

Linear list size bounds for Reed-Solomon beyond the Johnson radius

Ariel Gabizon

October 6, 2026

Abstract

Based on techniques discovered in the better.codes autoresearch project, we show that Reed-Solomon codes of rate ρ and block length n over a field of sufficiently large characteristic, have $C \cdot n$ list size bound when requiring fractional agreement α with a received word; where C, α are constants depending only on ρ and $\alpha < \sqrt{\rho}$. This complements the recent breakthrough results [BCP⁺26, Jer26] achieving n^c list size bounds with agreement $\rho + \epsilon$ for any constant $\epsilon > 0$ with an unspecified constant exponent c .

1 Introduction

The Johnson bound [Joh62] tells us that for any Reed-Solomon code of block length n and rate ρ the number of codewords having fractional agreement $\sqrt{\rho} + \epsilon$ with any vector $\mathbf{y} \in \mathbb{F}^n$ is at most a constant $C_{\rho, \epsilon}$. What happens at and below agreement $\sqrt{\rho}$ for RS codes has long remained unsolved. The recent better.codes¹ autoresearch project has seemed to “break through Johnson”, albeit for a specific RS code of block length $n = 2^{18}$. [BCP⁺26] extrapolated and built on ideas from better.codes, and managed to show for general RS codes over prime fields, list sizes stay polynomial in $q = |\mathbb{F}|$ while only requiring agreement $\rho + \epsilon$ for any constant $\epsilon > 0$ (and moreover, the list of close codewords can be efficiently found). Subsequently, Jeronimo [Jer26] showed that for the same fractional agreement list sizes can be bound polynomially in the block length n - which is crucial for applications of RS codes in zk-SNARKs where $q \gg n$. However the exponent in the polynomial is unspecified in [Jer26] and seems large. In this note, we have two goals.

- Illustrate the ideas from better.codes in a simpler way than [BCP⁺26, Jer26], by only going a “bit beyond Johnson”. Technically, this corresponds to only needing to look at the first derivative of a polynomial, as opposed to a large enough number of derivatives as in [BCP⁺26, Jer26].

¹See `better.codes` online.

- Obtain a *linear* in n bound on the number of close codewords rather than an unspecified polynomial number as in [Jer26].

We introduce some notation to present our main result.

Notation and terminology for the main result: $\mathbb{F}$ denotes a finite field of size q . k, n denote integers with $0 < k < n < q$. We denote vectors in $\mathbb{F}^n$ in bold letters, and their coordinates in non-bold letters. For example for $\mathbf{x} \in \mathbb{F}^n$ we denote $\mathbf{x} = (x_1, \dots, x_n)$. Fix any $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$. Fix any $0 < \alpha < 1$ and let $a := \lceil \alpha n \rceil$. We denote by $agree_\alpha(\text{RS}_k, \mathbf{x}, \mathbf{y})$ the set of polynomials $f \in \mathbb{F}_{<k}[X]$ such that $f(x_i) = y_i$ for at least a values $i \in [n]$.

Our main theorem is

Theorem 1. *Fix any $0 < \rho < 1$. Then there is a constant $0 < \alpha < \sqrt{\rho}$ and positive integers d, C depending only on ρ such that the following holds. Fix any positive integers $k \leq n$ with $k/n \leq \rho$. Let $p > \max\{d, k\}$ be prime and $q = p^t$ be a power of p larger than n . Let $\mathbb{F}$ be the field of size q . Then for any $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$, we have*

$$|agree_\alpha(\text{RS}_k, \mathbf{x}, \mathbf{y})| \leq Cn.$$

1.1 Overview of Techniques:

To understand the result, it is instructive to go all the way back to Sudan's original paper on list-decoding of Reed-Solomon [Sud97].

The Sudan list decoding algorithm: The basic idea of [Sud97] is to construct a non-zero bi-variate polynomial $Q(X, Y)$ such that for any $f \in \mathbb{F}_{<k}[X]$ close to our received word, we have $Q(X, f(X)) \equiv 0$. In other words, f is a root of Q as a univariate polynomial in Y over $\mathbb{F}(X)$. The main question, which all subsequent optimizations deals with, is *how close* f has to be to be a root. Let's sketch the calculation of that. Sudan allows in Q all monomials $X^i Y^j$ such that the $(1, k-1)$ -*weighted degree* - namely $i + (k-1) \cdot j$, is smaller than a prespecified bound D . One can show there are at least $D^2/2k$ such monomials. We put n constraints on Q 's coefficients - that $Q(x_i, y_i) = 0$ for each $i \in [n]$. An f agreeing with $\mathbf{y}$ on D locations has $Q(x_i, f(x_i)) = 0$ for D values $i \in [n]$. This implies in turn $Q(X, f(X)) = 0$ (identically as a polynomial). Thus, there can be at most $\deg_Y(Q) \leq D/(k-1)$ such f . The essential thing is that we can indeed find a *non-zero* Q satisfying the constraints. For this we need the number of coefficients to be at least the number of constraints. Namely,

$$D^2/2k \geq n,$$

translating to $D \geq \sqrt{2kn}$. Dividing by n we get

$$\alpha := (D/n) \geq \sqrt{2\rho}.$$

Namely, fractional agreement $\alpha = \sqrt{2\rho}$ with $\mathbf{y}$ is sufficient for f to be a root of Q .

