(U)$, so Q vanishes on the entire kernel of L_Q. This gives the roots at which we will later remove the extra multiplicity.

We choose a monic P of degree q^t, the smallest possible degree for a polynomial whose kernel has q^t points. This keeps the powers of q appearing in the two factors of the norm separated: the shift by $2t$ in $P(X)^{q^{2t}}$ exceeds the range of indices in P. Consequently, even after taking the trace, the polynomial representing Q on the field contains only mixed terms $X^{q^i+q^j}$ with $i \neq j$. Its degree is therefore less than $2n/q$ (in fact at most $n/q + n/q^2$), as required for the key identity.

The same restriction controls the correction factor L_Q. Its powers X^{q^k} have indices between t and $3t$, so it can be written as $L_Q = S^{q^t}$ with $\deg(S) \leqslant q^{2t}$. Here the polynomial root exists because every exponent is divisible by q^t and every coefficient has a q^tth root in the field. In particular, L_Q has the polynomial qth root we will need.

The subspace $W = P^{-1}(U)$ has q^{2t} points, all of which are roots of S. These already exhaust its degree bound. Thus S is a scalar multiple of the subspace polynomial of W, and $\deg(L_Q) = q^t \deg(S) = q^{3t} = n^{3/4}$. This explains the role of the subspaces in our construction: they ensure that the correction factor has all its roots among the zeros of Q, while its degree remains small compared with n.

We can now return to the error polynomials. The extra input from our construction is that every root of L_Q lies in the field and is a zero of Q. Using these two facts, the key identity (1) shows that each such root has multiplicity in Q exactly one greater than its multiplicity in L_Q. Hence L_Q divides Q, and dividing by the polynomial q'th root established above gives a polynomial $p_Q = Q/L_Q^{1/q}$ with precisely the same zeros as Q.

Once this division is justified, the common high-degree part follows directly from the key identity. Indeed, dividing the key identity by L_Q gives $p_Q^q = X^n - X + Q/L_Q$, and rearranging we have

$$(p_Q - X^{n/q})^q \equiv Q/L_Q - X.$$

Comparing degrees in the key identity gives $q \deg(Q) = n + \deg(L_Q)$, so $\deg(Q/L_Q) < n/q$. It follows that $p_Q = X^{n/q} - f_Q$ with $\deg(f_Q) < n/q^2$. This partial removal of multiplicity preserves every zero and gives error polynomials with the same leading term $X^{n/q}$, with all remaining terms of degree less than n/q^2, exactly as we desired.

There are many choices of U: when selecting an ordered basis, at least $q^{3t} - q^{2t}$ choices remain at each step while keeping H zero on the span. A fixed Q accounts for at most q^{2t^2} such bases, since the possible kernels of P lie inside the fixed $2t$-dimensional space $\ker(L_Q)$. Comparing these counts gives at least $q^{t^2}/2 = n^{\Omega_q(\log n)}$ distinct forms (Lemma 3.8).

Their zero sets have size $\deg(Q/L_Q) = n/q - O_q(n^{3/4})$. At most $q - 1$ forms give the same codeword after normalization. We therefore obtain a super-polynomial list at rate $R = q^{-2}$ with agreement fraction just below $\sqrt{R}$ (Section 3.1).

For the high-rate result, we use the agreement set $\{\alpha : Q(\alpha) \neq 1\}$, with slightly fewer than $(1 - 1/q)n$ points. Multiplying the factors $Q - c$ for $c \in \mathbb{F}_q \setminus \{1\}$ and again removing suitable multiplicities gives the required common high-degree part at rate $R = (1 - q^{-1})^2$, again just beyond the Johnson radius (Section 3.2).

3 Superpolynomial lists just past the Johnson radius in extension fields

In this section, we prove Theorem 1.1. Throughout this section, we fix a prime power q and an integer $t \geqslant 1$, and we set $m \coloneqq 4t$ to be the degree of the field extension $\mathbb{F}_{q^{4t}}/\mathbb{F}_q$ in which we work. For any integer $s \geqslant 1$, we write $\equiv$ to denote polynomial identities in $\mathbb{F}_{q^s}[X]$ and $=$ for equalities over $\mathbb{F}_{q^s}$. We call a polynomial $P \in \mathbb{F}_{q^s}[X]$ $\mathbb{F}_q$**-valued** if $P(\alpha) \in \mathbb{F}_q$ for every $\alpha \in \mathbb{F}_{q^s}$. The field **trace** from $\mathbb{F}_{q^s}$ to $\mathbb{F}_q$ is the polynomial $\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q} \in \mathbb{F}_{q^{4t}}[X]$ defined as

$$\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_q}(X) \coloneqq \sum_{i=0}^{s-1} X^{q^i}.$$

For the sake of brevity, we abbreviate $\mathrm{Tr}_{\mathbb{F}_{q^{4t}}/\mathbb{F}_q}$ to Tr throughout. Note that for any $\alpha \in \mathbb{F}_{q^{4t}}$, we have that $\mathrm{Tr}(\alpha)^q = \mathrm{Tr}(\alpha)$, and so $\mathrm{Tr}(\alpha) \in \mathbb{F}_q$. Thus, the trace map is an $\mathbb{F}_q$-valued polynomial.

Next, we recall linearized polynomials.

Definition 3.1 (Linearized polynomials)**.** A polynomial $L \in \mathbb{F}_{q^{4t}}[X]$ is said to be **linearized** if it has the form $L(X) \equiv \sum_{i=0}^{r} a_i X^{q^i}$ for some integer $r \geqslant 0$ and coefficients $a_0, \ldots, a_r \in \mathbb{F}_{q^{4t}}$. Such a polynomial is additionally said to be **symmetric** if $\mathrm{Tr}(L(\alpha)\beta) = \mathrm{Tr}(\alpha L(\beta))$ for every $\alpha, \beta \in \mathbb{F}_{q^{4t}}$.

To clarify the nomenclature behind linearized polynomials, observe that, equivalently, a polynomial $L \in \mathbb{F}_{q^{4t}}[X]$ is linearized if it satisfies the identities $L(X+Y) \equiv L(X)+L(Y)$ and $L(cX) \equiv cL(X)$ for every $c \in \mathbb{F}_q$. Thus, when $\deg(L) < q^{4t}$, one can equivalently regard linearized polynomials as $\mathbb{F}_q$-linear maps $L : \mathbb{F}_{q^{4t}} \to \mathbb{F}_{q^{4t}}$. Consequently, the set of roots of L over $\mathbb{F}_{q^{4t}}$ forms an $\mathbb{F}_q$-vector space. We call this set the **kernel** of L, denoted $\ker(L) \coloneqq \{\alpha \in \mathbb{F}_{q^{4t}} : L(\alpha) = 0\}$. Additionally, the **image** of L, denoted $\mathrm{im}(L) \coloneqq \{L(\alpha) : \alpha \in \mathbb{F}_{q^{4t}}\}$, also forms an $\mathbb{F}_q$-subspace.

Next, we state the following proposition, which characterizes $\mathbb{F}_q$-valued linearized polynomials.

Proposition 3.2 ($\mathbb{F}_q$-valued linearized polynomials)**.** *All $\mathbb{F}_q$-valued linearized polynomials $L \in \mathbb{F}_{q^{4t}}[X]$ satisfying $\deg(L) < q^{4t}$ are of the form $\mathrm{Tr}(\lambda X)$ for some unique $\lambda \in \mathbb{F}_{q^{4t}}$.*

Proof. For every $\lambda \in \mathbb{F}_{q^{4t}}$, the polynomial $\mathrm{Tr}(\lambda X) \equiv \sum_{i=0}^{4t-1} \lambda^{q^i} X^{q^i}$ is an $\mathbb{F}_q$-valued linearized polynomial of degree less than q^{4t}. Moreover, the map $\lambda \mapsto \mathrm{Tr}(\lambda X)$ is an injective $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^{4t}}$ into the $\mathbb{F}_q$-vector space of $\mathbb{F}_q$-valued linearized polynomials of degree less than q^{4t}. Each polynomial in this space is determined by its values on $\mathbb{F}_{q^{4t}}$, which form an $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^{4t}}$ to $\mathbb{F}_q$, and hence the space has dimension at most $4t = \dim_{\mathbb{F}_q}(\mathbb{F}_{q^{4t}})$. Thus, the map $\lambda \mapsto \mathrm{Tr}(\lambda X)$ is a bijection, which gives both the existence and the uniqueness of λ. □

Next, we introduce quadratic forms, the class of polynomials of primary interest in this work.

Definition 3.3 (Quadratic forms)**.** A **quadratic form** is any $\mathbb{F}_q$-valued polynomial $Q \in \mathbb{F}_{q^{4t}}[X]$ of the form

$$Q(X) \equiv \sum_{0 \leqslant i \leqslant j < 4t} a_{i,j} X^{q^i + q^j} \quad \text{with } a_{i,j} \in \mathbb{F}_{q^{4t}}.$$

To analyze quadratic forms, we consider their polarizations and the resulting linearized polynomial, which is the content of the following lemma.

