Reed–Solomon Mutual Correlated Agreement Beyond the Johnson Radius

Sunghyeon Jo
Georgia Institute of Technology
sjo65@gatech.edu

August 19, 2026

Abstract

Mutual correlated agreement (MCA) bounds how many points on an affine line of received words can agree with codewords on many coordinates when the line does not admit a common codeword explanation on those coordinates; the corresponding line parameters are called bad. MCA arises in the soundness analysis of code-based proof systems. For Reed–Solomon codes with arbitrary prescribed evaluation sets, existing deterministic bounds apply only at integer error budgets strictly below the exact Johnson boundary.

Fix integers $r \geq 2$ and $h \geq 1$. For every sufficiently large K, let $L \subseteq \mathbb{F}_q$ be any set of $n = rK$ distinct points and set $C = \mathrm{RS}_{<K}(\mathbb{F}_q, L)$. At error budget

$$E = \left\lfloor n - \sqrt{n(K-1)} \right\rfloor + h,$$

we prove that every affine line has at most $O_{r,h}(K^6)$ bad parameters. Hence

$$\varepsilon_{\mathrm{mca}}(C, E) = O_{r,h}(K^6/q).$$

Thus, at each fixed rate $1/r$, any fixed number of integer steps beyond Johnson admits a deterministic polynomial bound on the number of bad parameters; in relative-radius units, the gain is $O(1/n)$.

We also derive a MCA upper bound for maximum distance separable (MDS) codes from a sharp lower bound on the number of rejected local membership tests. For Reed–Solomon codes over sufficiently large fields, the resulting endpoint bound is exact whenever at most $K + 1$ agreements are required. It yields exact 2^{-128} thresholds for four explicit smooth-domain codes of length 64: we identify the largest safe integer budget and prove that the next one is unsafe. As a concrete application to the Grand MCA Challenge, we exhibit a single prime field $\mathbb{F}_Q$, with $Q < 2^{256}$, that supports the required smooth domains at all four target rates. With $K = 2^{18}$, the first post-Johnson budget has MCA error below 2^{-128} at rates $1/2, 1/4, 1/8$, and $1/16$, as does the second such budget at rate $1/8$.

Contents

1 Introduction **3**
- 1.1 Main results and techniques . . . 3
- 1.2 Related work . . . 4

2 Preliminaries **5**
- 2.1 Codes and smooth Reed–Solomon domains . . . 5
- 2.2 Integer-radius MCA . . . 5
- 2.3 A deterministic bound below the Johnson boundary . . . 6

3 Agreement-set shortening **7**
- 3.1 The shortening map . . . 7
- 3.2 Crossing the Johnson boundary . . . 8
- 3.3 Polynomial bounds beyond the Johnson boundary . . . 9

4 Non-asymptotic bounds from MDS circuits **10**
- 4.1 Rejecting-test abundance in MDS codes . . . 10
- 4.2 The circuit-incidence bound . . . 11
- 4.3 Exact Reed–Solomon behavior at the endpoint . . . 11
- 4.4 Combining the two upper bounds . . . 13

5 Consequences for the Grand MCA Challenge **13**
- 5.1 Challenge-scale parameters over a common field . . . 14
- 5.2 Exact length-64 thresholds . . . 15
- 5.3 All-radius bounds from large fields . . . 15
- 5.4 Discussion and limitations . . . 16

A Optimizing the shortening length at rate $1/4$ **18**

B Exact arithmetic certificates **18**
- B.1 Proth certificates . . . 18
- B.2 Exact evaluation below the Johnson boundary . . . 18

1 Introduction

Mutual correlated agreement (MCA) is an affine-line consistency property for linear codes. Informally, it asks whether many points on an affine line can individually agree with codewords on large coordinate sets even though the line itself has no consistent codeword explanation on those sets.

To make this precise, let $C \subseteq \mathbb{F}^L$ be a linear code and let

$$u_z = u_0 + zu_1, \qquad z \in \mathbb{F},$$

be an affine line of received words. A parameter z is bad at error budget E if u_z agrees with a codeword on some set $A \subseteq L$ of at least $|L| - E$ coordinates, but u_0 and u_1 do not both admit codeword explanations on that same set. An MCA bound controls the fraction of bad parameters uniformly over all affine lines.

MCA was introduced in the analysis of the WHIR proximity test [ACFY25]. Its error now appears in the soundness analysis of several code-based proof systems. The Grand MCA Challenge [ABF26] asks for sharp thresholds for Reed–Solomon codes on prescribed smooth evaluation domains. Its concrete regime includes rates $1/2, 1/4, 1/8$, and $1/16$, dimensions at most 2^{40}, fields smaller than 2^{256}, and target error 2^{-128}.

The natural benchmark is the exact Johnson boundary in error units. For a length-n, dimension-K Reed–Solomon code, it is

$$E_J(n, K) = n - \sqrt{n(K-1)}.$$

Deterministic bad-parameter bounds are known for every integer budget strictly below this value, for an arbitrary prescribed evaluation set [BCHKS25, Hab25]. We show that, at every fixed reciprocal-integer rate $1/r$ considered here, one may cross the boundary by any fixed number of integer error steps while retaining a polynomial bound. The corresponding improvement in relative radius is $O(1/n)$.

1.1 Main results and techniques

Write $B_C(E)$ for the maximum number of bad parameters on an affine line when at most E errors are allowed; see theorem 2.1. The main result is the following.

Theorem 1.1 (Main result, informal)**.** *Fix integers $r \geq 2$ and $h \geq 1$. For all sufficiently large K, let $L \subseteq \mathbb{F}$ have size rK, set $C = \mathrm{RS}_{<K}(\mathbb{F}, L)$, and put*

$$E = \left\lfloor rK - \sqrt{rK(K-1)} \right\rfloor + h.$$

Then E is the hth integer error budget strictly above the exact Johnson boundary, and

$$B_C(E) = O_{r,h}(K^6).$$

The theorem is uniform over the field and the evaluation set. Its proof uses two complementary mechanisms with different strengths. To obtain the asymptotic result near the Johnson boundary, we shorten coordinates chosen from each witnessing agreement set. An incidence argument for maximum distance separable (MDS) codes instead gives an explicit non-asymptotic bound at every radius and becomes exact when few agreements are required. Near Johnson at fixed positive rate, however, this bound is generally exponential in K, so the shortening argument is essential there.

Agreement-set shortening. A bad parameter comes with a witnessing set of at least $T = n - E$ agreement coordinates. Choose any t of them and shorten on those coordinates. The shortened word retains at least $T - t$ agreements in a Reed–Solomon code of length $n - t$ and dimension $K - t$, while the error budget remains E. Double counting the choices of shortening set gives

$$B_C(E) \le \frac{\binom{n}{t}}{\binom{T}{t}} \max_{|S|=t} B_{C_S}(E), \tag{1}$$

where C_S is the shortened code. For fixed r and h, a constant $t = t(r, h)$ moves every shortened code strictly below its own Johnson boundary. Applying the explicit deterministic estimate of [BCHKS25] then gives the $O_{r,h}(K^6)$ bound. Because t is constant and T is a constant fraction of n, the transfer factor in (1) is bounded independently of K.