Guruswami-Sudan introduce multiplicities: [GS99] essentially pushed the required fractional agreement down to $\sqrt{\rho}$. They did this by looking at roots of *high multiplicity*. Given (x, y) , look at a shifted version of Q :

$$Q'(X, Y) := Q(x + X, y + Y).$$

$Q(x, y) = 0$ is equivalent to $Q'(x, y)$ having a zero constant coefficient. Motivated by this, we can constrain in addition to $Q(x, y) = 0$, that all monomials $X^i Y^j$ of Q' total degree $i + j < m$ vanish. This is useful for the following reason: $f(x) = y$ now implies that $Q_f(X) := Q(X, f(X))$ has a zero of multiplicity m at x as a univariate; namely that $(X - x)^m$ divides g . This reduces by a factor of m the amount of agreement points of f with $\mathbf{y}$ needed, to obtain $g \equiv 0$.

On the other hand, we have increased the number of constraints: each (x_i, y_i) will have $\binom{m}{2}$ constraints corresponding to the monomials $X^i Y^j$ of Q' that need to vanish. One can show that as m grows the number of constraints grow slow enough, and consequently [GS99] can list decode from agreement close to $\sqrt{\rho}$ rather than [Sud97]’s $\sqrt{2\rho}$. Roughly speaking - this is because $\binom{m}{2} \sim m^2/2$ rather than being close to m^2 . This two in the denominator precisely ends up cancelling the factor of two in Sudan’s required agreement.

Multiplicity codes: Kopparty [Kop15] and Guruswami and Wang [GW11] noticed that we can list-decode from smaller agreement if the codeword additionally contains *derivative evaluations*. Namely, for some parameter d , a codeword symbol will contain in addition to $f(x_i)$, the values $f^{(1)}(x_i), \dots, f^{(d)}(x_i)$ - where $f^{(j)}$ denotes the j ’th derivative of f . The basic reason is that this gives us more data from which to interpolate our Q . Namely, we can work with a $d + 1$ -variate Q that we require to vanish at a point (x_i, y_i) where now $y_i \in \mathbb{F}^{d+1}$ is the i ’th symbol of the received word, containing the purported derivative evaluations at x_i .

The novelty of better.codes - “hidden derivatives”: The main novelty² in better.codes is observing that also for the RS code, it pays off to construct Q vanishing at a “jet curve” $(X, f(X), f'(X))$. This can seem surprising at first - the received word doesn’t contain derivative values, so how can we construct Q ? Let us illustrate this. Suppose f agrees with received word $\mathbf{y}$ at index i . We’d like to enforce $Q_f(x_i) = Q(x_i, f(x_i), f'(x_i)) = 0$ assuming $f(x_i) = y_i$. Since we don’t know $f'(x_i)$, our only way to do this is to constrain that $Q(x_i, y_i, Z) = 0$ identically as a polynomial in Z . This seems quite expensive in terms of the number of constraints. Specifically, if we allow degree s in Z , it translates to $s + 1$ linear constraints on the coefficients of Q . The point, however, is that when we enforce $Q_f(x_i)$ vanishing at higher multiplicities, because of the way derivatives of Q_f and Q interact via the chain rule we can save constraints. For example, use the chain rule to get

$$Q'_f(x_i) = Q_X(x_i, y_i, f'(x_i)) + Q_Y(x_i, y_i, f'(x_i))f'(x_i) + Q_Z(x_i, y_i, f'(x_i))f''(x_i).$$

²It seems the hidden derivatives approach was initiated by Bartosz Naskręcki: <https://github.com/proximity-prize/proximity-prize/pull/122>.

We want to ensure $Q'_f(x_i) = 0$. Since, again, we have no information about the values $f'(x_i), f''(x_i)$ we need to constrain the polynomial

$$F(Z, R) := Q_X(x_i, y_i, Z) + Q_Y(x_i, y_i, Z)Z + Q_Z(x_i, y_i, Z)R$$

to be identically zero. When $\deg_Z(Q) \leq s$, F has $2(s+1)$ coefficients that are linear combinations of Q 's coefficients. However, we get for free $Q_Z(x_i, y_i, Z) = 0$ as it is the derivative of $Q(x_i, y_i, Z)$ which we already constrained to be zero - saving us s constraints.

2 Preliminaries

Notation: As in the introduction, $\mathbb{F}$ denotes a finite field of size q and characteristic p . Denote by L the algebraic closure of $\mathbb{F}(X)$. For $Q(Y, Z) \in L[Y, Z]$ we denote by $\text{zeros}(Q)$ the set of all $(x, y) \in L^2$ with $Q(x, y) = 0$.

When discussing polynomials we at times omit the variables for notational clarity; e.g. f instead of $f(X)$ for $f \in \mathbb{F}[X]$. For $(s, t) \in K^2$, we use the notation

Bezout's theorem: We use the following corollary of Bezout. (Recall our L is algebraically closed.)