Lemma 3.4 (The polarization polynomial)**.** *Let $Q \in \mathbb{F}_{q^{4t}}[X]$ be any quadratic form. Then there is a unique linearized polynomial $L_Q \in \mathbb{F}_{q^{4t}}[X]$ with $\deg(L_Q) < q^{4t}$ satisfying*

$$Q(X+\alpha) - Q(X) - Q(\alpha) \equiv \mathrm{Tr}(XL_Q(\alpha)) \quad \text{for all } \alpha \in \mathbb{F}_{q^{4t}}.$$

Moreover, the linearized polynomial L_Q is symmetric.

Proof. Fix $\alpha \in \mathbb{F}_{q^{4t}}$, and define the polynomial

$$R_\alpha(X) \coloneqq Q(X+\alpha) - Q(X) - Q(\alpha).$$

First, observe that $R_\alpha(X)$ is a linearized polynomial with $\deg(R_\alpha) < q^{4t}$. Indeed, expanding things out, we see that

$$\begin{aligned} R_\alpha(X) &\equiv Q(X+\alpha) - Q(X) - Q(\alpha) \\ &\equiv \sum_{0 \leqslant i \leqslant j < 4t} a_{i,j} \left((X+\alpha)^{q^i+q^j} - X^{q^i+q^j} - \alpha^{q^i+q^j} \right) \\ &\equiv \sum_{0 \leqslant i \leqslant j < 4t} a_{i,j} \left(\alpha^{q^j} X^{q^i} + \alpha^{q^i} X^{q^j} \right). \end{aligned}$$

Thus, R_α consists of monomials of the form X^{q^i}, implying that it is linearized. Moreover, by definition, because Q is $\mathbb{F}_q$-valued, so is R_α. Thus, by Proposition 3.2, we can find a unique $\lambda(\alpha)$ satisfying $R_\alpha(X) \equiv \mathrm{Tr}(X\lambda(\alpha))$.

From the expansion above, observe that $R_{\alpha+\beta}(X) \equiv R_\alpha(X) + R_\beta(X)$. Thus, by uniqueness, we see that $\lambda(\alpha+\beta) = \lambda(\alpha) + \lambda(\beta)$ for any $\alpha, \beta \in \mathbb{F}_{q^{4t}}$. Similarly, $R_{c\alpha}(X) \equiv cR_\alpha(X)$ for every $c \in \mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^{4t}}$, so uniqueness gives $\lambda(c\alpha) = c\lambda(\alpha)$. Thus λ is $\mathbb{F}_q$-linear. By interpolation, we can thus find a unique linearized polynomial $L_Q \in \mathbb{F}_{q^{4t}}[X]$ with $\deg(L_Q) < q^{4t}$ satisfying $L_Q(\alpha) = \lambda(\alpha)$ for all $\alpha \in \mathbb{F}_{q^{4t}}$. Moreover, its symmetry follows from the observation that $R_\alpha(\beta) = R_\beta(\alpha)$, which is a direct consequence of the definition of R_α. □

As it turns out, a quadratic form Q and its polarization polynomial L_Q are connected through a distinct relationship, expressed by the following key identity.

Lemma 3.5 (Key identity)**.** *Let Q be a quadratic form with $\deg(Q) < 2q^{4t-1}$, or equivalently, with the coefficient $a_{4t-1,4t-1}$ of the highest possible monomial $X^{2q^{4t-1}}$ equal to zero. Then*

$$Q^q - Q \equiv (X^{q^{4t}} - X)L_Q. \tag{2}$$

Proof. Define the polynomial $G \coloneqq Q^q - Q - (X^{q^{4t}} - X)L_Q$. Because $\deg(Q) < 2q^{4t-1}$, we see that $\deg(G) < 2q^{4t}$. Moreover, from the fact that Q is $\mathbb{F}_q$-valued, we see that $G(\alpha) = 0$ for all $\alpha \in \mathbb{F}_{q^{4t}}$. Thus, we can write $G \equiv (X^{q^{4t}} - X)H$ for $H \in \mathbb{F}_{q^{4t}}[X]$ satisfying $\deg(H) < q^{4t}$. Now, for every $\alpha \in \mathbb{F}_{q^{4t}}$, by Lemma 3.4, observe that

$$\begin{aligned} G(X+\alpha) - G(X) &\equiv (Q(X+\alpha) - Q(X))^q - (Q(X+\alpha) - Q(X)) - (X^{q^{4t}} - X)L_Q(\alpha) \\ &\equiv (\mathrm{Tr}(XL_Q(\alpha)) + Q(\alpha))^q - (\mathrm{Tr}(XL_Q(\alpha)) + Q(\alpha)) - (X^{q^{4t}} - X)L_Q(\alpha) \end{aligned}$$

$$\equiv \sum_{i=1}^{4t} (XL_Q(\alpha))^{q^i} - \sum_{i=0}^{4t-1} (XL_Q(\alpha))^{q^i} - (X^{q^{4t}} - X)L_Q(\alpha)$$
$$\equiv (XL_Q(\alpha))^{q^{4t}} - XL_Q(\alpha) - (X^{q^{4t}} - X)L_Q(\alpha)$$
$$\equiv 0.$$

Since $G \equiv (X^{q^{4t}} - X)H$, we thus see that $H(X + \alpha) \equiv H(X)$ for all $\alpha \in \mathbb{F}_{q^{4t}}$. Combined with the bound $\deg(H) < q^{4t}$, we deduce that H is a constant polynomial. Since every monomial in G has degree at least 2, we see that H has no constant term. Hence $H \equiv 0$, which concludes the proof. □

Next, we will characterize the root structure of Q. To do so, we first distinguish the forms that vanish on the kernel of their polarization polynomial, which is an automatic feature when q is odd, but not when q is even.[2]

Definition 3.6 (Proper quadratic forms)**.** A quadratic form Q is said to be **proper** if $Q|_{\ker(L_Q)} = 0$, that is, $Q(\alpha) = 0$ for every $\alpha \in \ker(L_Q)$.

With this backdrop, under mild assumptions on Q, we can now present a characterization of the root structure of Q, and more generally its level sets.

Corollary 3.7 (Level sets)**.** *Let $Q \in \mathbb{F}_{q^{4t}}[X]$ be a nonzero proper quadratic form with $\deg(Q) < 2q^{4t-1}$. If L_Q splits over $\mathbb{F}_{q^{4t}}$, then L_Q divides Q and $\deg(Q) = (q^{4t} + \deg(L_Q))/q$. In this case, for every $c \in \mathbb{F}_q$,*

$$\left|\{\alpha \in \mathbb{F}_{q^{4t}} : Q(\alpha) = c\}\right| = \begin{cases} \deg(Q) - \deg(L_Q) & \text{if } c = 0, \\ \deg(Q) & \text{if } c \neq 0. \end{cases}$$

Proof. From the degree bound on Q, by Lemma 3.5, Eq. (2) holds. In particular, we see that L_Q must divide $Q^q - Q \equiv \prod_{c \in \mathbb{F}_q} (Q - c)$. Since Q is proper and L_Q splits completely, we thus see that $\gcd(L_Q, Q - c) = 1$ for every nonzero $c \in \mathbb{F}_q$. Thus, we deduce that L_Q divides Q.

Moreover, from Eq. (2), observe that

$$\frac{Q}{L_Q} \prod_{c \in \mathbb{F}_q^\times} (Q - c) \equiv X^{q^{4t}} - X.$$

In particular, the polynomials $Q - c$ for $c \in \mathbb{F}_q \setminus \{0\}$ and Q/L_Q all split completely and have no repeated roots. Furthermore, Q/L_Q shares the same set of roots as Q. Comparing degrees thus gives $q \deg(Q) - \deg(L_Q) = q^{4t}$ and the stated counts. □

Finally, we show that there are super-polynomially many choices of quadratic forms satisfying the needed assumptions.

Lemma 3.8 (A family of proper quadratic forms)**.** *There are at least $q^{t^2}/2$ distinct nonzero proper quadratic forms $Q \in \mathbb{F}_{q^{4t}}[X]$ with $\deg(Q) < 2q^{4t-1}$, for which L_Q has degree q^{3t} and all its roots lie in $\mathbb{F}_{q^{4t}}$, each with multiplicity q^t.*

[2] To see this when q is odd, notice that homogeneity of Q yields $Q(2X) \equiv 4Q(X)$. Plugging in $X = \alpha$ in Lemma 3.4, we see that $Q(\alpha) = \frac{1}{2}\operatorname{Tr}(\alpha L_Q(\alpha))$, which directly implies properness.

Proof. For any linearized polynomial $P \in \mathbb{F}_{q^{4t}}[X]$ with $\deg(P) \leqslant q^t$, let Q be the remainder of $\mathrm{Tr}_{\mathbb{F}_{q^{2t}}/\mathbb{F}_q}(P(X)^{q^{2t}+1})$ modulo $X^{q^{4t}} - X$. First, observe that Q is $\mathbb{F}_q$-valued, as the norm $z \mapsto z^{q^{2t}+1}$ maps $\mathbb{F}_{q^{4t}}$ into $\mathbb{F}_{q^{2t}}$. Moreover, by using $\deg(P) \leqslant q^t$, expanding $\mathrm{Tr}_{\mathbb{F}_{q^{2t}}/\mathbb{F}_q}(P(X)^{q^{2t}+1})$ and reducing modulo $X^{q^{4t}} - X$, one can check that Q consists of monomials of the form $X^{q^i+q^j}$ for $0 \leqslant i < j < 4t$. Consequently, Q is an $\mathbb{F}_q$-valued quadratic form satisfying the degree bound $\deg(Q) \leqslant q^{4t-1}+q^{4t-2} < 2q^{4t-1}$.