Non-asymptotic bounds from MDS circuits. Let a bad parameter be witnessed on m coordinates of an $[n, K]$ MDS code. For every test size $a \in \{K + 1, \dots, m\}$, the direction u_1 fails at least $\binom{m-1}{a-1}$ local membership tests. No rejecting test can be charged to two distinct bad parameters. Counting all a-coordinate tests and dividing by this guaranteed number of rejections gives

$$B_C(E) \le \min_{K+1 \le a \le T_{\text{eff}}} \left\lfloor \frac{\binom{n}{a}}{\binom{T_{\text{eff}}-1}{a-1}} \right\rfloor, \qquad T_{\text{eff}} = \max\{n - E, K + 1\}. \tag{2}$$

The number of guaranteed rejections is best possible. For Reed–Solomon codes, divided differences give a matching construction when $n - E \le K + 1$: if $M = \binom{n}{K+1}$ and $q > \binom{M}{2}$, then $B_C(E) = M$. This exact endpoint behavior yields a safe integer budget immediately followed by an unsafe one for suitable concrete parameters.

Certified challenge parameters. The two methods yield different kinds of concrete statements.

- Over a single explicit prime $Q < 2^{256}$, dimension $K = 2^{18}$ works simultaneously at all four target rates. The first integer budget beyond Johnson has MCA error below 2^{-128} in every case, and the rate-1/8 code also meets the target at the second budget.
- Four smooth length-64 Reed–Solomon codes have exact thresholds at consecutive integer budgets: the 2^{-128} target holds at one budget and fails at the next.

All numerical statements are verified using exact integer and rational comparisons, as described in section B.

1.2 Related work

The proximity-gap framework for Reed–Solomon codes was developed in [BCIKS20], and MCA was introduced in [ACFY25]. Our shortening argument uses the explicit deterministic estimate below Johnson from [BCHKS25]; the relevant reduced rate there is $(K - 1)/n$. The independent argument of [Hab25] reaches the same strict boundary from below.

Recent work establishes results approaching capacity for subspace-design codes and for Reed–Solomon codes with random evaluation points [GG25, GGSW26]. These results do not apply to a prescribed smooth multiplicative subgroup. Conversely, broad up-to-capacity statements are obstructed in general [CS25, KKH26], including for smooth prime-field families.

A contemporaneous manuscript [Cho26] also uses the fixed-support ownership fact: on one affine line, a given coordinate set can witness at most one bad parameter. Our additional ingredient is the rejecting-test abundance lemma. One non-codeword restriction of an MDS code forces $\binom{m-1}{a-1}$ rejecting a-subsets, which is exactly the denominator in (2).

The abundance lemma is also related to the weight distribution of MDS-code cosets. An a-subset accepts precisely when the corresponding coset of the punctured MDS code contains a representative that vanishes on those a coordinates. This connects the statement to work on weight distributions of MDS-code cosets [DMP21]. We use a direct induction because it gives the uniform extremal count required by the incidence argument.

A separate consequence concerns interleavings. The theorem of [Jo26] transfers every MCA bound proved here to row-wise interleavings of the same base code. The other terms in protocol soundness analyses, including interleaved list size and query error, remain separate.

The main theorem certifies a fixed number of integer steps beyond Johnson, not a positive constant improvement in relative radius. The length-64 thresholds are exact concrete-parameter statements whose values depend on both the code parameters and the field size. We make no claim about list decoding or end-to-end protocol security. Obtaining a constant-relative improvement for Reed–Solomon codes on a prescribed smooth subgroup remains open.

2 Preliminaries

2.1 Codes and smooth Reed–Solomon domains

Throughout the paper, n denotes the code length, K the dimension, E the allowed number of errors, and

$$T := n - E$$

the required number of agreements. We keep the integer E explicit because the exact Johnson boundary need not lie on the integer grid.

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field and let L be a coordinate set of size n. For $C \subseteq \mathbb{F}^L$ and $A \subseteq L$, write

$$C|_A := \{c|_A : c \in C\}.$$

A linear code $C \subseteq \mathbb{F}^L$ of dimension K is an $[n, K]$ maximum distance separable (MDS) code if puncturing to every K coordinates is an isomorphism onto $\mathbb{F}^K$. Equivalently, every nonzero codeword has at most $K - 1$ zero coordinates.

For a set $L \subseteq \mathbb{F}$ of n distinct elements and $1 \le K \le n$, define

$$\mathrm{RS}_{<K}(\mathbb{F}, L) := \{(p(\alpha))_{\alpha \in L} : p \in \mathbb{F}[X],\ \deg p < K\}.$$

This is an $[n, K]$ MDS code: two distinct codewords agree on at most $K - 1$ coordinates. The code rate is K/n, whereas the exact Johnson radius is

$$\delta_J(n, K) := 1 - \sqrt{\frac{K-1}{n}}. \tag{3}$$

This is Johnson's bound [Joh62] with the exact MDS distance. In integer-error units, write

$$E_J(n, K) := n - \sqrt{n(K-1)}. \tag{4}$$

When $n \mid (q-1)$, let $H_n \subseteq \mathbb{F}_q^\times$ denote the unique multiplicative subgroup of order n. Following the terminology of [ABF26], we call a multiplicative coset of H_n a *smooth domain* when n is a power of two; see Definition 2.12 there.

2.2 Integer-radius MCA

Fix words $u_0, u_1 \in \mathbb{F}^L$ and the affine line

$$u_z := u_0 + z u_1, \qquad z \in \mathbb{F}.$$

Definition 2.1 (Bad parameters)**.** Let $C \subseteq \mathbb{F}^L$ be linear and let $E \in \{0, \dots, n\}$ be an integer error budget. Put $T := n - E$. A parameter $z \in \mathbb{F}$ is *bad* for (u_0, u_1) at budget E if there are $A \subseteq L$ and $c_z \in C$ such that

$$|A| \geq T, \qquad u_z|_A = c_z|_A, \qquad (u_0|_A, u_1|_A) \notin (C|_A)^2.$$

Define

$$\begin{aligned} \mathrm{Bad}_C(u_0, u_1; E) &:= \{z \in \mathbb{F} : z \text{ is bad}\}, \\ B_C(u_0, u_1; E) &:= |\,\mathrm{Bad}_C(u_0, u_1; E)|, \\ B_C(E) &:= \max_{u_0, u_1 \in \mathbb{F}^L} B_C(u_0, u_1; E), \\ \varepsilon_{\mathrm{mca}}(C, E) &:= \frac{B_C(E)}{q}. \end{aligned}$$

The first two conditions say that u_z has a codeword explanation on at least $n - E$ coordinates. The last condition says that those same coordinates do not explain the whole affine line.

This is the affine-line specialization of MCA used in [ABF26, ACFY25]. For a real radius $\delta \in [0, 1]$, the standard condition $|A| \geq (1 - \delta)n$ is equivalent to $|A| \geq n - \lfloor \delta n \rfloor$. Accordingly,

$$\varepsilon_{\mathrm{mca}}(C, \delta) := \varepsilon_{\mathrm{mca}}(C, \lfloor \delta n \rfloor). \tag{5}$$

The function is nondecreasing in E and is a step function of δ.