Theorem 2. *Let $T(Y, Z) \in L[Y, Z]$ be an irreducible polynomial. Let $H \in L[Y, Z]$ be any non-zero polynomial such that T doesn't divide H . Then*

$$|\text{zeros}(T) \cap \text{zeros}(H)| \leq \deg(T)\deg(H).$$

3 Main argument structure

Given $f \in \mathbb{F}_{<k}[X]$ and $Q \in \mathbb{F}[X, Y, Z]$ we define the *jet polynomial of f with respect to Q* as

$$Q_f(X) := Q(X, f(X), f'(X)).$$

Now, there are two components needed. The first is constructing a low-degree Q such that Q_f is the zero polynomial whenever f has large agreement with $\mathbf{y}$.

Theorem 3. *Fix $0 < \rho < 1$. There is a constant $0 < \rho < \alpha < \sqrt{\rho}$, and positive integer d both depending only on ρ such that the following holds. Fix any $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$. There exists a non-zero polynomial $Q \in \mathbb{F}[X, Y, Z]$ with $\deg_{Y,Z}(Q) < d$ such that any $f \in \text{agree}_\alpha(\text{RS}_k, \mathbf{x}, \mathbf{y})$, we have $Q_f(X) = 0$.*

The second component is showing any such Q cannot have many “roots” f that have large agreement with $\mathbf{y}$.

Theorem 4. *Fix any constants α, ρ with $0 < \rho < \alpha < \sqrt{\rho} < 1$, and positive integer d . There is a constant C depending only on α, ρ, d such that the following holds. Let $\mathbb{F}$ be a field of characteristic larger than $\max\{d, k\}$. Let $Q \in \mathbb{F}[X, Y, Z]$ be non-zero with $\deg_{Y,Z}(Q) \leq d$.*

Then for any $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$ the number of $f \in \text{agree}_\alpha(\text{RS}_k, \mathbf{x}, \mathbf{y})$ with $Q_f = 0$ is at most Cn .

It is immediate that the two theorems imply Theorem 1.

Proof. Of theorem 1 Given $0 < \rho < 1$ take the constants α, d obtained from ρ in Theorem 3. Now given $k, n, \mathbf{x}, \mathbf{y}$, let Q be the polynomial obtained from Theorem 3 such that for all $f \in \text{agree}_\alpha(\text{RS}_k, \mathbf{x}, \mathbf{y})$ $Q(X, f, f') = 0$ with $\deg_{Y,Z}(Q) \leq d$.

Now apply Theorem 4 to $\mathbf{x}, \mathbf{y}, Q$ to obtain that the number of $f \in \text{agree}_\alpha(\text{RS}_k, \mathbf{x}, \mathbf{y})$ with $Q(X, f, f') = 0$ is at most $C \cdot n$. Since all $f \in \text{agree}_\alpha(\text{RS}_k, \mathbf{x}, \mathbf{y})$ satisfy $Q(X, f, f') = 0$, we get

$$|\text{agree}_\alpha(\text{RS}_k, \mathbf{x}, \mathbf{y})| \leq C \cdot n.$$

This proves Theorem 1. □

It is left to prove Theorems 3 and 4. This is done in the next two sections.

4 Interpolation

In this section we prove Theorem 3.

Terminology: For integer h we denote $(h)_+ := \max\{h, 0\}$.

We make a non-standard definition of a tri-variate polynomial $Q(X, Y, Z)$ vanishing with multiplicity at a point $(x, y) \in \mathbb{F}^2$.

Definition 4.1. Fix a polynomial $Q(X, Y, Z) \in \mathbb{F}[X, Y, Z]$ such that $\deg_Z(Q) \leq s$. Fix any $x, y \in \mathbb{F}$. Let

$$P(X, Y, Z) := Q(x + X, y + XY, Z).$$

We say that Q vanishes with multiplicity m at (x, y) if we can write for some polynomial $D \in \mathbb{F}[X, Y, Z]$.

$$P(X, Y, Z) = \sum_{r=0}^{m-1} X^r C_r(Y, Z) + X^m D(X, Y, Z),$$

such that for each $r \in \{0, \dots, m-1\}$, C_r is a polynomial (only) in Y, Z with $(Y - Z)^{m-r} | C_r(Y, Z)$.

The following claim demonstrates the usefulness of the above definition. In words - if Q vanishes with multiplicity m at (x, y) , $f(x) = y$ implies that Q_f vanishes with multiplicity m in the standard sense for a univariate.

Claim 4.2. Fix $Q(X, Y, Z) \in \mathbb{F}[X, Y, Z]$ such that $\deg_Z(Q) \leq s$. Fix $x, y \in \mathbb{F}$ such that Q vanishes with multiplicity m at (x, y) . Let $f \in \mathbb{F}_{<k}[X]$ satisfy $f(x) = y$. Then $Q_f(X)$ is divisible by $(X - x)^m$.

