A PINCER, SPARSE, AND CERTIFICATE PICTURE FOR THE MUTUAL CORRELATED AGREEMENT THRESHOLD

PRZEMEK CHOJECKI

Abstract. For Reed–Solomon codes with $k \le 2^{40}$ and $|\mathbb{F}| < 2^{256}$ — the parameter box singled out by the Proximity Prize — we give a sharpened pincer picture for the grand mutual correlated agreement threshold $\delta^*_C(2^{-128})$. For $|\mathbb{F}| < 2^{128}$ the threshold is exactly 0. For $|\mathbb{F}| \ge 2^{128}$ and the four challenge rates, ordinary locator-prefix floors already force plain correlated-agreement failure from $\delta = 1 - \rho - s_\rho/n$ up to capacity, where $s_\rho = \lceil \alpha_\rho n \rceil$ and $\alpha_{1/2} = 1/300$, $\alpha_{1/4} = 3/1000$, $\alpha_{1/8} = 41/20000$, $\alpha_{1/16} = 3/2500$; in particular the old near-capacity problem has a negative answer on an explicit upper slice of its band. On the safe side, a self-contained theorem gives MCA with error $(\lfloor \delta n \rfloor + 1)/q$ below one third of the distance, an elementary half-Johnson certificate improves that self-contained edge in low-rate rows, and the unique-decoding proximity gap of Ben-Sasson–Carmon–Ishai–Kopparty–Saraf raises the safe frontier to one half of the distance whenever $|\mathbb{F}| \ge 2^{128} n$. We then integrate the sparse band reductions: the mutual-only layer is exactly the maximum of the sparse layer $\sigma_C(\delta)/q$ and plain CA, non-tangent sparse witnesses have an explicit Reed–Solomon normal form and budget-rigidity constraint, and in the sub-half-radius part of the residual plain-CA band a radius-free rider argument reduces failures to deficient interleaved pair lists for doubly sparse far pairs. The half-distance wall is sharp, and the remaining threshold problem is reduced to a middle plain-CA band together with a sparse, budget-restricted value-set problem. Finally, a companion certificate framework turns these bounds into finite row certificates for deployed multiplicative, circle, and genus-one/rational-smooth rows.

1. Introduction and main result

The Proximity Prize [PP26] and the challenge collection of Arnon, Boneh and Fenzi [ABF26] ask for the largest proximity parameter δ at which mutual correlated agreement (MCA) holds for a Reed–Solomon code with error at most a stated target, and single out one parameter box: *"we are mostly interested in determining δ^*_C when $L \subseteq \mathbb{F}$ is a smooth domain, $k \le 2^{40}$, and $|\mathbb{F}| < 2^{256}$."* This paper gives a pincer answer for that box: a certified safe region, a certified unsafe region strictly below capacity, and an exact formulation of the residual kernel. Write $C = \mathrm{RS}[\mathbb{F}, D, k]$ for the code of polynomials of degree less than k evaluated on a domain D of size n, $\rho = k/n$, $q = |\mathbb{F}|$, and let $\delta^*_C(\varepsilon^*)$ be the threshold of Definition 2.1 below, at the grand challenge target $\varepsilon^* = 2^{-128}$.

This note is deliberately organized around the companion cap manuscript [Cho26b], which is the main Proximity Prize submission document in the RS–MCA package. The role of the present note is narrower: it extracts the threshold pincer, sparse residual layer, and certificate target from that main paper, so that the remaining proof obligations can be audited without duplicating the full scanner, transport, and deployed-row certificate sections. Consequently, the hypotheses, endpoint conventions, denominators, and final submission claims should be read from [Cho26b]; this note is a compact roadmap and theorem companion, not a competing authority.

Date: July 2, 2026.

Theorem 1.1. *Let $q = |\mathbb{F}| < 2^{256}$, let $D \subseteq \mathbb{F}^\times$ be a coset of a cyclic subgroup of even order n, and let $C = \mathrm{RS}[\mathbb{F}, D, k]$ with $\rho = k/n \in \{\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}\}$, $k \le 2^{40}$ and $n \ge 2^{15}$. Put*

$$\alpha_\rho := \begin{cases} 1/300, & \rho = \frac{1}{2}, \\ 3/1000, & \rho = \frac{1}{4}, \\ 41/20000, & \rho = \frac{1}{8}, \\ 3/2500, & \rho = \frac{1}{16}, \end{cases} \qquad s_\rho := \lceil \alpha_\rho n \rceil,$$

and put $g_\rho := 2^{-9}$ for $\rho \ge \frac{1}{8}$ and $g_\rho := 2^{-10}$ for $\rho = \frac{1}{16}$.