For a target $2^{-\lambda}$, define

$$E^*_\lambda(C) := \max\{E \in \{0, \dots, n\} : \varepsilon_{\mathrm{mca}}(C, E) \leq 2^{-\lambda}\},$$

when the set is nonempty. If $E^*_\lambda(C) < n$, then the safe real radii form the half-open interval

$$\left[0, \frac{E^*_\lambda(C) + 1}{n}\right).$$

Thus the natural real-valued threshold is a supremum; it need not be attained. We report the largest safe integer budget, the supremal real radius, and the endpoint status.

We repeatedly use the following reduction.

Lemma 2.2 (Direction criterion)**.** *Suppose $u_z|_A \in C|_A$. Then*

$$(u_0|_A, u_1|_A) \notin (C|_A)^2 \quad \Longleftrightarrow \quad u_1|_A \notin C|_A.$$

If C is $[n, K]$ MDS, every bad witness has $|A| \geq K + 1$.

Proof. If $u_1|_A = d_1|_A$ for some $d_1 \in C$ and $u_z|_A = c_z|_A$, then $u_0|_A = (c_z - z d_1)|_A$, so the pair has a mutual codeword explanation. The converse is immediate. If $|A| \leq K$, puncturing an MDS code to A is surjective, so every word on A belongs to $C|_A$. □

2.3 A deterministic bound below the Johnson boundary

The shortening argument will reduce our problem to a Reed–Solomon code on an arbitrary evaluation set strictly below its Johnson boundary. We record the precise bound used at that point.

For integers N, d, E with $0 < d < N$ and $0 < E < N$, put

$$\rho := \frac{d}{N}, \qquad \gamma := \frac{E}{N}, \qquad \eta := 1 - \sqrt{\rho} - \gamma.$$

When $\eta > 0$, define

$$m_{\mathrm{B}} := \max\left\{\left\lceil \frac{\sqrt{\rho}}{\eta} \right\rceil, 3\right\}, \qquad x_{\mathrm{B}} := m_{\mathrm{B}} + \frac{1}{2}, \tag{6}$$

$$\mathsf{J}(N, d, E) := \left(\frac{2x_{\mathrm{B}}^5 + 3x_{\mathrm{B}}\gamma\rho}{3\rho^{3/2}}\right) N + \frac{x_{\mathrm{B}}}{\sqrt{\rho}}. \tag{7}$$

At a fixed positive reduced rate ρ, the qualitative dependence is

$$\mathsf{J}(N, d, E) = O(N\eta^{-5}).$$

The main K^6 theorem uses only this qualitative dependence. The exact expression is used for the leading constant and concrete evaluations; section B explains how those evaluations are certified by exact rational arithmetic.

The next theorem is the affine-line specialization of Theorem 4.6 in [BCHKS25].

Theorem 2.3 (Bound below Johnson)**.** *Let $C = \mathrm{RS}_{<d+1}(\mathbb{F}_q, L)$ have length N. If*

$$(N - E)^2 > Nd, \tag{8}$$

then

$$B_C(E) \le \mathsf{J}(N, d, E). \tag{9}$$

In the notation of [BCHKS25], the code dimension is $d + 1$, the reduced rate is $\rho = d/N$, and the curve parameter is $\gamma = E/N$. The strict condition (8) is equivalent to $\gamma < 1 - \sqrt{\rho}$.

3 Agreement-set shortening

3.1 The shortening map

Ordinary shortening keeps codewords that vanish on a chosen coordinate set S and then deletes those coordinates. To apply this operation to an arbitrary received word, we first subtract the polynomial interpolating its values on S. The difference vanishes on S, so dividing by the vanishing polynomial of S produces a normalized word on the remaining coordinates.

Let $C = \mathrm{RS}_{<K}(\mathbb{F}, L)$ and fix $S \subseteq L$ of size $t < K$. Put

$$P_S(X) := \prod_{\alpha \in S} (X - \alpha).$$

For $w \in \mathbb{F}^L$, let $I_S(w)$ be the degree-$< t$ polynomial interpolating $w|_S$. For $S = \varnothing$, set $I_S(w) = 0$ and $P_S = 1$. Define

$$Q_S(w)(x) := \frac{w(x) - I_S(w)(x)}{P_S(x)}, \qquad x \in L \setminus S. \tag{10}$$

The map Q_S is linear and sends codewords of $\mathrm{RS}_{<K}$ to codewords of $\mathrm{RS}_{<K-t}$. The punctured domain $L \setminus S$ need not remain smooth; this causes no problem because theorem 2.3 holds for an arbitrary Reed–Solomon evaluation set.

Lemma 3.1 (Badness is preserved by shortening)**.** *Let z be bad for $C = \mathrm{RS}_{<K}(\mathbb{F}, L)$ at error budget E, witnessed by $A \subseteq L$. If $S \subseteq A$, $|S| = t < K$, and $t \le T = n - E$, then z is bad at the same error budget E for*

$$C_S := \mathrm{RS}_{<K-t}(\mathbb{F}, L \setminus S)$$

on the shortened line $Q_S(u_0) + zQ_S(u_1)$.

Proof. Let $c_z \in C$ agree with u_z on A. Since $S \subseteq A$, the interpolants $I_S(c_z)$ and $I_S(u_z)$ coincide. Hence $Q_S(c_z)$ agrees with $Q_S(u_z)$ on $A \setminus S$, and $Q_S(c_z) \in C_S$. The shortened agreement threshold is $(n-t) - E = T - t$, which is met.

Suppose that codewords $g_i \in C_S$ agree with $Q_S(u_i)$ on $A \setminus S$ for $i = 0, 1$. Let G_i be degree-$< K - t$ polynomials representing g_i and set

$$p_i(X) := I_S(u_i)(X) + P_S(X)G_i(X).$$

Then $\deg p_i < K$, and its evaluation agrees with u_i on S by construction and on $A \setminus S$ after applying Q_S. This lifts to a mutual codeword explanation on A, contradicting badness. □

Theorem 3.2 (Agreement-set shortening transfer)**.** *Let $C = \mathrm{RS}_{<K}(\mathbb{F}, L)$ have length n, and let $T = n - E$. For every $0 \le t < K$ with $t \le T$,*

$$B_C(u_0, u_1; E)\binom{T}{t} \le \sum_{\substack{S \subseteq L \\ |S|=t}} B_{C_S}(Q_S(u_0), Q_S(u_1); E). \tag{11}$$

Consequently,

$$B_C(E) \le \frac{\binom{n}{t}}{\binom{T}{t}} \max_{|S|=t} B_{C_S}(E). \tag{12}$$

Proof. For each bad parameter z, choose one witnessing set A_z. It contains at least $\binom{T}{t}$ subsets S of size t. By theorem 3.1, every pair (z, S) with $S \subseteq A_z$ contributes the same parameter to the shortened bad set for S. Counting these pairs first by z and then by S proves (11); maximizing gives (12). □

The factor $\binom{n}{t}/\binom{T}{t}$ is the price of not knowing which coordinates occur in a bad witness. When t is fixed and T is a constant fraction of n, this factor is bounded independently of the block length.