Proof. Define the so-called secant polynomial S_f of f at x :

$$S_f(X) := \frac{f(x+X) - f(x)}{X} = \frac{f(x+X) - y}{X}.$$

We have $f(x+X) = y + X \cdot S_f(X)$. Taking derivatives

$$f'(x+X) = S_f(X) + X \cdot S'_f(X).$$

Thus, the difference between the S_f and $f'(x+X)$ is a multiple of X - and we will use this shortly.

As before, define $P(X, Y, Z) := Q(x+X, y+XY, Z)$. Substituting $Y = S_f(X)$, $Z = f'(x+X)$ we get

$$P(X, S_f(X), f'(x+X)) = Q(x+X, y+X \cdot S_f(X), f'(x+X)) = Q(x+X, f(x+X), f'(x+X)) = Q_f(x+X).$$

The vanishing of Q with multiplicity m at (x, y) implies that for some polynomials $\{B_r(Y, Z)\}_{0 \leq r < m}$ and $D(X, Y, Z)$

$$P(X, Y, Z) = \sum_{r=0}^{m-1} X^r (Y - Z)^{m-r} B_r(Y, Z) + X^m D(X, Y, Z).$$

We thus have

$$\begin{aligned} Q_f(x+X) &= \sum_{r=0}^{m-1} X^r (S_f(X) - f'(x+X))^{m-r} B_r(S_f(X), f'(x+X)) + X^m D(X, S_f(X), f'(x+X)) \\ &= \sum_{r=0}^{m-1} -X^r (X^{m-r} S'_f(X)^{m-r}) B_r(S_f(X), f'(x+X)) + X^m D(X, S_f(X), f'(x+X)), \\ &= -X^m \sum_{r=0}^{m-1} S'_f(X)^{m-r} B_r(S_f(X), f'(x+X)) + X^m D(X, S_f(X), f'(x+X)), \end{aligned}$$

which is clearly a multiple of X^m . □

The following claim will upper bound the number of linear constraints required to enforce vanishing with multiplicity at a point.

Claim 4.3. *There is a universal constant C_2 such that the following holds. Fix any $s \leq m$. Let*

$$\kappa := m^2 s / 2 - m s^2 / 2 + s^3 / 3.$$

Fix any $x, y \in \mathbb{F}$. There is a set of at most $\kappa + C_2 \cdot m^2$ linear constraints on the coefficients of a trivariate $Q(X, Y, Z) \in \mathbb{F}[X, Y, Z]$ that imply Q vanishes at (x, y) with order m .

Proof. Fix $r \in [m]$. We work separately with the homogenous components of each C_r enforcing for each one that it is divisible by $(Y - Z)^{m-r}$. Note that the Y -degree of C_r is at most r : Since we are looking at $P = Q(x + X, y + XY, Z)$ the Y degree of any monomial is at most the X degree, and $C_r(Y, Z)$ is multiplied by X^r . Thus, the total degree of C_r is at most $r + s$ since $\deg_Z(Q) \leq s$. Now fix $0 \leq q \leq r + s$, and let $C_{r,q}$ be the q -th homogenous part of C_r . Write

$$C_{r,q} = \sum_{i=0}^r c_{r,q,i} Y^i Z^{q-i}.$$

Note that in fact the range of indices i is smaller: as the Z degree is s , we can't have a monomial $Y^i Z^{q-i}$ unless $q - i \leq s$; equivalently, unless $i \geq q - s$. In this context, define the interval $D_{r,q}$ of valid indices:

$$D_{r,q} := [(q - s)_+, (q - s)_+ + 1, \dots, \min\{r, q\}].$$

Thus, we in fact have

$$C_{r,q} = \sum_{i \in D_{r,q}} c_{r,q,i} Y^i Z^{q-i}.$$

Denote $d_{r,q} := |D_{r,q}|$. Thus, we have $d_{r,q} = \min\{r, q\} - (q - s)_+ + 1$.

Note that we can always enforce $(Y - Z)^{m-r}$ dividing $C_{r,q}$ using at most $d_{r,q}$ linear constraints: Each coefficient $c_{r,q,i}$ is a linear combination of Q 's coefficients, and we can simply enforce all of them to be zero.

On the other hand we can always enforce the same divisibility condition by at most $m - r$ linear constraints: To see this, define the univariate polynomial

$$h(Y) = h_{r,q}(Y) := C_{r,q}(Y, 1) = \sum_{i \in D_{r,q}} c_{r,q,i} Y^i$$

We claim it suffices to constrain $(Y - 1)^{m-r}$ divides $h(Y)$: Assume that indeed $h = (Y - 1)^{m-r} g(Y)$. We have that $C_{r,q}(Y, Z) = Z^q h(Y/Z)$, so this would imply

$$C_{r,q} = Z^q (Y/Z - 1)^{m-r} g(Y/Z)$$

We can assume that $q > m - r$ (otherwise we already know that $d_{r,q} \leq q + 1 \leq m - r$ constraints suffice), so the expression is

$$= (Y - Z)^{m-r} Z^{q-(m-r)} g(Y/Z),$$

which is divisible by $(Y - Z)^{m-r}$. Finally, it is known that enforcing $(Y - 1)^{m-r} | h(Y)$ translates to $m - r$ linear constraints on $h_{r,q}(Y)$'s coefficients, which in turn translates to $m - r$ constraints on Q 's coefficients.