Now, for any $\alpha, \beta \in \mathbb{F}_{q^{4t}}$, from the linearity of P, observe that

$$\begin{aligned}
\mathrm{Tr}(\alpha L_Q(\beta)) &= Q(\alpha+\beta) - Q(\alpha) - Q(\beta) \\
&= \mathrm{Tr}_{\mathbb{F}_{q^{2t}}/\mathbb{F}_q}(P(\alpha+\beta)^{q^{2t}+1}) - \mathrm{Tr}_{\mathbb{F}_{q^{2t}}/\mathbb{F}_q}(P(\alpha)^{q^{2t}+1}) - \mathrm{Tr}_{\mathbb{F}_{q^{2t}}/\mathbb{F}_q}(P(\beta)^{q^{2t}+1}) \\
&= \mathrm{Tr}_{\mathbb{F}_{q^{2t}}/\mathbb{F}_q}(P(\alpha)^{q^{2t}}P(\beta)) + \mathrm{Tr}_{\mathbb{F}_{q^{2t}}/\mathbb{F}_q}(P(\beta)^{q^{2t}}P(\alpha)) \\
&= \mathrm{Tr}(P(\alpha)^{q^{2t}}P(\beta)).
\end{aligned}$$

By the bound $\deg(P) \leqslant q^t$, we can write $P(X) \equiv \sum_{i=0}^{t} b_i X^{q^i}$. Thus, by the linearity of trace and the identity $\mathrm{Tr}(\gamma^q) = \mathrm{Tr}(\gamma)$, we see that

$$\begin{aligned}
\mathrm{Tr}(P(\alpha)^{q^{2t}}P(\beta)) &= \mathrm{Tr}\left(\left(\sum_{i=0}^{t} b_i^{q^{2t}} \alpha^{q^{2t+i}}\right)\left(\sum_{j=0}^{t} b_j \beta^{q^j}\right)\right) \\
&= \sum_{i=0}^{t}\sum_{j=0}^{t} \mathrm{Tr}\left(b_i^{q^{2t}} b_j \alpha^{q^{2t+i}} \beta^{q^j}\right) \\
&= \sum_{i=0}^{t}\sum_{j=0}^{t} \mathrm{Tr}\left(b_i^{q^{4t-i}} b_j^{q^{2t-i}} \alpha \beta^{q^{2t+j-i}}\right) \\
&= \mathrm{Tr}\left(\alpha\left(\sum_{i=0}^{t}\sum_{j=0}^{t} b_i^{q^{4t-i}} b_j^{q^{2t-i}} \beta^{q^{2t+j-i}}\right)\right).
\end{aligned}$$

By the uniqueness of L_Q from Lemma 3.4, we see that

$$L_Q(X) \equiv \sum_{i=0}^{t}\sum_{j=0}^{t} b_i^{q^{4t-i}} b_j^{q^{2t-i}} X^{q^{2t+j-i}}.$$

In particular, we see that $\deg(L_Q) \leqslant q^{3t}$ and L_Q is a q^t-th power.

It thus remains to show the properness of Q and the complete splitting of L_Q, which will depend on further properties of P, and to count the resulting quadratic forms. To this end, let $Q_0(z) \coloneqq \mathrm{Tr}_{\mathbb{F}_{q^{2t}}/\mathbb{F}_q}(z^{q^{2t}+1})$ and $\langle u, v\rangle \coloneqq \mathrm{Tr}(u^{q^{2t}}v)$ for $u, v, z \in \mathbb{F}_{q^{4t}}$. Since the reduction modulo $X^{q^{4t}} - X$ does not change values on $\mathbb{F}_{q^{4t}}$, we have $Q(\alpha) = Q_0(P(\alpha))$ and $\mathrm{Tr}(\alpha L_Q(\beta)) = \langle P(\alpha), P(\beta)\rangle$ for every $\alpha, \beta \in \mathbb{F}_{q^{4t}}$. Moreover, from the polarization identity

$$Q_0(u+v) - Q_0(u) - Q_0(v) = \langle u, v\rangle \quad \text{for any } u, v \in \mathbb{F}_{q^{4t}},$$

we see that the $\mathbb{F}_q$-bilinear form $\langle\cdot,\cdot\rangle$ is symmetric. It is also nondegenerate, because $\mathrm{Tr}(\lambda X)$ is a nonzero polynomial of degree less than q^{4t} for every $\lambda \neq 0$. For an $\mathbb{F}_q$-subspace $V \subseteq \mathbb{F}_{q^{4t}}$, we write

$$V^\perp \coloneqq \{\alpha \in \mathbb{F}_{q^{4t}} : \langle \alpha, v\rangle = 0 \text{ for every } v \in V\}.$$

We will show that Q has all the remaining properties in the lemma whenever P satisfies the following two conditions.

(C1) The polynomial P has q^t roots in $\mathbb{F}_{q^{4t}}$. In particular, P fully splits.

(C2) The function Q_0 vanishes on the subspace $U \coloneqq (\mathrm{im}(P))^\perp$.

Indeed, suppose that P satisfies (C1) and (C2), and let us first show the full splitting of L_Q. Let $\beta \in \mathbb{F}_{q^{4t}}$. Observe that $L_Q(\beta) = 0$ exactly when $\mathrm{Tr}(\alpha L_Q(\beta)) = 0$ for every $\alpha \in \mathbb{F}_{q^{4t}}$. As $\mathrm{Tr}(\alpha L_Q(\beta)) = \langle P(\alpha), P(\beta)\rangle$, this happens exactly when $P(\beta)$ is orthogonal to every element of $\mathrm{im}(P)$, that is, when $P(\beta) \in (\mathrm{im}(P))^\perp = U$. Thus, we see that $\ker(L_Q) = P^{-1}(U)$.

Next, we count the elements of this kernel. Since $\langle\cdot,\cdot\rangle$ is nondegenerate, every $\mathbb{F}_q$-subspace $V \subseteq \mathbb{F}_{q^{4t}}$ satisfies $\dim(V^\perp) = 4t - \dim(V)$ and $(V^\perp)^\perp = V$. By (C1), we have $\dim(\ker(P)) = t$, and hence $\dim(\mathrm{im}(P)) = 3t$ and $\dim(U) = 4t - 3t = t$. Moreover, U lies in the image of P. Indeed, for all $u, v \in U$, condition (C2) and the polarization identity of Q_0 give $\langle u, v\rangle = Q_0(u+v) - Q_0(u) - Q_0(v) = 0$. Thus $U \subseteq U^\perp = \mathrm{im}(P)$. Since $U \subseteq \mathrm{im}(P)$, the preimage $P^{-1}(U)$ consists of $|U| = q^t$ cosets of $\ker(P)$, and hence $|\ker(L_Q)| = q^t \cdot q^t = q^{2t}$. Since L_Q is a q^t-th power, this shows the full splitting of L_Q.

We now show that Q is proper, that is, that $Q(\beta) = 0$ for every $\beta \in \ker(L_Q)$. Let $\beta \in \ker(L_Q)$. Since $\ker(L_Q) = P^{-1}(U)$, the element $P(\beta)$ lies in U. By (C2), the function Q_0 vanishes on U, and hence $Q(\beta) = Q_0(P(\beta)) = 0$. Thus Q vanishes on $\ker(L_Q)$.

It thus remains to construct enough polynomials P satisfying (C1) and (C2). Let $\mathcal{U}$ be the set of t-dimensional $\mathbb{F}_q$-subspaces $U \subseteq \mathbb{F}_{q^{4t}}$ on which Q_0 vanishes. The following claim shows that each subspace in $\mathcal{U}$ gives exactly one monic polynomial P satisfying (C1) and (C2).

Claim 1 (From subspaces to polynomials). For every $U \in \mathcal{U}$, there is exactly one monic linearized polynomial $P_U \in \mathbb{F}_{q^{4t}}[X]$ of degree q^t with $\mathrm{im}(P_U) = U^\perp$. Moreover, P_U satisfies (C1) and (C2).