3.2 Crossing the Johnson boundary

Put $d = K - 1$. After shortening t coordinates, the new length, reduced degree parameter, and agreement threshold are

$$N = n - t, \qquad d_t = d - t, \qquad T_t = T - t.$$

The shortened Johnson surplus is the linear function

$$\begin{aligned} T_t^2 - N d_t &= (T-t)^2 - (n-t)(d-t) \\ &= T^2 - nd + t(n + d - 2T). \end{aligned} \tag{13}$$

The shortened code lies strictly below its Johnson boundary exactly when the left-hand side of (13) is positive. The fact that this expression is linear in t is what makes a fixed amount of shortening useful.

Corollary 3.3 (Transferred bound below Johnson)**.** *Let $C = \mathrm{RS}_{<K}(\mathbb{F}, L)$ have length n, put $T = n - E$, and assume $E > 0$. If*

$$0 \le t \le \min\{T, K-2\}, \qquad (T-t)^2 > (n-t)(K-1-t), \tag{14}$$

then

$$B_C(E) \le \frac{\binom{n}{t}}{\binom{T}{t}} \mathsf{J}(n-t, K-1-t, E). \tag{15}$$

Proof. Every shortened code has length $n-t$ and positive reduced degree parameter $K-1-t$. The second condition in (14) is exactly its strict Johnson condition at budget E. Apply theorem 2.3 in (12). □

3.3 Polynomial bounds beyond the Johnson boundary

This subsection contains the asymptotic core of the paper. The transfer yields a polynomial bad-parameter bound at any fixed number of integer steps beyond Johnson, for every fixed rate $1/r$.

Theorem 3.4 (Fixed integer steps beyond Johnson)**.** *Fix integers $r \geq 2$ and $h \geq 1$, and put*

$$t_{r,h} := \left\lfloor \frac{2h\sqrt{r}}{(\sqrt{r}-1)^2} \right\rfloor + 1. \tag{16}$$

There are constants $K_0(r,h)$ and $A_{r,h} > 0$ such that the following holds. For every $K \geq K_0(r,h)$, let $n = rK$, let $L \subseteq \mathbb{F}$ have size n, and let $C = \mathrm{RS}_{<K}(\mathbb{F}, L)$. Define

$$E_{r,h} := \lfloor E_J(n,K) \rfloor + h. \tag{17}$$

Then $E_{r,h}$ is the hth integer error budget strictly above the exact Johnson boundary $E_J(n,K)$ and

$$B_C(E_{r,h}) \leq A_{r,h} K^6. \tag{18}$$

Proof. The deficit before shortening. Write $s = \sqrt{r}$, $x = \sqrt{rK(K-1)}$, and

$$T = n - E_{r,h} = \lceil x \rceil - h.$$

Increase $K_0(r,h)$, if necessary, so that $T > t_{r,h}$, $K \geq t_{r,h} + 2$, and $0 < E_{r,h} < n$ throughout the argument. Then $\theta := x - T$ lies in $(h-1, h]$. The original Johnson deficit satisfies

$$0 < x^2 - T^2 = \theta(x+T) < 2hsK.$$

Because $T < x$,

$$n + (K-1) - 2T > (r + 1 - 2s)K - 1 = (s-1)^2 K - 1.$$

Crossing the boundary. Let $t = t_{r,h}$ and $c_{r,h} := t_{r,h}(s-1)^2 - 2hs > 0$. By (13),

$$(T-t)^2 - (n-t)(K-1-t) > c_{r,h}K - t_{r,h}. \tag{19}$$

For sufficiently large K, this is positive and at least $c_{r,h}K/2$; also $t_{r,h} \leq \min\{T, K-2\}$.

Applying the bound below Johnson. Set $N = n - t_{r,h}$, $d_t = K - 1 - t_{r,h}$, and $T_t = T - t_{r,h}$. Rationalizing the shortened Johnson gap gives

$$\eta_t := \frac{T_t}{N} - \sqrt{\frac{d_t}{N}} = \frac{T_t^2 - N d_t}{N(T_t + \sqrt{N d_t})} = \Omega_{r,h}(K^{-1}). \tag{20}$$

d_t/N is bounded above and below by positive constants depending only on r. Therefore $m_{\mathrm{B}} = O_{r,h}(K)$ in (6), and (7) gives $\mathsf{J}(N, d_t, E_{r,h}) = O_{r,h}(K^6)$. Finally, $t_{r,h}$ is fixed and

$$\frac{\binom{n}{t_{r,h}}}{\binom{T}{t_{r,h}}} = O_{r,h}(1).$$

Apply theorem 3.3. □

Remark 3.5. For the first integer budget strictly above the exact Johnson boundary, the sufficient shortening lengths from (16) at rates $1/2, 1/4, 1/8, 1/16$ are $17, 5, 2, 1$, respectively. Larger fixed values can improve concrete constants while preserving the K^6 exponent.

The leading constant can depend strongly on the fixed shortening length. At rate $1/4$, the choice $t = 11$ uniquely minimizes the asymptotic leading constant supplied by this method; the exact statement and calculation are given in section A.

4 Non-asymptotic bounds from MDS circuits

This section develops a second, complementary tool. It applies to every MDS code and every error budget, but it serves a different regime from agreement-set shortening. Near the Johnson boundary at fixed positive rate, the resulting binomial count may be exponential in K; its strength is explicit non-asymptotic control and exact endpoint behavior.

For an $[n, K]$ MDS code, every $K+1$ coordinates support a unique nonzero parity-check relation up to scaling, and no smaller coordinate set does. These minimal dependent coordinate sets are the circuits of the associated code matroid. The argument below counts incidences between bad parameters and rejecting local membership tests supported on such circuits and their supersets.

4.1 Rejecting-test abundance in MDS codes

Every $K+1$ coordinates of an MDS code impose a linear membership test, and the same question may be asked on any $a \geq K+1$ coordinates. For $A \subseteq S$, the test accepts w if $w|_A \in C|_A$ and rejects otherwise. The next lemma is the new combinatorial input: a non-codeword must fail many such tests, and the minimum possible number of failures is exact.

Let C be an $[n, K]$ MDS code, let $S \subseteq L$, and let $w \in \mathbb{F}^S$. For $a \geq K+1$, put

$$\mathcal{R}_a(w; S) := \left\{ A \in \binom{S}{a} : w|_A \notin C|_A \right\}.$$

Lemma 4.1 (Rejecting-test abundance)**.** *Let $m := |S| \geq K+1$ and suppose $w \notin C|_S$. Then, for every $K+1 \leq a \leq m$,*

$$|\mathcal{R}_a(w; S)| \geq \binom{m-1}{a-1}. \tag{21}$$

The bound is sharp for every a.

Proof. It suffices to work with the punctured $[m, K]$ MDS code $C|_S$; we keep the notation C. We use strong induction on m, simultaneously for all $0 \leq K < m$. For $K = 0$, choose a coordinate x with $w(x) \neq 0$. Every a-set containing x rejects.