Thus, the total number of constraints to enforce Q vanishing with multiplicity m on (x, y) is bounded by

$$\sum_{r=0}^{m-1} \sum_{q=0}^{r+s} \min\{m - r, d_{r,q}\}$$

and we must upper bound this quantity. We begin by upper bounding $\sum_{r=0}^{m-1} \sum_{q=0}^{r+s} d_{r,q}$ and later will subtract a lower bound on what the minimum with $m - r$ reduces.

Bounding the sum of $d_{r,q}$ values Fix r . $\sum_{q=0}^{r+s} d_{r,q}$ corresponds very simply to the number of all monomials $Y^i Z^j$ where $0 \leq i \leq r, 0 \leq j \leq s$ (each such monomial will be in *some* homogenous component of C_r). Thus $\sum_{q=0}^{r+s} d_{r,q} = (r+1) \cdot (s+1)$ and

$$\sum_{r=0}^{m-1} \sum_{q=0}^{r+s} d_{r,q} = (s+1) \sum_{r=0}^{m-1} (r+1) = (s+1)(m+2)(m+1)/2.$$

lower bounding the sum of differences $(d_{r,q} - (m-r))_+$. Define $\Delta_{r,q} = (d_{r,q} - (m-r))_+$. Note that our number of constraints is precisely

$$\sum_{r=0}^{m-1} \sum_{q=0}^{r+s} (d_{r,q} - \Delta_{r,q})$$

Thus we need to lower bound $\sum_{r=0}^{m-1} \sum_{q=0}^{r+s} \Delta_{r,q}$ in order to get an upper bound on the number of constraints.

We claim that $\sum_{q=0}^{r+s} \Delta_{r,q} = (2r+1-m)(s+1-(m-r))$: Recall how before to compute $\sum_{q=0}^{r+s} d_{r,q}$ we were thinking of the grid of all $0 \leq i \leq r, 0 \leq j \leq s$. For a given $0 \leq q \leq r+s$, the pairs (i, j) in the grid contributing to $d_{i,j}$ are on the diagonal line of pairs $(\ell, q-\ell)$. It can be seen that removing from this grid the upper left rectangular grid of size $r+1-(m-r) \times (s+1)-(m-r)$ exactly removes from each $D_{r,q}$ options beyond the first $m-r$ - if such exist. We thus have

$$\sum_{r=0}^{m-1} \sum_{q=0}^{r+s} \Delta_{r,q} = \sum_{m-s \leq r \leq m} (r+1-(m-r))(s+1-(m-r))$$

Turning this into a sum on $h := m-r$ instead

$$\begin{aligned} &= \sum_{0 \leq h \leq s} (m+1-2h)(s+1-h) = s(s+1)(m+1) + \sum_{h=0}^{s-1} -(m+1)h - (s+1)2h + 2h^2 \\ &= s(s+1)(m+1) - (m+1+2(s+1))(s+1)s/2 + 2s(s+1)(2s+1)/6 \end{aligned}$$

Note that all the pesky $+1$'s will result in terms that are $O(m^2)$, so we can write (using $s \leq m$) this as

$$\geq s^2 m/2 - s^3/3 - C m^2$$

for some universal constant C .

Summing: Thus, the number of constraints is upper bounded by

$$s m^2/2 - s^2 m/2 + s^3/3 + C \cdot m^2$$

□

Let $D := \alpha mn$. Define $\mathcal{D}$ to be the set of coefficients with weighted degree smaller than D and Z -degree at most s .

$$\mathcal{D} := \{X^i Y^j Z^\ell \mid i + (k-1)j + (k-2)\ell < D, 0 \leq \ell \leq s\}$$

Next, we need to lower bound the number of coefficients. One can prove using coefficient counting similar to [GS99] for example that

Claim 4.4. *For a universal (possibly negative) constant C_2 we have*

$$|\mathcal{D}|/n > (\alpha^2/\rho) \cdot m^2 s/2 - \alpha m s^2/2 + \rho s^3/6 + C_2 m^2$$

Our main “interpolation lemma” is

Lemma 4.5. *Fix $0 < \rho < 1$. There are constants $\rho < \alpha < \sqrt{\rho}$, and C depending only on ρ such that the following holds. Fix any $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$. There exists $Q \in \mathbb{F}[X, Y, Z]$ with non-zero coefficients only at monomials in $\mathcal{D}$ such that Q vanishes with multiplicity m at (x_i, y_i) for each $i \in [n]$.*

Proof. To guarantee a non-zero Q vanishing with multiplicity m at each (x_i, y_i) , we need the number of coefficients available divided by n to be larger than the number of constraints required for such vanishing. Omitting the $O(m^2)$ terms, using Claims 4.3 and 4.4 the lower bound on the number of coefficients, and upper bound on number of constraints are respectively

- $(\alpha^2/\rho) \cdot m^2 s/2 - \alpha m s^2/2 + \rho s^3/6$.
- $m^2 s/2 - m s^2/2 + s^3/3$.