Proof of claim. Fix bases $e_1, \dots, e_{4t}$ of $\mathbb{F}_{q^{4t}}$ and $u_1, \dots, u_t$ of U over $\mathbb{F}_q$. The linearized polynomials $P(X) \equiv \sum_{i=0}^{t} b_i X^{q^i}$ form an $\mathbb{F}_q$-vector space of dimension $4t(t+1)$, and the condition $\mathrm{im}(P) \subseteq U^\perp$ amounts to the $4t^2$ equations $\langle P(e_k), u_l\rangle = 0$ for all $k \in [4t]$ and $l \in [t]$. Since $4t(t+1) > 4t^2$, some nonzero P satisfies this condition. Because $\mathrm{im}(P) \subseteq U^\perp$, the kernel of P has at least $q^{4t}/\left|U^\perp\right| = q^t$ points, and since $\deg(P) \leqslant q^t$, it follows that $\deg(P) = q^t$ and $|\ker(P)| = q^t$, and hence $\mathrm{im}(P) = U^\perp$. For $\lambda \in \mathbb{F}_{q^{4t}}$ defined by the equation $\lambda^{q^t} = b_t^{-1}$, observe that the polynomial $P_U(X) \coloneqq P(\lambda X)$ is monic with the same image and degree, which establishes the existence of such a polynomial.

For uniqueness, let P' be another monic linearized polynomial of degree q^t with $\mathrm{im}(P') = U^\perp$. Because both P' and P_U are monic, $P_U - P'$ is a linearized polynomial of degree less than q^t. Moreover, its image lies in $U^\perp$, which implies that its kernel has size at least $q^{4t}/\left|U^\perp\right| = q^t$, which is impossible for a nonzero polynomial of degree less than q^t. Hence $P' \equiv P_U$. Finally, P_U satisfies (C1) because $|\ker(P_U)| = q^{4t}/\left|U^\perp\right| = q^t$, and it satisfies (C2) because $(\mathrm{im}(P_U))^\perp = (U^\perp)^\perp = U$. ∎

Next, we show that $\mathcal{U}$ is large. Let $N_t \coloneqq \prod_{i=0}^{t-1}(q^t - q^i)$ denote the number of ordered bases of a t-dimensional $\mathbb{F}_q$-vector space.

Claim 2 (Many subspaces). We have $|\mathcal{U}| \geqslant (q^{3t} - q^{2t})^t / N_t$.

Proof of claim. Since each $U \in \mathcal{U}$ has exactly N_t ordered bases, it suffices to show that there are at least $(q^{3t} - q^{2t})^t$ tuples $(u_1, \dots, u_t)$ of linearly independent vectors such that Q_0 vanishes on

their span, which we will show by iteratively choosing each vector. Let $0 \leqslant i < t$, and suppose that Q_0 vanishes on the $\mathbb{F}_q$-span of linearly independent $u_1, \dots, u_i$, which we denote by U_i. Let $\alpha \in \mathbb{F}_{q^{4t}}$. For all $c \in \mathbb{F}_q$ and $u \in U_i$, the polarization identity of Q_0 and its homogeneity show that $Q_0(c\alpha + u) = c^2 Q_0(\alpha) + c\langle \alpha, u \rangle$. Hence Q_0 vanishes on the span of U_i and α when $Q_0(\alpha) = 0$ and $\alpha \in U_i^\perp$. Thus, any choice of $\alpha \in Q_0^{-1}(0) \cap (U_i^\perp \setminus U_i)$ would suffice.

Next, we lower bound $\left|Q_0^{-1}(0) \cap (U_i^\perp \setminus U_i)\right|$. First, observe that the norm map $z \mapsto z^{q^{2t}+1}$ maps $\mathbb{F}_{q^{4t}}^\times$ onto $\mathbb{F}_{q^{2t}}^\times$ and takes each value exactly $q^{2t}+1$ times. Moreover, the trace map $\mathrm{Tr}_{\mathbb{F}_{q^{2t}}/\mathbb{F}_q}$ has $q^{2t-1}-1$ zeros in $\mathbb{F}_{q^{2t}}^\times$. Thus, Q_0 has $1 + (q^{2t}+1)(q^{2t-1}-1) = q^{4t-1} - (q-1)q^{2t-1}$ zeros in $\mathbb{F}_{q^{4t}}$. Now, observe that

$$\left|Q_0^{-1}(0) \cap (U_i^\perp \setminus U_i)\right| \geqslant \left|Q_0^{-1}(0)\right| - \left|Q_0^{-1}(0) \cap (\mathbb{F}_{q^{4t}} \setminus U_i^\perp)\right| - \left|Q_0^{-1}(0) \cap U_i\right|.$$

Since Q_0 vanishes on U_i, we thus see that $\left|Q_0^{-1}(0) \cap U_i\right| = |U_i| = q^i$. As for $\left|Q_0^{-1}(0) \cap (\mathbb{F}_{q^{4t}} \setminus U_i^\perp)\right|$, first observe that $U_i \subseteq U_i^\perp$, because $\langle u, v \rangle = Q_0(u+v) - Q_0(u) - Q_0(v) = 0$ for all $u, v \in U_i$. Hence the subspace $U_i^\perp$ is a union of cosets of U_i, and therefore so is $\mathbb{F}_{q^{4t}} \setminus U_i^\perp$. Now, fix a coset $\alpha + U_i$ with $\alpha \notin U_i^\perp$. For every $u \in U_i$, we have $Q_0(u) = 0$, and so the polarization identity of Q_0 gives $Q_0(\alpha + u) = Q_0(\alpha) + \langle \alpha, u \rangle$. Since $\alpha \notin U_i^\perp$, the map $u \mapsto \langle \alpha, u \rangle$ is a nonzero $\mathbb{F}_q$-linear functional on U_i, and hence it takes every value in $\mathbb{F}_q$ equally often. In particular, $Q_0(\alpha + u) = 0$ for exactly a $1/q$ fraction of the elements $u \in U_i$. Thus $\left|Q_0^{-1}(0) \cap (\alpha + U_i)\right| = q^{i-1}$ for every $\alpha \notin U_i^\perp$. Summing over these cosets, we thus see that $\left|Q_0^{-1}(0) \cap (\mathbb{F}_{q^{4t}} \setminus U_i^\perp)\right| = (q^{4t} - q^{4t-i})/q$. Plugging in the values for all three terms, we therefore find that

$$\left|Q_0^{-1}(0) \cap (U_i^\perp \setminus U_i)\right| \geqslant (q^{4t-1} - (q-1)q^{2t-1}) - \frac{q^{4t} - q^{4t-i}}{q} - q^i = q^{4t-i-1} - (q-1)q^{2t-1} - q^i.$$

Since $i \leqslant t-1$, we have $q^{4t-i-1} \geqslant q^{3t}$ and $q^i \leqslant q^{2t-1}$, and hence this count is at least $q^{3t} - (q-1)q^{2t-1} - q^{2t-1} = q^{3t} - q^{2t}$. Multiplying these bounds over each $i \in \{0, 1, \dots, t-1\}$ gives at least $(q^{3t} - q^{2t})^t$ such tuples, concluding the proof of this claim. ■

Finally, we lower bound the number of resulting quadratic forms from such polynomials P_U by upper bounding the number of subspaces U that can give the same form Q. Indeed, suppose that P_U gives the quadratic form Q. Then, by the identity $\mathrm{Tr}(\alpha L_Q(\beta)) = \langle P_U(\alpha), P_U(\beta) \rangle$ for every $\alpha, \beta \in \mathbb{F}_{q^{4t}}$, we see that $\ker(P_U)$ is a t-dimensional subspace of $\ker(L_Q)$. Moreover, since $P_U \equiv \prod_{\gamma \in \ker(P_U)} (X - \gamma)$, two different polynomials P_U give rise to different kernels. Since P_U determines $U = (\mathrm{im}(P_U))^\perp$, different subspaces U give different polynomials P_U, and hence different kernels $\ker(P_U)$. Since each such kernel has exactly N_t ordered bases, all among the $|\ker(L_Q)|^t = q^{2t^2}$ t-tuples of elements of $\ker(L_Q)$, we therefore see that at most q^{2t^2}/N_t different choices of U give Q as a quadratic form. Thus, by Claim 2, we conclude that there are at least

$$\frac{|\mathcal{U}|\, N_t}{q^{2t^2}} \geqslant \frac{(q^{3t} - q^{2t})^t}{q^{2t^2}} = q^{t^2}(1 - q^{-t})^t \geqslant \frac{q^{t^2}}{2}$$

different such quadratic forms Q. This concludes the proof of the lemma. □

3.1 The low-rate construction

In this subsection, we prove the low-rate part of Theorem 1.1.

Proof of Theorem 1.1 at rate q^{-2}. Set $n \coloneqq q^{4t}$ and $R \coloneqq q^{-2}$. Our received word will be the vector $y \coloneqq (\alpha^{n/q})_{\alpha \in \mathbb{F}_{q^{4t}}}$, i.e., the evaluation of the monomial $X^{n/q}$. For the family of at least $q^{t^2}/2$ quadratic forms Q given by Lemma 3.8, we will show that the corresponding vectors $(f(\alpha))_{\alpha \in \mathbb{F}_{q^{4t}}}$, where

$$f \coloneqq X^{n/q} - \frac{Q}{L_Q^{1/q}},$$

are codewords near y. Indeed, first, by Lemma 3.8, observe that L_Q is a fully split polynomial that is a q^t-th power. Thus, we can write $L_Q^{1/q}$ to denote its unique polynomial q-th root. Moreover, by Corollary 3.7, we see that $L_Q^{1/q}$ divides Q. Thus, f is a well-defined function that is moreover a polynomial in $\mathbb{F}_{q^{4t}}[X]$. To see that $(f(\alpha))_{\alpha \in \mathbb{F}_{q^{4t}}}$ is a bona fide codeword, it remains to show that f has degree less than Rn, which we will now show.