Assume $K \geq 1$, fix $x \in S$, and put $S' = S \setminus \{x\}$. First suppose $w|_{S'} \in C|_{S'}$. Choose $c \in C$ agreeing with w on S'. Such a codeword exists by assumption. Since $w \notin C$, $c(x) \neq w(x)$. Every a-set A containing x rejects: otherwise a codeword c' agreeing with w on A would agree with c on the $a-1 \geq K$ coordinates of $A \setminus \{x\}$, so the MDS property would force $c = c'$, a contradiction at x. This gives $\binom{m-1}{a-1}$ rejecting sets.

Now suppose $w|_{S'} \notin C|_{S'}$. This case implies $m - 1 \geq K+1$. By induction, at least $\binom{m-2}{a-1}$ rejecting a-sets avoid x, with the term interpreted as zero when $a = m$. By surjectivity of the puncturing map at coordinate x, choose $c \in C$ with $c(x) = w(x)$ and set $v = w - c$. Let

$$C_x := \{d|_{S'} : d \in C,\ d(x) = 0\}.$$

Then C_x is an $[m-1, K-1]$ MDS code and $v|_{S'} \notin C_x$. Moreover, for $B \subseteq S'$,

$$w|_{B \cup \{x\}} \in C|_{B \cup \{x\}} \quad \Longleftrightarrow \quad v|_B \in C_x|_B.$$

Induction applied to C_x gives at least $\binom{m-2}{a-2}$ rejecting a-sets containing x. Pascal's identity proves (21).

For sharpness, take $w = c + e_x$, where $c \in C$ and e_x is nonzero only at x. An a-set omitting x accepts. If an a-set containing x accepted, then its punctured MDS code would contain a nonzero word of weight one, contradicting its minimum distance $a - K + 1 \geq 2$. Thus an a-set rejects exactly when it contains x. □

4.2 The circuit-incidence bound

Theorem 4.2 (Circuit-incidence bound)**.** *Let $C \subseteq \mathbb{F}_q^L$ be an $[n, K]$ MDS code with $1 \le K < n$. Fix $E \in \{0, \dots, n\}$, put $T = n - E$, and define the effective witness threshold*

$$T_{\text{eff}} := \max\{T, K + 1\}.$$

Then

$$B_C(E) \le \min_{K+1 \le a \le T_{\text{eff}}} \left\lfloor \frac{\binom{n}{a}}{\binom{T_{\text{eff}}-1}{a-1}} \right\rfloor. \tag{22}$$

In particular, with $M := \binom{n}{K+1}$,

$$B_C(E) \le \left\lfloor \frac{M}{\binom{T_{\text{eff}}-1}{K}} \right\rfloor \le M. \tag{23}$$

Proof. Fix u_0, u_1. For every bad parameter z, choose one witnessing set S_z. By theorem 2.2, $|S_z| \ge T_{\text{eff}}$ and $u_1|_{S_z} \notin C|_{S_z}$. Fix $a \in \{K + 1, \dots, T_{\text{eff}}\}$. By theorem 4.1, S_z contains at least

$$\binom{|S_z| - 1}{a - 1} \ge \binom{T_{\text{eff}} - 1}{a - 1}$$

a-subsets A on which $u_1|_A \notin C|_A$. For each such A, $u_z|_A \in C|_A$ because $A \subseteq S_z$.

A fixed A is charged by at most one parameter. Indeed, if distinct z, z' both give code restrictions on A, subtraction and division by $z - z'$ imply $u_1|_A \in C|_A$, contradicting rejection. There are only $\binom{n}{a}$ possible a-sets. Double counting proves (22); choosing $a = K + 1$ gives (23). □

The bound is strongest when the agreement threshold is close to the MDS dimension. Two adjacent cases will be used later:

$$T \le K + 1 \quad \Longrightarrow \quad B_C(E) \le M, \tag{24}$$

$$T = K + 2 \quad \Longrightarrow \quad B_C(E) \le \left\lfloor \frac{M}{K + 1} \right\rfloor. \tag{25}$$

4.3 Exact Reed–Solomon behavior at the endpoint

The circuit bound is most informative when the required agreement $T = n - E$ is small. When $T \le K + 1$, an accepting $(K + 1)$-coordinate test supplies the agreement part of a badness witness. For Reed–Solomon codes these tests have an explicit form. This gives a lower bound on $B_C(E)$ that becomes exact when the field is sufficiently large.

Let $C = \mathrm{RS}_{<K}(\mathbb{F}_q, L)$. For a $(K + 1)$-subset $R \subseteq L$, define the divided-difference functional

$$\lambda_R(w) := \sum_{\alpha \in R} \frac{w(\alpha)}{\prod_{\beta \in R \setminus \{\alpha\}} (\alpha - \beta)}. \tag{26}$$

It is the coefficient of X^K in the degree-at-most-K polynomial interpolating $w|_R$. Hence

$$w|_R \in C|_R \quad \Longleftrightarrow \quad \lambda_R(w) = 0. \tag{27}$$

For $g = (\alpha^K)_{\alpha \in L}$,

$$\lambda_R(g) = 1 \qquad \text{for every } R \in \binom{L}{K + 1}. \tag{28}$$

Theorem 4.3 (Bounds when $T \le K+1$)**.** *Let $C = \mathrm{RS}_{<K}(\mathbb{F}_q, L)$ have length n, let $M = \binom{n}{K+1}$, and suppose $T = n - E \le K+1$. Then*

$$\left\lceil \frac{Mq}{q+M-1} \right\rceil \le B_C(E) \le \min\{M, q\}. \tag{29}$$

If $q > \binom{M}{2}$, then

$$B_C(E) = M, \qquad \varepsilon_{\mathrm{mca}}(C, E) = \frac{M}{q}. \tag{30}$$

Proof. Only the lower bounds require proof. Choose $f \in \mathbb{F}_q^L$ uniformly at random and put $Y_R := \lambda_R(f)$ for $R \in \binom{L}{K+1}$. Distinct circuit functionals are distinct: their supports differ and every coefficient in (26) is nonzero. Thus, for $R \neq R'$,

$$\Pr[Y_R = Y_{R'}] = \frac{1}{q}.$$

If X counts colliding unordered pairs, then $\mathbb{E}[X] = \binom{M}{2}/q$, so some f satisfies $X \le \binom{M}{2}/q$.

Let D be the number of distinct values among the Y_R's, with multiplicities $m_1, \dots, m_D$. Then

$$\sum_i m_i = M, \qquad \sum_i m_i^2 = M + 2X \le \frac{M(q+M-1)}{q}.$$

Cauchy–Schwarz gives $D \ge Mq/(q+M-1)$. For each distinct value y, take a set R with $Y_R = y$ and set $z = -y$ on the affine line $u_z = f + zg$. Then $\lambda_R(u_z) = 0$, so $u_z|_R \in C|_R$, while $\lambda_R(g) = 1$, so the direction $g|_R$ is not in $C|_R$. Since $|R| = K+1 \ge T$, theorem 2.2 makes each of these D parameters bad.