Dividing both quantities by $(m^2 s)/2$, and denoting $\sigma := s/m$, we get

- $(\alpha^2/\rho) - \alpha\sigma + (\rho/3)\sigma^2$.
- $1 - \sigma + 2/3\sigma^2$.

Subtracting the second line from the first, we get

$$(\alpha^2/\rho - 1) + (1 - \alpha)\sigma + \frac{\rho - 2}{3}\sigma^2.$$

We wish to ensure this quantity is strictly larger than zero. In such a case, we can take a large enough constant m so that it remains positive when we add the $O(m^2)$ terms in the exact expression. Since the σ^2 coefficient is negative, we can find the unique maximum according to where the derivative vanishes. This occurs at $\sigma = \frac{3(1-\alpha)}{2(2-\rho)}$. Substituting this value we get

$$\frac{\alpha^2}{\rho} - 1 + \frac{3(1-\alpha)^2}{4(2-\rho)}$$

It is easy to see this expression will be positive for some $\alpha < \sqrt{\rho}$: At $\alpha = \sqrt{\rho}$ the first two terms cancel out, and we are left only with $\frac{3(1-\sqrt{\rho})^2}{4(2-\rho)} > 0$. So by continuity there

must be $\alpha < \sqrt{\rho}$ that leaves this expression positive. As a concrete value, what can take for example $\alpha := \sqrt{\rho} \left(1 - \frac{(1-\sqrt{\rho})^2}{8}\right)$. $\square$

Finally, we prove Theorem 3

proof of theorem 3. Use Lemma 4.5 to get Q vanishing with multiplicity m at each point (x_i, y_i) . Given $f \in \text{agree}_\alpha(\text{RS}_k, \mathbf{x}, \mathbf{y})$ we have from Claim 4.2 that $Q_f(x_i) = Q(x_i, f(x_i), f'(x_i))$ vanishes with multiplicity m for the $\lceil \alpha n \rceil$ agreement points of f with $\mathbf{y}$. Since $\deg(Q_f) < \alpha mn$ this implies Q_f is identically zero as required. $\square$

5 Bounding the number of roots

In this section we show that a non-zero bi-variate $Q \in L[Y, Z]$ cannot have too many “roots” f in the sense of $Q(f, f') = 0$ that agree with a given received word $\mathbf{y}$ at many places. We set some terminology in order to precisely state our claim.

Notation and Terminology In this section L denotes the algebraic closure of $\mathbb{F}(X)$. We work throughout the section with a polynomial $Q \in \mathbb{F}[X, Y, Z]$. We denote $d := \deg_{Y,Z}(Q)$ - meaning the total degree in variables Y, Z . We assume $a, k, n, S, \mathbf{x}, \mathbf{y}$ are defined as before. We assume the characteristic $p > k$. We say $f \in \mathbb{F}_{<k}[X]$ is a *root* of Q if $Q(X, f, f') = 0$ and $f(x_i) = y_i$ for at least a values $i \in [n]$. In other words f is a root of Q if $f \in \text{agree}_\alpha(\text{RS}_k, \mathbf{x}, \mathbf{y})$ and $Q(X, f, f') = 0$.

We denote by $Q_X, Q_Y, Q_Z \in \mathbb{F}[X, Y, Z]$ the derivatives of Q with respect to X, Y, Z respectively. Denote $H(X, Y, Z) := Q_Z$. We say that f is a *regular root* if $H(X, f, f') \neq 0$. Otherwise, we say f is a *singular root*.

Square-freeness: We sometimes think of Q as a bi-variate $Q \in L[Y, Z]$.³ We assume that $Q(Y, Z) \in L[Y, Z]$ is a non-zero bi-variate over L that is *square free*. That is,

$$Q(Y, Z) = \prod_{i=1}^t T_i(Y, Z)$$

where $T_i \in L(Y, Z)$ is irreducible and $\gcd(T_i, T_j) = 1$ for $i \neq j$. Note that we can move to the square-free part of Q from Section 4 without changing the set of roots f according to our above definition.

We begin by showing that for a regular root f we can derive all its derivatives via a differential equation.

³Note that every element of $\mathbb{F}[X, Y, Z]$ can be thought of as an element of $L[Y, Z]$; but the converse is not true: An element of $L[Y, Z]$ might have “weird” coefficients like $\sqrt{X}$ and so does not naturally map to a tri-variate in $\mathbb{F}[X, Y, Z]$.

Lemma 5.1. *For each $2 \leq j \leq k$ there exists a polynomial $F_j \in \mathbb{F}[X, Y, Z]$ such that for any regular root $f \in \mathbb{F}_{<k}[X]$*

$$f^{(j)} = \frac{F_j(X, f, f')}{H(X, f, f')^{2j-3}}.$$

Furthermore, we have $\deg_{Y,Z}(F_j) \leq d \cdot (2j - 3)$.