Claim 1 (Degree bound). We have $\deg(f) < n/q^2 = Rn$.

Proof of claim. By Lemma 3.5, observe that we have the following identity:

$$f^q \equiv \left(X^{n/q} - \frac{Q}{L_Q^{1/q}} \right)^q \equiv X - \frac{Q}{L_Q}.$$

By Lemma 3.8 and Corollary 3.7, the quotient Q/L_Q has degree less than n/q. Hence, the right-hand side of the above identity has degree less than n/q. Comparing degrees gives $q \deg(f) < n/q$, which establishes this claim. ■

Next, we show that $(f(\alpha))_{\alpha \in \mathbb{F}_{q^{4t}}}$ agrees with y in at least $(\sqrt{R} - o(1))n$ coordinates.

Claim 2 (Agreements near Johnson). The codeword $(f(\alpha))_{\alpha \in \mathbb{F}_{q^{4t}}}$ agrees with y in at least $n/q - q^{3t} = (\sqrt{R} - n^{-1/4})n$ positions.

Proof of claim. Since y is the evaluation of the monomial $X^{n/q}$, the codeword $(f(\alpha))_{\alpha \in \mathbb{F}_{q^{4t}}}$ agrees with y at exactly the roots in $\mathbb{F}_{q^{4t}}$ of the error polynomial $X^{n/q} - f \equiv Q/L_Q^{1/q}$. By Corollary 3.7, the set of roots of $Q/L_Q^{1/q}$ is the same as that of Q and has size $\deg(Q) - \deg(L_Q)$, which is at least $n/q - q^{3t}$ by the degree bound $\deg(L_Q) \leqslant q^{3t}$. ■

Finally, observe that two quadratic forms Q and Q' in the family from Lemma 3.8 yield the same codeword only when $Q' \equiv cQ$ for some $c \in \mathbb{F}_q^\times$. Indeed, since $\deg(f) < n$, the codeword determines f, and hence both $Q/L_Q^{1/q} \equiv X^{n/q} - f$ and $Q/L_Q \equiv X - f^q$, by the identity in the proof of Claim 1. Their ratio is $(L_Q^{1/q})^{q-1}$, so $L_Q^{1/q}$ is determined up to multiplication by an element of $\mathbb{F}_q^\times$, and consequently so is Q. Thus, we conclude that the full-length Reed–Solomon code over $\mathbb{F}_{q^{4t}}$ of rate R has at least $q^{t^2}/(2(q-1)) = n^{\Omega_q(\log n)}$ codewords at relative distance $1 - \sqrt{R} + O_q(n^{-1/4})$ from y, as Theorem 1.1 asserts. □

3.2 The high-rate construction

In this subsection, we prove the high-rate part of Theorem 1.1.

Proof of Theorem 1.1 at rate $(1-q^{-1})^2$. Set $n \coloneqq q^{4t}$ and $R \coloneqq (1-q^{-1})^2$. Our received word will be the vector $y \coloneqq (\alpha^{(q-1)n/q})_{\alpha \in \mathbb{F}_{q^{4t}}}$, i.e., the evaluation of the monomial $X^{(q-1)n/q}$. For the family of at least $q^{t^2}/2$ quadratic forms Q given by Lemma 3.8, we will show that the corresponding vectors $(f(\alpha))_{\alpha \in \mathbb{F}_{q^{4t}}}$, where

$$f \coloneqq X^{(q-1)n/q} - \frac{\sum_{j=1}^{q-1} Q^j}{(L_Q^{1/q})^{q-1}},$$

are codewords near y. Indeed, as in Section 3.1, $L_Q^{1/q}$ is a polynomial, and the denominator $(L_Q^{1/q})^{q-1}$ divides L_Q, which divides Q by Corollary 3.7. Thus, f is a polynomial in $\mathbb{F}_{q^{4t}}[X]$. To see that $(f(\alpha))_{\alpha \in \mathbb{F}_{q^{4t}}}$ is a bona fide codeword, it remains to show that f has degree less than Rn, which we will now show.

Claim 1 (Degree bound). We have $\deg(f) < (q-1)^2 n/q^2 = Rn$.

Proof of claim. Let $E \coloneqq X^{(q-1)n/q} - f$ be the quotient in the definition of f. Adding and subtracting $(Q/L_Q^{1/q})^{q-1}$, write f as

$$f \equiv \left(X^{(q-1)n/q} - \left(\frac{Q}{L_Q^{1/q}} \right)^{q-1} \right) - \left(E - \left(\frac{Q}{L_Q^{1/q}} \right)^{q-1} \right).$$

We will show that both differences on the right-hand side have degree less than Rn.

For the first difference, by Claim 1 in Section 3.1, we can write $Q/L_Q^{1/q} \equiv X^{n/q} - g$ with $\deg(g) < n/q^2$. Expanding $(X^{n/q} - g)^{q-1}$, every term other than $X^{(q-1)n/q}$ has degree at most $(q-2)n/q + \deg(g) < (q-2)n/q + n/q^2 = Rn$, and hence the first difference has degree less than Rn.

For the second difference, since $\sum_{j=1}^{q-1} Q^j \equiv (Q^q - Q)/(Q-1)$, by Lemma 3.5, observe that we have the following identity:

$$E \equiv \frac{X^{q^{4t}} - X}{Q-1} L_Q^{1/q}. \tag{3}$$

By Corollary 3.7, $Q-1$ has $\deg(Q)$ distinct simple roots in $\mathbb{F}_{q^{4t}}$, implying that $(X^{q^{4t}} - X)/(Q-1)$ is a polynomial. Multiplying the identity by $Q/L_Q^{1/q}$ and subtracting $(Q/L_Q^{1/q})^q \equiv X^{q^{4t}} - X + Q/L_Q$, which also follows from Lemma 3.5, gives

$$\frac{Q}{L_Q^{1/q}} \left(E - \left(\frac{Q}{L_Q^{1/q}} \right)^{q-1} \right) \equiv \frac{(X^{q^{4t}} - X)Q}{Q-1} - \frac{Q^q}{L_Q} \equiv \frac{X^{q^{4t}} - X}{Q-1} - \frac{Q}{L_Q}.$$

By Lemma 3.8 and Corollary 3.7, we have $\deg((X^{q^{4t}} - X)/(Q-1)) = n - \deg(Q) < (q-1)n/q$ and $\deg(Q/L_Q) < n/q$. Hence, the right-hand side of the above identity has degree less than $(q-1)n/q$. Since $Q/L_Q^{1/q} \equiv X^{n/q} - g$ has degree n/q, comparing degrees gives that the second difference has degree less than $(q-2)n/q < Rn$. Both differences thus have degree less than Rn, and therefore $\deg(f) < Rn$. ∎

Next, we show that $(f(\alpha))_{\alpha \in \mathbb{F}_{q^{4t}}}$ agrees with y in at least $(\sqrt{R} - o(1))n$ coordinates.

Claim 2 (Agreements near Johnson). The codeword $(f(\alpha))_{\alpha \in \mathbb{F}_{q^{4t}}}$ agrees with y in at least $(q-1)n/q - q^{3t-1} \geqslant (\sqrt{R} - n^{-1/4})n$ positions.

Proof of claim. Since y is the evaluation of the monomial $X^{(q-1)n/q}$, the codeword $(f(\alpha))_{\alpha\in\mathbb{F}_{q^{4t}}}$ agrees with y at exactly the roots in $\mathbb{F}_{q^{4t}}$ of the error polynomial $X^{(q-1)n/q} - f \equiv E$. By Eq. (3) in the proof of the degree bound, the polynomial $(X^{q^{4t}} - X)/(Q-1)$ divides the error polynomial E. This quotient has roots exactly outside $Q^{-1}(1)$, and the remaining factor $L_Q^{1/q}$ has all its roots in $Q^{-1}(0)$ because Q is proper. Thus, the codeword agrees with y exactly outside the level set $Q^{-1}(1)$. By Corollary 3.7, this level set has size $\deg(Q) = (n + \deg(L_Q))/q$, which is at most $n/q + q^{3t-1}$ by the degree bound $\deg(L_Q) \leqslant q^{3t}$. ■

Finally, observe that two quadratic forms Q and Q' in the family from Lemma 3.8 yield the same codeword only when $Q' \equiv Q$. Indeed, the codeword $(f(\alpha))_{\alpha\in\mathbb{F}_{q^{4t}}}$ disagrees with y exactly on the level set $Q^{-1}(1)$, which by Corollary 3.7 consists of the $\deg(Q)$ roots of $Q-1$. These roots determine $Q-1$ up to a nonzero constant factor, and the constant term $Q(0) - 1 = -1$ fixes that factor. Thus, we conclude that the full-length Reed–Solomon code over $\mathbb{F}_{q^{4t}}$ of rate R has at least $q^{t^2}/2 = n^{\Omega_q(\log n)}$ codewords at relative distance at most $1 - \sqrt{R} + O_q(n^{-1/4})$ from y, as Theorem 1.1 asserts. □

4 Growing lists below capacity over prime fields

4.1 Linear-sized lists from multiplicative subgroups

Throughout this section, we fix a prime p and set the block length to be $n = p$, with our main focus being the full Reed–Solomon code over $\mathbb{F}_p$. For integers d, t with $1 \leqslant d < t$ such that $t \mid p-1$, let $k = t - \lceil t/d \rceil + 1$, $\gamma \in \mathbb{F}_p^\times$ be a generator of $\mathbb{F}_p^\times$, and let $H \coloneqq \{\gamma^{(p-1)/t}, \gamma^{2(p-1)/t}, \ldots, \gamma^{p-1}\}$. Let

$$P_f(X) \coloneqq \prod_{u\in H} (X - f(u)).$$

Lemma 4.1 (Coefficient cancellation on a multiplicative subgroup)**.** *Let $f \in \mathbb{F}_p[X]$ have degree d, where $1 \leqslant d < t$ and $f(0) = 0$. The coefficient of X^{t-j} in P_f vanishes for every integer j with $1 \leqslant j < t/d$. Equivalently,* $\deg(X^t - P_f) \leqslant t - \lceil t/d \rceil$.