If $q > \binom{M}{2}$, then $\mathbb{E}[X] < 1$. Some f has $X = 0$, giving M distinct bad parameters. The upper bound (24) proves equality. □

The construction above uses the Reed–Solomon monomial direction in (28). Large-field endpoint exactness is nevertheless an MDS phenomenon, as the next proposition shows. It is not needed for the challenge applications, and its union-bound field condition is slightly stronger than the Reed–Solomon-specific one.

Proposition 4.4 (MDS exactness over large fields)**.** *Let C be any $[n, K]$ MDS code with $1 \le K < n$, put $M = \binom{n}{K+1}$, and suppose*

$$q > \max\left\{ M, \binom{M}{2} \right\}.$$

Then $B_C(E) = M$ whenever $T = n - E \le K+1$.

Proof. For each $(K+1)$-set R, let h_R be a nonzero parity-check functional for $C|_R$, extended by zero outside R. Its support is exactly R, so the h_R are pairwise nonproportional. Choose u_1 outside the union of the M hyperplanes $h_R(u_1) = 0$. For each pair $R \neq R'$, equality of

$$-\frac{h_R(u_0)}{h_R(u_1)} \quad \text{and} \quad -\frac{h_{R'}(u_0)}{h_{R'}(u_1)}$$

is a proper hyperplane condition on u_0. Choose u_0 outside all $\binom{M}{2}$ collision hyperplanes. The field-size assumptions and union bounds guarantee both choices. The resulting M distinct roots are bad, and (24) is the matching upper bound. □

Corollary 4.5 (Adjacent integer-budget threshold)**.** *Fix $1 \le K \le n-2$ and $\lambda \ge 1$, and put*

$$M := \binom{n}{K+1}, \qquad U := \left\lfloor \frac{M}{K+1} \right\rfloor.$$

Suppose

$$q > \binom{M}{2}, \qquad 2^{\lambda} U \le q < 2^{\lambda} M. \tag{31}$$

Then, for $C = \mathrm{RS}_{<K}(\mathbb{F}_q, L)$,

$$\varepsilon_{\mathrm{mca}}(C, E) \le 2^{-\lambda} \quad \Longleftrightarrow \quad E \le n - K - 2.$$

Consequently,

$$E^*_{\lambda}(C) = n - K - 2, \qquad \sup\{\delta : \varepsilon_{\mathrm{mca}}(C, \delta) \le 2^{-\lambda}\} = \frac{n-K-1}{n},$$

and the real endpoint is not attained.

Proof. For $E \le n-K-2$, one has $T \ge K+2$, and theorem 4.2 with $a = K+1$ gives $B_C(E) \le U$. For $E \ge n-K-1$, one has $T \le K+1$, and theorem 4.3 gives $B_C(E) = M$. Apply (31) and (5). □

4.4 Combining the two upper bounds

For $C = \mathrm{RS}_{<K}(\mathbb{F}_q, L)$, $E > 0$, $T = n - E$, and $T_{\mathrm{eff}} = \max\{T, K+1\}$, the two independent methods give

$$B_C(E) \le \min\left\{ \min_{K+1 \le a \le T_{\mathrm{eff}}} \left\lfloor \frac{\binom{n}{a}}{\binom{T_{\mathrm{eff}}-1}{a-1}} \right\rfloor, \min_{\substack{0 \le t \le \min\{T, K-2\} \\ (T-t)^2 > (n-t)(K-1-t)}} \frac{\binom{n}{t}}{\binom{T}{t}} \mathsf{J}(n-t, K-1-t, E) \right\}. \tag{32}$$

The second minimum is $+\infty$ when no t is admissible. The two terms have different purposes: the shortening term yields the polynomial near-Johnson estimate of theorem 3.4, whereas the circuit term dominates in the small-agreement regime and supplies the exact thresholds for the concrete codes below.

5 Consequences for the Grand MCA Challenge

The challenge-scale certificates below use agreement-set shortening. The exact length-64 crossings instead combine the MDS circuit upper bound with the matching Reed–Solomon endpoint construction. For $B_C(E) > 0$, define the MCA security at budget E by

$$s_C(E) := \log_2 \frac{q}{B_C(E)}.$$

A lower bound on $s_C(E)$ is equivalent to an upper bound on the MCA error. We set $s_C(E) = +\infty$ when $B_C(E) = 0$.

5.1 Challenge-scale parameters over a common field

Define

$$Q := (2^{128} - 255)2^{128} + 1 = 2^{256} - 255 \cdot 2^{128} + 1. \tag{33}$$

The displayed expression shows that $Q < 2^{256}$ and $v_2(Q-1) = 128$, where v_2 is the exponent of 2 in an integer. Section B certifies primality using Proth's theorem.

Theorem 5.1 (Certified post-Johnson budgets)**.** *Let $K = 2^{18}$. For each $r \in \{2, 4, 8, 16\}$, set $n = rK$, let $L = H_n \subseteq \mathbb{F}_Q^\times$, and put*

$$C_r := \mathrm{RS}_{<K}(\mathbb{F}_Q, L), \qquad E_r := \lfloor E_J(n, K) \rfloor + 1.$$

Then E_r is the first integer budget strictly above the exact Johnson boundary $E_J(n, K)$ and

$$\varepsilon_{\mathrm{mca}}(C_r, E_r) < 2^{-128} \tag{34}$$

for all four rates. The parameters satisfy $K < 2^{40}$, $Q < 2^{256}$, and the evaluation domains are smooth. Moreover, for the rate-1/8 code,

$$E_8^{(2)} := \lfloor E_J(8K, K) \rfloor + 2 = 1{,}355{,}700$$

is the second integer budget strictly above the exact Johnson boundary and

$$\varepsilon_{\mathrm{mca}}(C_8, E_8^{(2)}) < 2^{-128}. \tag{35}$$

Rate	Budget	n	E	t	$\log_2 B_C(E)$	$s_C(E)$
1/2	first	2^{19}	153,562	29	< 127.950275	> 128.049725
1/4	first	2^{20}	524,290	11	< 124.377940	> 131.622060
1/8	first	2^{21}	1,355,699	6	< 124.091663	> 131.908337
1/8	second	2^{21}	1,355,700	8	< 126.631006	> 129.368994
1/16	first	2^{22}	3,145,731	5	< 126.367700	> 129.632300

Table 1: The first integer budget beyond Johnson at all four target rates and the second budget at rate 1/8, over the common prime field $\mathbb{F}_Q$. The column t is the shortening length used in theorem 3.3. The final two columns give, respectively, a certified upper bound on $\log_2 B_C(E)$ and a certified lower bound on $s_C(E) = \log_2 Q - \log_2 B_C(E)$.