1. *If $q < 2^{128}$, then $\delta^*_C(2^{-128}) = 0$.*
2. *If $q \ge 2^{128}$, then*
$$\delta^*_C(2^{-128}) \le 1 - \rho - \frac{s_\rho}{n}.$$
More strongly, $\varepsilon_{\mathrm{ca}}(C, \delta) > 2^{-128}$, and hence $\varepsilon_{\mathrm{mca}}(C, \delta) > 2^{-128}$, for every $\delta \in [1 - \rho - s_\rho/n, 1 - \rho)$. Since $s_\rho/n \ge \alpha_\rho > g_\rho$, this gives a negative answer to the original plain-CA question on the nonempty upper slice $[1 - \rho - s_\rho/n,\ 1 - \rho - g_\rho)$ of its band.
3. *If moreover $q \ge 2^{128} n$, then unconditionally $\frac{1}{n}\lfloor \frac{n-k}{3} \rfloor \le \delta^*_C(2^{-128}) \le 1 - \rho - s_\rho/n$, a determination within a multiplicative factor smaller than three; and, using additionally the unique-decoding proximity gap of* [BCIKS20], *$\frac{1}{n}\lfloor \frac{n-k}{2} \rfloor \le \delta^*_C(2^{-128}) \le 1 - \rho - s_\rho/n$, a determination within a factor smaller than two.*
4. *If $2^{128} \le q < 2^{128} n$, the same upper bound holds, and the unconditional lower bound is r^*/n with $r^* := \min\big(\lfloor (n-k)/3 \rfloor, \lfloor 2^{-128} q \rfloor - 1\big)$, which degrades to 0 as q approaches 2^{128}; no factor claim is made in this thin regime.*

Every ingredient except the single import in (3) is proved here from first principles: a graded locator-prefix pigeonhole (Lemma 3.1), a deep-point list-to-correlated-agreement conversion (Theorem 3.2), an ordinary locator-prefix specialization that resolves the top of the plain-CA band (Corollary 3.4), a deep-regime theorem showing MCA *holds* with error $(\lfloor \delta n \rfloor + 1)/q$ below one third of the minimum distance for every linear code (Theorem 4.1), and a theorem showing that below one half of the distance mutual and plain correlated agreement coincide up to an explicit tangent term (Theorem 4.2). The sparse reductions of Section 7 then sharpen the residual kernel: MCA is exactly the maximum of plain CA and a sparse mutual layer, the sparse layer has a Reed–Solomon normal form with a budget-rigidity constraint, and the sub-half-radius part of the remaining plain-CA problem reduces to deficient interleaved pair lists for doubly sparse far pairs. No value-set counting, exponential-sum estimate, or equidistribution input is used. The one import, [BCIKS20, Thm. 4.1], is a published theorem, so clause (3) stands on the literature as stated; we track it separately only to delimit the self-contained core. Section 8 then proves two barriers — an entropy envelope past which no prefix floor can certify failure (Proposition 8.1), and a ceiling of $\frac{1}{k}$ on the error certifiable through the conversion (Proposition 8.2) — and states the residual kernel after the two broad band questions are sharpened: a smaller plain-CA interval (Problem 8.5) and the sparse mutual obstruction (Problem 8.4). Remarks 3.7–3.8 complete the parameter box: characteristic-two additive smooth domains and odd 3-smooth orders satisfy the same baseline bounds, small n down to 2^{12} retains a nonvacuous cap of gap $3/n$, and rates outside the four challenge values are covered by the same finite criterion.

The upper bounds sharpen, and the composition follows, a line of work on capacity-edge obstructions: the conditional universal cap of [Cho26b] (gap 2^{-11} under $|\mathbb{F}| \ge 2n$), the locator framework of [Cho26a], and the conversion perspective of [CS25]; the strongest known positive results for plain correlated agreement are [BCIKS20, BCHKS25], reaching the Johnson radius. A companion manuscript [Cho26b] develops the deployed-parameter refinements (subfield-pigeonhole floors widening the unsafe frontier to gap $\approx 2^{-4.96}$ at $n = 2^{21}$, circle and genus-one rows, explicit witnesses) and the structured form of the remaining problem. To keep this note compact, we record the following companion certificate refinements rather than reproducing the long scanner and transport sections.

Proposition 1.2 (companion certificate refinements for threshold determination)**.** *Fix a target $\varepsilon^* \in (0,1)$. The following consequences of the companion paper* [Cho26b] *may be combined with Theorem 1.1.*

(1) (Self-contained half-Johnson safe edge.) *Let $C = \mathrm{RS}[\mathbb{F}, D, k]$, let $r \geq 0$, and put*

$$J_2(r) := \frac{n\,(n-2r-k+1)}{(n-2r)^2-(k-1)n}.$$

If $n-2r>0$, $(n-2r)^2 > (k-1)n$, and

$$1 + (r+1)J_2(r) \leq \varepsilon^* q,$$

then $\delta_C^*(\varepsilon^*) \geq r/n$. Asymptotically this gives an import-free safe edge at $\delta \approx (1-\sqrt{\rho})/2$, so the self-contained lower edge in Theorem 1.1 may be replaced by

$$\max\left\{\frac{1}{n}\left\lfloor\frac{n-k}{3}\right\rfloor, \frac{r_{\mathrm{hJ}}}{n}\right\},$$

where r_{hJ} is the largest integer satisfying the displayed half-Johnson certificate.