Proof. Let $\omega = \gamma^{(p-1)/t}$ and write $f(X) \equiv \sum_{r=1}^{d} a_r X^r$. As a polynomial in the coefficients a_r, the coefficient of X^{t-j} in P_f is homogeneous of degree j and invariant under $a_r \mapsto \omega^r a_r$, since this replaces $f(u)$ by $f(\omega u)$. Give a_r weight r. Every monomial that occurs must have weight divisible by t, but its weight lies between j and dj. There is no such monomial when $1 \leqslant j < t/d$, proving the lemma. □

Lemma 4.2. *Let $p \equiv 2 \pmod 3$ be a prime, and let $H \subseteq \mathbb{F}_p^\times$ be a multiplicative subgroup of size $t \equiv 2 \pmod 3$. Let $f_a(x) = (x+a)^3 - a^3$ for any $a \in \mathbb{F}_p$. For any $a \neq b \in \mathbb{F}_p$, $f_a(H) \neq f_b(H)$.*

Proof. Firstly, we note that since $p \equiv 2 \pmod 3$, the functions f_a are all injective. Now, We do a simple moment calculation to get the following:

$$\begin{aligned}\sum_{h\in H} f_a(h)^{(t+1)/3} &= \sum_{h\in H} h^{t+1} + \sum_{h\in H} (t+1)/3 \cdot 3a \cdot h^t + \sum_{h\in H} p_a(h) \\ &= a(t+1)\cdot|H| + \sum_{h\in H}(h + p_a(h)) \\ &= a(t+1)\cdot|H|\end{aligned}$$

where $p_a(h)$ is a polynomial in h with no constant term and degree less than t. Note that $t+1 < p$ since H is not the full multiplicative group as $p-1 \equiv 2 \not\equiv t \pmod 3$. Thus, we get that $f_a(H)$ and $f_b(H)$ are distinct. □

Lemma 4.3. *Let $f \in \mathbb{F}_p[X]_{\leqslant d}$ be any polynomial such that $|f(H)| = |H|$, $f(0) = 0$, and let $g \coloneqq X^t - P_f(X)$. Then $\deg(g) < k$ and*

$$d_H((\alpha^t)_{\alpha\in\mathbb{F}}, (g(\alpha))_{\alpha\in\mathbb{F}}) = n - t.$$

Proof. Observe that the degree bound follows from Lemma 4.1 and for any $\alpha \in \mathbb{F}_p$, $\alpha^t - g(\alpha) = P_f(\alpha)$. Since $f(H)$ has size at least $|H|$, P_f has at least $|H|$ roots, and these are exactly the evaluation points for which $\alpha^t = g(\alpha)$. □

We now have the necessary ingredients to establish Theorem 1.2.

Theorem 1.2 (Linear-sized lists below capacity over prime fields)**.** *Let $m \geqslant 2$ be an integer such that $m \equiv 2 \pmod 3$. Then, there exist infinitely many primes p such that the full-length Reed–Solomon code over $\mathbb{F}_p$ of length $n = p$ and dimension $\frac{2(p+m-1)}{3m}$ has an explicit received word $y \in \mathbb{F}_p^n$ at Hamming distance exactly $p - \frac{p-1}{m}$ from at least n codewords.*

Proof. Let $p \equiv 2 \pmod 3, p \equiv 1 \pmod m$ with $p \geqslant 3m+2$, let $t = \frac{p-1}{m}$, $d = 3$. Observe that $H = \{\gamma^m, \gamma^{2m}, \ldots, \gamma^{p-1}\}$. Thus,

$$k = t - \frac{t+1}{3} + 1 = \frac{2(t+1)}{3} = \frac{2(p+m-1)}{3m}.$$

Note that $t \equiv 2 \pmod 3$ since $p-1 \equiv 1$ and $m \equiv 2 \pmod 3$.

For any $a \in \mathbb{F}_p$, consider $f_a(X) = (X+a)^3 - a^3$ and observe that all of them are injective on all of $\mathbb{F}_p$ and not just H since $p \equiv 2 \pmod 3$. It is now sufficient to prove that for any $a \neq b$, $f_a(H) \neq f_b(H)$ since then for the received word $y = \{\alpha^t\}_{\alpha\in\mathbb{F}_p}$, and for all $a \in \mathbb{F}_p$, we have that $\Delta(y, \{\alpha^t - P_{f_a}(\alpha)\}_{\alpha\in\mathbb{F}_p}) = n - t$. This follows from Lemma 4.2 and Lemma 4.3.

There are infinitely many primes which are $2 \pmod 3$ and $1 \pmod m$ since 3 and m are co-prime due to Dirichlet's theorem. □

4.2 Polynomially growing lists via amplification

Let $\mathrm{RS}((\alpha_1, \ldots, \alpha_n), k)$ be a Reed–Solomon code such that there is a polynomial $y : \mathbb{F}_q \to \mathbb{F}_q$ of degree $D \geqslant k-1$, and message polynomials $g_1, \ldots, g_L$ such that

$$d_H((y(\alpha_1), \ldots, y(\alpha_n)), (g_i(\alpha_1), \ldots, g_i(\alpha_n))) \leqslant n - a$$

then for any $S \subseteq [L]$ of size ℓ, let

$$G_S = y^\ell - \prod_{s\in S}(y - g_s)$$

and let $Y = y^\ell$.

Observe that $\deg G_S \leqslant (\ell-1)D + k - 1$, and they all agree with the received word Y in $|\{i : \exists s \in S \mid g_s(\alpha_i) = y(\alpha_i)\}|$ which we can hope is as big as ℓa.

In particular, if the sets $Z_s = \{i \mid g_s(\alpha_i) = y(\alpha_i)\}$ were disjoint, we get that $\mathrm{RS}((\alpha_1, \ldots, \alpha_n), D(\ell-1)+k)$ has a received word, and $\geqslant \binom{L}{\ell}$ codewords at distance $\leqslant n - a\ell$.

For a different construction, we may require a more fine-grained analysis to show that these $\binom{L}{\ell}$ codewords are distinct and many of the sets are big.

Theorem 1.4 (Arbitrary polynomial-lists)**.** *For any integer $\ell \geqslant 2$, there are infinitely many primes p such that the full-length Reed–Solomon code over $\mathbb{F}_p$ of length $n = p$ and rate $R = \Omega(1/\ell)$ is not $(1 - R - \Omega(1/\ell^2), \binom{n}{\ell}/2)$-list-decodable.*

Proof. We use the above amplification idea on the construction in Theorem 1.2.

For simplicity let $\varepsilon = 1/\ell$. Let $m = 12\ell^2 + 2$, and p be any sufficiently large prime such that $p \equiv 1 \pmod m$ and $p \equiv 2 \pmod 3$. Now, $t = (p-1)/m$ and $k \leqslant \left\lceil \frac{2(p+1)}{3m} \right\rceil$.

Then, we know by Theorem 1.2 that if we let $H = \{\gamma^m, \gamma^{2m}, \ldots, \gamma^{p-1}\}$, let $f_a(x) = (x+a)^3 - a^3$, then $d_H((\alpha^t)_{\alpha\in\mathbb{F}_p}, (\alpha^t - P_{f_a}(\alpha))_{\alpha\in\mathbb{F}_p}) = n - t$ and all $f_a(H)$ are distinct.

For $S \subseteq \mathbb{F}_p$ of size ℓ, let $P_S = \prod_{s\in S} P_{f_s}$, and let $Y = \{\alpha^{\ell t}\}_{\alpha\in\mathbb{F}_p}$. Let $G_S = X^{\ell t} - P_S(X)$. Let $K = t(\ell-1) + k = O(p/\ell)$. Thus, the full Reed–Solomon code of rate $R = \frac{K}{p} = \Theta(1/\ell) = \Theta(\varepsilon)$ contains the messages given by $\{G_S(\alpha)\}_{\alpha\in\mathbb{F}}$.