Proof. The Proth certificate and factorization of $Q - 1$ prove the field and subgroup claims. For the four first-budget rows, exact integer comparisons verify

$$(n - E_r)^2 < n(K-1) \le (n - E_r + 1)^2. \tag{36}$$

The second rate-1/8 budget is $E_8^{(2)} = E_8 + 1$. For each of the five rows, with its displayed E and t, one also has

$$(n - E - t)^2 > (n - t)(K - 1 - t).$$

Thus theorem 3.3 applies. For each row, the exact comparison

$$2^{128} \frac{\binom{n}{t}}{\binom{n-E}{t}} \mathsf{J}(n - t, K - 1 - t, E) < Q$$

is certified by rational square-root bounds as described in section B. The decimal logarithms in table 1 are not used in the proof. □

5.2 Exact length-64 thresholds

For $K \in \{32, 16, 8, 4\}$, define

$$q_{32} = (2^{93} - 231)2^{93} + 1, \qquad q_{16} = (2^{88} - 223)2^{89} + 1,$$
$$q_8 = (2^{80} - 31)2^{81} + 1, \qquad q_4 = (2^{75} - 321)2^{75} + 1.$$

Section B certifies these numbers prime using Proth's theorem; each contains the order-64 subgroup H_{64}. The next theorem gives exact crossings: the target holds at one integer budget and fails at the immediately following budget.

Theorem 5.2 (Exact 2^{-128} thresholds)**.** *For each row of table 2, let* $C = \mathrm{RS}_{<K}(\mathbb{F}_{q_K}, H_{64})$. *Then*

$$\varepsilon_{\mathrm{mca}}(C, \delta) \le 2^{-128} \iff 0 \le \delta < \frac{E_{\mathrm{bad}}}{64}. \tag{37}$$

Equivalently, E_{safe} *is the largest safe integer budget,* $E_{\mathrm{bad}} = E_{\mathrm{safe}} + 1$ *is unsafe, and* $E_{\mathrm{bad}}/64$ *is the nonattained supremal real threshold.*

Rate	K	q_K bit length	E_J^{in}	E_{safe}	E_{bad}	steps beyond Johnson	security at safe / bad
1/2	32	186	19	30	31	11	130.420/125.376
1/4	16	177	33	46	47	13	130.795/126.707
1/8	8	161	42	54	55	12	129.489/126.319
1/16	4	150	50	58	59	8	129.460/127.138

Table 2: Exact integer-budget thresholds at length 64. $E_J^{\mathrm{in}} = \lceil 64 - \sqrt{64(K-1)} \rceil - 1$ is the largest integer budget strictly below the Johnson boundary $E_J(64, K)$. The q_K bit length is $\lfloor \log_2 q_K \rfloor + 1$, and the number of steps beyond Johnson is $E_{\mathrm{safe}} - E_J^{\mathrm{in}}$. The final column gives the lower bound $\log_2(q_K/U)$ at the safe point and the exact value $\log_2(q_K/M)$.

Proof. For every row, exact arithmetic verifies

$$q_K > \binom{M}{2}, \qquad 2^{128}U \le q_K < 2^{128}M, \quad M = \binom{64}{K+1}, \quad U = \left\lfloor \frac{M}{K+1} \right\rfloor.$$

Primality and $64 \mid (q_K - 1)$ are certified in table 3. Apply theorem 4.5. The security values are decimal summaries of the exact integer comparisons. □

5.3 All-radius bounds from large fields

If $2^{128}\binom{n}{K+1} < q$, the circuit bound alone puts the MCA error below 2^{-128} at every radius. The following examples show this effect.

Proposition 5.3 (All-radius examples)**.** *Let* Q *be as in* (33)*, let* $n = 128$*, and let* $K \in \{64, 32, 16, 8\}$. *For* $C = \mathrm{RS}_{<K}(\mathbb{F}_Q, H_{128})$,

$$\varepsilon_{\mathrm{mca}}(C, \delta) < 2^{-128} \qquad \text{for every } \delta \in [0, 1].$$

Thus every real radius is safe, and the largest is 1.

Proof. For each listed K, exact arithmetic gives

$$2^{128}\binom{128}{K+1} < Q.$$

The claim follows from (23), uniformly in E. □

5.4 Discussion and limitations

The two application families answer different questions. The length-64 examples determine the 2^{-128} crossing exactly, but the fields were chosen so that q_K lies between $2^{128}U$ and $2^{128}M$, producing a safe budget followed immediately by an unsafe one. The challenge-scale examples use one common field and certify the first integer budget beyond Johnson at all four target rates, and the second budget at rate 1/8; they do not provide matching unsafe-side converses at the next integer budgets.

The circuit estimate also exposes a basic regime in which field size makes every radius trivially safe. For every error budget,

$$\varepsilon_{\mathrm{mca}}(C, E) \le \frac{\binom{n}{K+1}}{q}.$$

Thus, if $\binom{n}{K+1} \le q2^{-\lambda}$, every radius meets the target for elementary counting reasons, as in theorem 5.3. A challenge instance intended to have a nontrivial threshold must rule out this regime, or otherwise constrain the relation among n, K, and $\log q$.

MCA is only one term in proof-system soundness. Interleaved list size, sampling error, alphabet size, and commitment costs remain separate. The statements here are coding-theoretic certificates, not complete protocol parameter sets.

The main unresolved problem is asymptotic: obtain a positive constant relative improvement beyond Johnson for Reed–Solomon codes on a prescribed smooth subgroup while keeping the bad-parameter count sufficiently small. Shortening $\Theta(n)$ coordinates incurs an exponential transfer factor in general, whereas fixed shortening moves the relative radius by only $O(1/n)$. Progress therefore requires new structural information about agreement sets on smooth domains.

Acknowledgement

AI usage disclosure. ChatGPT was used for exploratory discussions and to identify potentially relevant formulas and results from prior work. OpenAI Codex was used to assist with manuscript preparation, including editing, reorganization, consistency checks, and LaTeX maintenance, and with implementing computational checks of the concrete parameter bounds and exact-arithmetic certificates reported in the paper. The author independently verified all mathematical arguments, cited references, and computational results, and takes full responsibility for the paper's contents and correctness.

References

[ABF26] G. Arnon, D. Boneh, and G. Fenzi. Open problems in list decoding and correlated agreement. *IACR Cryptology ePrint Archive*, Paper 2026/680, 2026. https://eprint.iacr.org/2026/680.

[ACFY25] G. Arnon, A. Chiesa, G. Fenzi, and E. Yogev. WHIR: Reed–Solomon proximity testing with super-fast verification. In *Advances in Cryptology–EUROCRYPT 2025*, LNCS 15604, pages 214–243, 2025. https://doi.org/10.1007/978-3-031-91134-7_8.

[BCHKS25] E. Ben-Sasson, D. Carmon, U. Haböck, S. Kopparty, and S. Saraf. On proximity gaps for Reed–Solomon codes. *ECCC* TR25-169 and *IACR Cryptology ePrint Archive*, Paper 2025/2055, 2025. https://eccc.weizmann.ac.il/report/2025/169/. https://eprint.iacr.org/2025/2055.

[BCIKS20] E. Ben-Sasson, D. Carmon, Y. Ishai, S. Kopparty, and S. Saraf. Proximity gaps for Reed–Solomon codes. In *Proceedings of the 61st IEEE Symposium on Foundations of Computer Science (FOCS 2020)*, pages 900–909, 2020. https://doi.org/10.1109/FOCS46700.2020.00088.