Proof. We prove the lemma by induction on j . Fix a regular root $f \in \mathbb{F}_{<k}[X]$. For $j = 2$: Since f is a root we know that $Q_f = Q(X, f, f')$ is identically zero, and hence so is Q'_f . Using the chain rule for derivatives, recalling that $H = Q_Z$, we get

$$0 = Q'_f(X) = Q_X(X, f, f') + Q_Y(X, f, f')f' + H(X, f, f')f''.$$

As f is regular we can divide by $H(X, f, f')$ and get

$$f''(X) = -\frac{Q_X(X, f, f') + Q_Y(X, f, f')f'}{H(X, f, f')}$$

Thus, if we set $F_2(X, Y, Z) := -(Q_X + Q_Y \cdot Z)$ we have

$$F_2(X, f, f')/H(X, f, f') = f''(X).$$

As $\deg_{Y,Z}(F_2) \leq d$ this proves the induction base for $j = 2$.

Proceeding to the induction step, define for a tri-variate polynomial $F[X, Y, Z]$,

$$\mathcal{E}(F) := H(F_X + F_Y \cdot Z) - F_Z(Q_X + Q_Y \cdot Z)$$

We have

$$(F(X, f, f'))' = \frac{\mathcal{E}(F)(X, f, f')}{H(X, f, f')}$$

and $\deg_{Y,Z}(\mathcal{E}(F)) \leq \deg_{Y,Z}(F) + d$.

Now assume that

$$f^{(j)} = \frac{F_j(X, f, f')}{H^{2j-3}(X, f, f')}.$$

Let $F = F_j$. Omitting below the substitution (X, f, f') in all tri-variate polynomials to avoid cumbersome notation, using the chain rule we have

$$f^{(j+1)} = \frac{\frac{\mathcal{E}(F)}{H} H^{2j-3} - (2j-3) \cdot F H^{2j-4} \frac{\mathcal{E}(H)}{H}}{H^{4j-6}}$$

Multiplying numerator and denominator by H we get

$$= \frac{\mathcal{E}(F) H^{2j-3} - (2j-3) H^{2j-4} F \mathcal{E}(H)}{H^{4j-5}}$$

Cancelling as many H factors as possible we get

$$= \frac{\mathcal{E}(F) H - (2j-3) F \mathcal{E}(H)}{H^{2j-1}}.$$

Define $F_{j+1} := \mathcal{E}(F) H - (2j-3) F \mathcal{E}(H)$. Note that $\deg(F_{j+1}) \leq \deg(F_j) + 2d \leq 2d + (2j-3)d = (2j-1)d$, where we used the induction hypothesis for j in the second inequality.

Since $(2j-1)d = (2(j+1)-3)d$ this proves the induction step for $j+1$. □

“Formal derivative” evaluation equation

5.1 The A_i curves

To get a good bound on the number of regular roots, we need to show they are contained in many intersections of $\text{zeros}(Q)$ with other curves. For this purpose, first define

$$F_0(Y, Z) := Y/H^3(Y, Z), F_1(Y, Z) := Z/H(Y, Z).$$

Note that while F_0, F_1 are not polynomials, they satisfy the formula in Lemma 5.1. Namely, for $j = 0, 1$

$$f^{(j)} = \frac{F_j(X, f, f')}{H^{2j-3}}$$

for any regular root f .

Now define for $i \in [n]$

$$A_i(Y, Z) := \sum_{0 \leq j < k} \frac{(x_i - X)^j}{j!} F_j(Y, Z) H^{2(k-j)-2} - H^{2k-5} y_i.$$

The point is that when x_i is an agreement point for f , (f, f') will be contained in A_i .

Claim 5.2. *For a regular root f , $(f, f') \in \text{zeros}(A_i)$ when $f(x_i) = y_i$.*

Proof. We will use the following “evaluation via formal derivatives” formula that holds for any $f \in \mathbb{F}_{<k}[X]$ and $x \in \mathbb{F}$:

$$f(x) = \sum_{0 \leq j < k} \frac{(x - X)^j}{j!} f^{(j)}(X)$$

Fix $i \in [n]$ and a regular root f . From Lemma 5.1 we have for all j

$$f^{(j)} = \frac{F_j(X, f, f')}{H(X, f, f')^{2j-3}}.$$

We substitute this expression for the derivatives of f inside the aforementioned evaluation formula and get

$$f(x_i) = \sum_{0 \leq j < k} \frac{(x_i - X)^j}{j!} \frac{F_j(X, f, f')}{H(X, f, f')^{2j-3}}$$

Multiplying by $H(X, f, f')^{2k-5}$ to clear denominators, we have

$$H(X, f, f')^{2k-5} f(x_i) = \sum_{0 \leq j < k} \frac{(x_i - X)^j}{j!} H(X, f, f')^{2(k-j)-2} F_j(X, f, f').$$

Now, observe that when $f(x_i) = y_i$, this is precisely the equation defining A_i evaluated at (f, f') . That is, $A(f, f') = 0$. $\square$

We want to use Theorem 2 to bound the intersections $\text{zeros}(T) \cap \text{zeros}(A_i)$ of irreducible components T of Q with the A_i curves. For this, we need to deal separately with the cases where T divides A_i , which we do next.