We also have that

$$d_h((\alpha^{\ell t})_{\alpha\in\mathbb{F}_p}, (\alpha^{\ell t} - P_S(\alpha))_{\alpha\in\mathbb{F}_p}) = n - \left|\bigcup_{s\in S} f_s(H)\right|.$$

Thus, it suffices to prove that for many $S \subseteq \mathbb{F}_p$ of size ℓ, the resulting polynomials G_S are distinct and $\left|\bigcup_{s\in S} f_s(H)\right| > K + \Omega(k)$. We prove the second part first. Observe that

$$\begin{aligned}
\mathbb{E}_{S\subseteq\mathbb{F}_p,|S|=\ell} \sum_{(s_1,s_2)\in\binom{S}{2}} |f_{s_1}(H) \cap f_{s_2}(H)| &\leqslant \binom{\ell}{2} \mathbb{E}_{s_1\in\mathbb{F}_p, s_2\in\mathbb{F}_p\setminus\{s_1\}} |\{(u,v) \in H\times H \mid f_{s_1}(u) = f_{s_2}(v)\}| \\
&\leqslant \binom{\ell}{2} \frac{\sum_{s_1\in\mathbb{F}_p, u,v\in H} \mathbb{E}_{s_2\in\mathbb{F}_p\setminus\{s_1\}} \mathbf{1}(f_{s_1}(u) = f_{s_2}(v))}{p} \\
&\leqslant \binom{\ell}{2} \cdot |H|^2 \cdot \frac{2}{p-1} \quad \leqslant \frac{\ell^2 t^2}{p} \quad \leqslant \frac{\ell t}{12\ell} \\
&\leqslant \frac{t}{12}
\end{aligned}$$

The key observation is that for any fixed s_1, u, v, there are at most 2 choices of s_2 such that $(u+s_1)^3 - s_1^3 = (v+s_2)^3 - s_2^3$ since this is a quadratic equation in s_2.

Thus, $|\{S \mid \sum_{(s_1,s_2)\in\binom{S}{2}} |f_{s_1}(H) \cap f_{s_2}(H)| \leqslant t/6\}| \geqslant \binom{p}{\ell} \cdot \frac{1}{2}$. In particular, this means that for at least $\frac{\binom{n}{\ell}}{2}$ different choices of S, we have that $\left|\bigcup_{s\in S} f_s(H)\right| \geqslant t\ell - \sum_{(s_1,s_2)\in\binom{S}{2}} |f_{s_1}(H) \cap f_{s_2}(H)| \geqslant t\ell - \frac{t}{6} = K + \Omega(k)$.

Now, it suffices to prove that all these polynomials P_S are distinct. Thus, we prove the following stronger lemma which is sufficient.

Lemma 4.4. *Fix $\ell \geqslant 1, m \geqslant 2$ with $m \equiv 2 \pmod 3$. For every sufficiently large prime p with $p \equiv 1 \pmod m$ and $p \equiv 2 \pmod 3$, for any $S_1 \neq S_2 \subseteq \mathbb{F}_p$, with $|S_1| = |S_2| = \ell$,*

$$\prod_{s\in S_1} P_{f_s}(X) \neq \prod_{s\in S_2} P_{f_s}(X)$$

Proof. As a variant on the computation for the linear lists where we showed that $\sum_{h\in H} f_a(h)^{(t+1)/3}$ uniquely recovers a, we repeat the same argument with higher moments.

Let

$$m_{S,r} = \sum_{s\in S}\sum_{h\in H} f_s(h)^{(t+1)/3+r}$$

Observe that if $P_{S_1} = P_{S_2}$ then $m_{S_1,r} = m_{S_2,r}$ for all $r \in \mathbb{N}$. Additionally, from Theorem 1.2, we have that $m_{S,0} = (t+1)|H|\sum_{s\in S} s$.

We now only use $r \in \{0, 1, \ldots, 2\ell\}$. Similarly,

$$\begin{aligned}\sum_{h\in H} f_a(h)^{(t+1)/3+r} &= \sum_{j\neq t} C_{r,j}(a)\sum_{h\in H} h^j + \sum_{h\in H} C_{r,t}(a)h^t \\ &= C_{r,t}(a)|H|\end{aligned}$$

Here we use that every exponent satisfies $j \leqslant t+1+3r < 2t$, since we will assume that p is sufficiently large such that $t > 6\ell + 1$.

Now, it suffices to prove that for any fixed ℓ, m, r, for large enough choices of $\mathbb{F}_p$, $C_{r,t}(a)$ is exactly a degree $3r+1$ function of a. Specifically, $f_a(X)^{(t+1)/3+r} = (X^3 + 3aX^2 + 3a^2X)^{(t+1)/3+r}$. Observe that this is a homogeneous bivariate polynomial in variables a, X of degree $3(r+(t+1)/3) = t+3r+1$. Thus, the X^t variable will have a corresponding a^{3r+1} term. Our goal is now to simply compute what this term is. Observe that $C_{r,t}(a) = C_{r,t}(1)a^{3r+1}$ due to the homogeneity. Thus, we only focus on proving $C_{r,t}(1) \neq 0 \pmod p$ for sufficiently large primes p.

Let $d_r = (t+1)/3 + r$ and $e_r = 3r+1$. Now, observe that if we use b terms of the form $3a^2X$, to get the term of degree e_r in a, we must use $e_r - 2b$ terms of the form $3aX^2$ and the remaining of the form X^3. Thus,

$$\begin{aligned}C_{r,t}(1) &= \left(\sum_{b=0}^{\lfloor e_r/2\rfloor} 3^{e_r-b}\binom{d_r}{b, e_r-2b, d+b-e_r}\right) \\ &= \left(\sum_{b=0}^{\lfloor e_r/2\rfloor} \frac{1}{b!(e_r-2b)!}\prod_{i=0}^{e_r-b-1}(3d_r - 3i)\right) \\ &= \left(\sum_{b=0}^{\lfloor e_r/2\rfloor} \frac{1}{b!(e_r-2b)!}\prod_{i=0}^{e_r-b-1}(t+e_r-3i)\right),\end{aligned}$$

Observe that we are only interested in $C_{r,t} \pmod p$ and $t \equiv -1/m \pmod p$. Hence,

$$m^{e_r}\cdot e_r!\cdot C_{r,t}(1) = \left(\sum_{b=0}^{\lfloor e_r/2\rfloor} \frac{e_r!}{b!(e_r-2b)!}\prod_{i=0}^{e_r-b-1}\left(\frac{-1}{m}+e_r-3i\right)\cdot m^{e_r}\right) \pmod p$$

Thus,

$$M_r = \sum_{b=0}^{\lfloor e_r/2\rfloor} \frac{e_r!}{b!(e_r-2b)!}\prod_{i=0}^{e_r-b-1}\left(\frac{-1}{m}+e_r-3i\right)\cdot m^{e_r} \equiv (-1)^{e_r} \pmod m.$$

Hence, picking any prime $p > |M_r|, (6\ell+1)m+1$ for all $r \in \{0, 1, \ldots, 2\ell\}$, we get that $M_r \pmod p \neq 0$ and hence $C_{r,t}(1) \neq 0 \pmod p$. Consequently, given $\prod_{s\in S} P_{f_s}(X)$, we can recover $\sum_{s\in S} s^{3r+1}$ for $r \in \{0, 1, \ldots, 2\ell\}$.

We need to simply show that given these moments, we can recover the set S. Let S_1, S_2 be any two such sets for which all above moments are equal, and T be their symmetric difference, i.e., $T = (S_1 \cup S_2) \setminus (S_1 \cap S_2)$. Now, for $x \in T$, let $c_x = (-1)^b x$ if $x \in S_b$. Since all the above moments are the same, we have that

$$\sum_{x \in T} c_x (x^3)^r = 0$$

for all $r \in \{0, 1, \ldots, 2\ell\}$. Thus, either all $c_x = 0 \; \forall x \in T \implies T \subseteq \{0\}$, or the resulting Vandermonde matrix of $\{(x^3)^r\}_{r \in \{0,\ldots,|T|-1\}, t \in T}$ is singular. But, since $p \equiv 2 \pmod 3$, the cubing $x \mapsto x^3$ map is injective and the resulting Vandermonde matrix is invertible. Thus, $T \subseteq \{0\}$ but the size of T is $2\ell - 2|S_1 \cap S_2|$ which is even. Hence, for any distinct S_1, S_2, there are some unequal moments as desired and we get the desired result. □

Now, we can simply take the messages G_S for the $\geqslant \binom{n}{\ell}/2$ sets S for which $\sum_{s_1, s_2 \in \binom{S}{2}} |f_{s_1}(H) \cap f_{s_2}(H)| \leqslant t/6$ and the result follows. □

Acknowledgments

We thank Zihan Zhang for helpful discussions. We also thank the Simons Institute for the Theory of Computing for hosting us during the Fall 2026 program on *Pseudorandomness & High-Dimensional Expansion*.