[Cho26] P. Chojecki. Universal field-size caps and a two-sided sandwich for mutual correlated agreement on smooth Reed–Solomon domains. Working manuscript, version 12, July 2026. https://github.com/przchojecki/rs-mca/blob/0f3f562082c7ea8099100950167fc34532d3f48c/cs25_cap_v12.pdf.

[CS25] E. Crites and A. Stewart. On Reed–Solomon proximity gaps conjectures. *IACR Cryptology ePrint Archive*, Paper 2025/2046, 2025. https://eprint.iacr.org/2025/2046.

[DMP21] A. A. Davydov, S. Marcugini, and F. Pambianco. On the weight distribution of the cosets of MDS codes. *arXiv:2101.12722*, 2021. https://doi.org/10.48550/arXiv.2101.12722.

[GG25] R. Goyal and V. Guruswami. Optimal proximity gaps for subspace-design codes and (random) Reed–Solomon codes. *IACR Cryptology ePrint Archive*, Paper 2025/2054, 2025. https://eprint.iacr.org/2025/2054.

[GGSW26] R. Goyal, V. Guruswami, Y. Sun, and M. Wootters. Locality of curve-decoding and improved proximity gaps. *arXiv:2607.08516*, 2026. https://doi.org/10.48550/arXiv.2607.08516.

[Hab25] U. Haböck. A note on mutual correlated agreement for Reed–Solomon codes. *IACR Cryptology ePrint Archive*, Paper 2025/2110, 2025. https://eprint.iacr.org/2025/2110.

[Jo26] S. Jo. Interleaving stability for mutual correlated agreement and curve decodability. *IACR Cryptology ePrint Archive*, Paper 2026/891, 2026. https://eprint.iacr.org/2026/891.

[Joh62] S. M. Johnson. A new upper bound for error-correcting codes. *IRE Transactions on Information Theory*, 8(3):203–207, 1962. https://doi.org/10.1109/TIT.1962.1057714.

[KKH26] D. Krachun, S. Kazanin, and U. Haböck. Failure of proximity gaps close to capacity. *IACR Cryptology ePrint Archive*, Paper 2026/782, 2026. https://eprint.iacr.org/2026/782.

[Pro78] F. Proth. Théorèmes sur les nombres premiers. *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, 87:926, 1878.

A Optimizing the shortening length at rate 1/4

The following specialization explains the choice $t = 11$ used in the rate-1/4 concrete certificate. It is not needed for the qualitative $O_{r,h}(K^6)$ theorem.

Corollary A.1 (Rate 1/4: optimized fixed shortening)**.** *Let $m \geq 13$, let $|L| = 4m$, and put $C_m = \mathrm{RS}_{<m}(\mathbb{F}, L)$. The first integer error budget strictly above the exact Johnson boundary is $E = 2m + 2$, and*

$$B_{C_m}(2m+2) \leq \frac{\binom{4m}{11}}{\binom{2m-2}{11}} \mathsf{J}(4m-11, m-12, 2m+2) = O(m^6). \tag{38}$$

Among fixed integers $t > 4$, the choice $t = 11$ uniquely minimizes the asymptotic leading constant supplied by this method.

Proof. The Johnson boundary in error units is $E_J(4m, m) = 4m - 2\sqrt{m(m-1)}$, which lies strictly between $2m+1$ and $2m+2$. Thus $T = 2m - 2$. For a fixed $t > 4$,

$$(T-t)^2 - (4m-t)(m-1-t) = (t-4)m + 3t + 4. \tag{39}$$

Taking $t = 11$ gives a positive surplus $7m + 37$, and (38) follows from theorem 3.3.

For completeness, (20) and (39) give

$$\eta_t = \frac{t-4}{16m} + O(m^{-2}), \qquad m_{\mathrm{B}} = \frac{8m}{t-4} + O(1).$$

Substitution in (7), together with $\binom{4m}{t}/\binom{2m-2}{t} = 2^t + O(m^{-1})$, gives leading term

$$\left(\frac{2^{t+21}}{3(t-4)^5} + o(1) \right) m^6.$$

The ratio of consecutive leading constants is $2((t-4)/(t-3))^5$; it is below one at $t = 10$, above one at $t = 11$, and increases thereafter. □

B Exact arithmetic certificates

All comparisons used in theorems 5.1 to 5.3 can be verified without floating point.

B.1 Proth certificates

Every integer q listed in table 3 has the form $q = k2^s + 1$, with k odd and $k < 2^s$. Proth's theorem [Pro78] states that

$$w^{(q-1)/2} \equiv -1 \pmod{q}$$

certifies primality.

B.2 Exact evaluation below the Johnson boundary

Recall the parameters m_{B}, x_{B}, and $\mathsf{J}(N, d, E)$ from (6)–(7).

For shortened parameters (N, d, E), put $A = N - E$. When the ceiling in (6) is greater than 3, a proposed integer m_{B} is certified by

$$(m_{\mathrm{B}} - 1)^2 A^2 < d\, m_{\mathrm{B}}^2 N, \qquad d(m_{\mathrm{B}} + 1)^2 N \leq m_{\mathrm{B}}^2 A^2. \tag{40}$$

Use	K	prime $q = k2^s + 1$	s	witness w
length 64, rate 1/2	32	$(2^{93} - 231)2^{93} + 1$	93	3
length 64, rate 1/4	16	$(2^{88} - 223)2^{89} + 1$	89	5
length 64, rate 1/8	8	$(2^{80} - 31)2^{81} + 1$	81	11
length 64, rate 1/16	4	$(2^{75} - 321)2^{75} + 1$	75	3
common field	–	$(2^{128} - 255)2^{128} + 1$	128	3

Table 3: Prime fields and Proth witnesses. In each short-code row, $64 \mid q - 1$; for the common field, $v_2(q - 1) = 128$.

These inequalities are equivalent to

$$\frac{m_{\mathrm{B}} - 1}{m_{\mathrm{B}}} \frac{A}{N} < \sqrt{\frac{d}{N}} \leq \frac{m_{\mathrm{B}}}{m_{\mathrm{B}} + 1} \frac{A}{N}.$$

If $m_{\mathrm{B}} = 3$, one instead directly verifies that the ratio in (6) is at most 3. The five values of m_{B} in table 1, in table order, are

$$427{,}898, \qquad 299{,}571, \qquad 268{,}638, \qquad 252{,}017, \qquad 226{,}714.$$

Choose a rational $L_0 > 0$ with $L_0^2 < d/N$. Keeping d/N exact and replacing only the positive square-root denominators in (7) gives

$$\mathsf{J}(N, d, E) < N \frac{2x_{\mathrm{B}}^5 + 3x_{\mathrm{B}}(E/N)(d/N)}{3L_0^3} + \frac{x_{\mathrm{B}}}{L_0}. \tag{41}$$

For the five instances in table 1, the 40-decimal truncation of $\sqrt{d/N}$ is a certified strict lower bound and makes the right-hand side rational. Multiplication by the exact binomial ratio then reduces every security claim to an integer comparison.