Claim 5.3. *Let T be an irreducible component of Q . If $T|A_i$ for at least k values $i \in [n]$ then T contains at most one regular root of Q .*

Proof. For each $i \in [n]$ $T|A_i$ implies that for any $f \in T$, $A_i(f, f') = 0$. When f is a regular root this implies $f(x_i) = y_i$. If that holds for k different $i \in [n]$ there is a unique $f \in \mathbb{F}_{<k}[X]$ that satisfies these constraints. $\square$

Now we are ready to bound the total number of regular roots in an irreducible component.

Lemma 5.4. *Fix any irreducible component T of Q . Then T contains at most $\frac{(n-k)(2k-3)d\deg(T)}{(a-k)} \leq \frac{1-\rho}{\alpha-\rho}(2k-3)d\deg(T)$ regular roots.*

Proof. If $T|A_i$ for k values $i \in [n]$ the claim follows from Claim 5.3. Assume otherwise. Call A_i good if T doesn't divide A_i . For such i we can conclude by Theorem 2 that $|\text{zeros}(T) \cap \text{zeros}(A_i)| \leq (2k-3)d\deg(T)$. Let N be the number of regular roots in T . Each such f is contained in good A_i for at least $a-k$ i 's. So we have

$$(a-k) \cdot N \leq (n-k)(2k-3)d\deg(T),$$

implying

$$N \leq \frac{(n-k)(2k-3)d\deg(T)}{a-k}$$

$\square$

5.2 The singular case

Now we bound the number of singular roots of an irreducible component T of Q .

Claim 5.5. *Assume that $\text{char}(L) > d$. If T is an irreducible component of Q . Then the number of singular roots $f \in T$ is smaller than $\deg(T)d$.*

Proof. Suppose first that $T \nmid H$. Any singular root f satisfies $H(f, f') = T(f, f') = 0$. Since T is irreducible we have from Theorem 2 that the number of singular roots in T is at most $\deg(T) \cdot \deg(H) < \deg(T)d$.

Now suppose T divides H . We show this implies $T_Z = 0$: Recall that Q is assumed to be square-free. Write $Q = T \cdot R$ for R with $\gcd(T, R) = 1$. Now take the derivative of Q in variable Z using the product rule. ⁴

$$H = Q_Z = T_Z R + T R_Z$$

⁴Observe that the derivative of Q in Z as a bi-variate over L is the same as its derivative $H = Q_Z$ by Z as a tri-variate in $\mathbb{F}[X, Y, Z]$.

If T divides H we can write for some $P \in L[Y, Z]$

$$TP = T_Z R + T R_Z$$

which implies

$$T(P - R_Z) = T_Z R$$

Now look at two cases. If $T_Z \neq 0$ then we must have that T divides T_Z . But this is impossible since $\deg(T_Z) < \deg(T)$. Suppose that $T_Z = 0$. Since $\text{char}(L) > d$ this implies T doesn't depend on Z . So $T = T(Y)$. Thus, any root f contained in T , satisfies $T(f) = 0$. In other words, f is an actual root of T as a univariate polynomial over L ; and so, there can only be $\deg_Y(T)$ roots (regular or singular) contained in T . $\square$

5.3 final calculation

Proof. (of Theorem 4) First note that given any non-zero $Q \in L[Y, Z]$ as in the theorem statement, we can always move to the square free part of Q . This doesn't increase the degree d or change the set of roots (f, f') . Let $\eta := (d + \frac{1-\rho}{\alpha-\rho}(2k-3))$. In summary, according to Claims 5.5 and 5.4 the total number of roots in a component T is at most $\eta \deg(T)$ and so the total number of roots is at most $\eta \cdot d$. Define $C := 2\rho d(d + \frac{1-\rho}{\alpha-\rho})$. Using $2k-3 \leq 2\rho n$ we have that the total number of roots is at most Cn . Noting that C is indeed a constant depending only on d, α, ρ , this concludes the proof. $\square$

Acknowledgements

We thank Matteo Frigo and the authors of [BCP⁺26] for discussions and comments.

References

- [BCP⁺26] J. Brakensiek, Y. Chen, A. Putterman, Z. Zhang, and K. Zhe Zheng. Algorithmic list decoding of reed-solomon codes up to capacity. Technical Report TR26-164, Electronic Colloquium on Computational Complexity, 2026.
- [GS99] V. Guruswami and M. Sudan. Improved decoding of reed-solomon and algebraic-geometry codes. *IEEE Transactions on Information Theory*, 45(6):1757–1767, 1999.
- [GW11] V. Guruswami and C. Wang. Optimal rate list decoding via derivative codes. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, volume 6845 of *Lecture Notes in Computer Science*, pages 593–604. Springer, 2011.
- [Jer26] F. Granha Jeronimo. Algorithmic list decoding at capacity and optimal proximity gaps for reed-solomon codes. Technical Report TR26-169, Electronic Colloquium on Computational Complexity, 2026.

- [Joh62] S. M. Johnson. A new upper bound for error-correcting codes. *IRE Transactions on Information Theory*, 8(3):203–207, 1962.
- [Kop15] S. Kopparty. List-decoding multiplicity codes. *Theory of Computing*, 11:149–182, 2015.
- [Sud97] M. Sudan. Decoding of reed solomon codes beyond the error-correction bound. *Journal of Complexity*, 13(1):180–193, 1997.