AI methodology

Initial versions of our key statements were established by GPT-6 Astra Pro over various conversations. Our main contributions are in abstracting and simplifying the proof ideas, and in the exposition. In particular, the proofs presented in the paper are substantially simpler and clearer in our opinion.

Immediately following the breakthrough result of [BCP+26], we wondered if their results can be improved, specifically whether beyond Johnson-radius list-decoding is possible for all Reed–Solomon codes, and whether list sizes can be improved to a fixed constant for large prime fields.

In conversations with GPT-6 Astra Pro, we started exploring both ideas. Soon after, the AI gave us an early construction of $n^{\Omega(\log n)}$ list-size just beyond Johnson for small characteristic fields using a result of [Sch20]. We closely understood this construction and then worked extensively to simplify it over the next few weeks. In this paper, we present a completely elementary proof of the lower bound.

For the prime field case, GPT-6 similarly arrived at a non-elementary construction of low-degree functions after finding Lemma 4.1 to prove the requisite lower bounds. After understanding the approach, we first simplified the constructions by choosing the "moving" functions f instead as *random* low-degree polynomials. Then, with the help of AI, we further refined it to the simple choice of $(x + a)^3 - a^3$ presented in the paper (at the expense that the result as written now only works for infinitely many as opposed to all primes).

The amplification argument of Section 4.2 was then discovered in discussions with GPT-6 where we looked for generic ways to bootstrap the lower bounds.

We take full responsibility for the correctness and quality of exposition of the results presented in this paper.

References

[AGG+25] Omar Alrabiah, Zeyu Guo, Venkatesan Guruswami, Ray Li, and Zihan Zhang. Random Reed–Solomon codes achieve list-decoding capacity with linear-sized alphabets. *Advances in Combinatorics*, 2025, 2025. Article 8. 2

[AGG26] Omar Alrabiah, Rohan Goyal, and Venkatesan Guruswami. Explicit reed-solomon subspace designs: Optimal list and line decoding, 2026. *arXiv preprint arXiv:2610.36215*. 3

[AGL24] Omar Alrabiah, Venkatesan Guruswami, and Ray 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 (STOC)*, pages 1458–1469, 2024. 2

[BCP+26] Joshua Brakensiek, Yeyuan Chen, Aaron (Louie) Putterman, Zihan Zhang, and Kai Zhe Zheng. Algorithmic list decoding of Reed-Solomon codes up to capacity. Technical Report TR26-164, Electronic Colloquium on Computational Complexity (ECCC), 2026. Revision 1, September 2026 (the original version was titled "... up to capacity in the low-rate regime"). 2, 3, 20

[Ber68] Elwyn R. Berlekamp. *Algebraic Coding Theory*. McGraw-Hill, New York, 1968. 1

[BGM23] Joshua Brakensiek, Sivakanth Gopi, and Visu Makam. Generic Reed-Solomon codes achieve list-decoding capacity. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC)*, pages 1488–1501, 2023. 2

[BSKR10] Eli Ben-Sasson, Swastik Kopparty, and Jaikumar Radhakrishnan. Subspace polynomials and limits to list decoding of Reed-Solomon codes. *IEEE Transactions on Information Theory*, 56(1):113–120, 2010. Preliminary version in FOCS 2006. 2, 5, 6

[CGH+26] Dan Carmon, Lior Goldberg, Ulrich Haböck, Leonardo Lerer, Ilya Lesokhin, Shahar Papini, and Shahar Samocha. S-two whitepaper. Cryptology ePrint Archive, Paper 2026/532, 2026. 3

[CW07] Qi Cheng and Daqing Wan. On the list and bounded distance decodability of Reed-Solomon codes. *SIAM Journal on Computing*, 37(1):195–209, 2007. Preliminary version in FOCS 2004. 2

[DKTZ26] Quang Dao, Scott Duke Kominers, Justin Thaler, and Kai Zhe Zheng. Counterexamples to beyond-Johnson proximity gaps over binary fields. Technical Report TR26-237, Electronic Colloquium on Computational Complexity (ECCC), 2026. 4

[Eli57] Peter Elias. List decoding for noisy channels. Technical Report 335, Research Laboratory of Electronics, Massachusetts Institute of Technology, 1957. 1

[Eli91] Peter Elias. Error-correcting codes for list decoding. *IEEE Transactions on Information Theory*, 37(1):5–12, 1991. 1

[FKS22] Asaf Ferber, Matthew Kwan, and Lisa Sauermann. List-decodability with large radius for Reed-Solomon codes. *IEEE Transactions on Information Theory*, 68(6):3823–3828, 2022. Preliminary version in FOCS 2021. 2

[GLS+21] Zeyu Guo, Ray Li, Chong Shangguan, Itzhak Tamo, and Mary 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*, pages 708–719, 2021. 2

[GR06] Venkatesan Guruswami and Atri Rudra. Limits to list decoding Reed-Solomon codes. *IEEE Transactions on Information Theory*, 52(8):3642–3649, 2006. Preliminary version in STOC 2005. 2

[GRS00] Oded Goldreich, Ronitt Rubinfeld, and Madhu Sudan. Learning polynomials with queries: The highly noisy case. *SIAM Journal on Discrete Mathematics*, 13(4):535–570, 2000. 1

[GS99] Venkatesan Guruswami and Madhu Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Transactions on Information Theory*, 45(6):1757–1767, 1999. Preliminary version in FOCS 1998. 1

[GS01] Venkatesan Guruswami and Madhu Sudan. Extensions to the Johnson bound. Manuscript, February 2001. 1

[GS03] Venkatesan Guruswami and Igor Shparlinski. Unconditional proof of tightness of Johnson bound. In *Proceedings of the 14th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 754–755, 2003. 1

[GST23] Eitan Goldberg, Chong Shangguan, and Itzhak 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. 2

[Gur02] Venkatesan Guruswami. Limits to list decodability of linear codes. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, pages 802–811, 2002. 1

[GV05] Venkatesan Guruswami and Alexander Vardy. Maximum-likelihood decoding of Reed–Solomon codes is NP-hard. *IEEE Transactions on Information Theory*, 51(7):2249–2256, 2005. 2

[GZ23] Zeyu Guo and Zihan 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 (FOCS)*, pages 164–176, 2023. 2

[HKS26] Prahladh Harsha, Mrinal Kumar, and Ramprasad Saptharishi. Reed-Solomon codes at capacity: Algorithmic list-decoding and proximity gaps. arXiv:2610.08610, 2026. 3

[Jer26] Fernando Granha Jeronimo. Algorithmic list decoding at capacity and optimal proximity gaps for Reed-Solomon codes. Technical Report TR26-169, Electronic Colloquium on Computational Complexity (ECCC), 2026. 3

[JH01] Jørn Justesen and Tom Høholdt. Bounds on list decoding of MDS codes. *IEEE Transactions on Information Theory*, 47(4):1604–1609, 2001. 2, 5

[Joh62] Selmer M. Johnson. A new upper bound for error-correcting codes. *IRE Transactions on Information Theory*, 8(3):203–207, 1962. 1

[KKH26] Dmitry Krachun, Stepan Kazanin, and Ulrich Haböck. Failure of proximity gaps close to capacity. Cryptology ePrint Archive, Paper 2026/782, 2026. 3

[Mas69] James L. Massey. Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, 15(1):122–127, 1969. 1

[Pet60] W. Wesley Peterson. Encoding and error-correction procedures for the Bose-Chaudhuri codes. *IRE Transactions on Information Theory*, 6(4):459–470, 1960. 1

[RS60] Irving S. Reed and Gustave Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960. 1

[RW14] Atri Rudra and Mary 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 (STOC)*, pages 764–773, 2014. 2

[Sch20] Kai-Uwe Schmidt. Quadratic and symmetric bilinear forms over finite fields and their association schemes. *Algebraic Combinatorics*, 3(1):161–189, 2020. 20

[Sin64] Richard C. Singleton. Maximum distance q-nary codes. *IEEE Transactions on Information Theory*, 10(2):116–118, 1964. 1

[ST23] Chong Shangguan and Itzhak Tamo. Generalized Singleton bound and list-decoding Reed-Solomon codes beyond the Johnson radius. *SIAM Journal on Computing*, 52(3):684–717, 2023. Preliminary version, titled "Combinatorial list-decoding of Reed-Solomon codes beyond the Johnson radius," in STOC 2020. 2

[Sud97] Madhu Sudan. Decoding of Reed Solomon codes beyond the error-correction bound. *Journal of Complexity*, 13(1):180–193, 1997. 1

[WB86] Lloyd R. Welch and Elwyn R. Berlekamp. Error correction for algebraic block codes. U.S. Patent 4,633,470, December 1986. 1

[Woz58] John M. Wozencraft. List decoding. *Quarterly Progress Report, Research Laboratory of Electronics, Massachusetts Institute of Technology*, 48:90–95, 1958. 1

[Zhu26] Minshen Zhu. Superpolynomial lists for Reed–Solomon codes over binary extension fields. arXiv:2610.15815, 2026. 4

[ZP81] Victor V. Zyablov and Mark S. Pinsker. List concatenated decoding. *Problems of Information Transmission*, 17(4):236–240, 1981. 1

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il