(2) (Finite staircase certificates.) *For a fixed finite-slope line field F_{line}, write $q_{\mathrm{line}} := |F_{\mathrm{line}}|$, and let $B_{\mathrm{mca}}(a)$ be the maximum number of MCA-bad line parameters with an agreement witness of size at least a. Then, at the closed integer radius $\delta = 1 - a/n$,*

$$\varepsilon_{\mathrm{mca}}(C, 1-a/n) = \frac{B_{\mathrm{mca}}(a)}{q_{\mathrm{line}}}.$$

Thus determining $\delta_C^*(\varepsilon^*)$ is an integer-staircase problem: find the first agreement a for which

$$B_{\mathrm{mca}}(a) \leq \varepsilon^* q_{\mathrm{line}}.$$

A one-step certificate

$$B_{\mathrm{mca}}(a_0) > \varepsilon^* q_{\mathrm{line}}, \qquad B_{\mathrm{mca}}(a_0+1) \leq \varepsilon^* q_{\mathrm{line}}$$

pins the threshold to the adjacent closed-ball endpoint $\delta = 1 - a_0/n$ in the usual supremum convention. More generally, a row certificate consists of an unsafe prefix/rational-floor handle and a safe handle (deep, half-Johnson, or the single imported half-distance CA theorem)*. Once its integer inequalities are checked, it proves a concrete interval*

$$\frac{r_{\mathrm{safe}}}{n} \leq \delta_C^*(\varepsilon^*) \leq 1 - \frac{a_{\mathrm{unsafe}}}{n}.$$

If the unsafe and safe certificates occur at consecutive agreements, they determine the threshold to one integer step. In particular, for the KoalaBear sextic row at target 2^{-128},

$$\delta_C^*(2^{-128}) \in \left[\tfrac{349525}{2^{21}}, \tfrac{15331}{32768}\right], \quad \textit{self-contained,}$$
$$\delta_C^*(2^{-128}) \in \left[\tfrac{1}{4}, \tfrac{15331}{32768}\right], \quad \textit{with the imported half-distance theorem.}$$

The optimized unsafe handle behind the KoalaBear upper edge is

$$(c, m, w, \Delta) = (16, 69748, 4211, 67392), \qquad 1 - \frac{mc}{n} = 1 - \frac{16\cdot 69748}{2^{21}} = \frac{15331}{32768}.$$

Here Δ is the checked surplus in the companion certificate. The same certificate framework applies to map-smooth, circle, and genus-one/rational-smooth rows after the transports proved in [Cho26b].

(3) (Failure profile.) *Let $T = \frac{1}{k}(1-\frac{n}{q})$ and suppose a list floor gives $L \geq 1 + \kappa q T$ at an integer-admissible radius. Then*

$$\varepsilon_{\mathrm{ca}}(C, \delta) \geq \frac{\kappa}{\kappa+1} T,$$

and hence MCA failure follows on the same monotone interval. This does not move the right edge of δ^*, but it improves the failure margin; at the KoalaBear first staircase step one has $\kappa \geq 2^{54}$.

Justification. Clause (1) is the elementary half-Johnson CA theorem of [Cho26b]: two bad slopes recover a pair-list at agreement $n-2r$, the pair-interleaved Johnson bound gives $J_2(r)$, and the pincer from CA to MCA transfers the result below half the distance. Clause (2) is the finite scanner/certificate closure of [Cho26b]: the function $B_{\mathrm{mca}}(a)$ is exactly the retained bad-slope numerator at agreement a, unsafe handles are prefix or rational floors composed with the deep-point conversion, and safe handles are the deep, half-Johnson, or imported half-distance certificates. The KoalaBear interval and handle are the exact integer certificates printed there. Clause (3) is the optimized form of the same deep-point conversion: rearranging its dichotomy with $\eta = \varepsilon_{\mathrm{ca}}/T$ gives the factor $\kappa/(\kappa+1)$. □

Remark 1.3 (a second row-certificate example). For the Mersenne-31 circle line-round row at target 2^{-100}, [Cho26b] gives the parallel intervals

$$\delta_C^* \in \left[\tfrac{349525}{2^{21}}, \tfrac{30663}{65536}\right], \quad \text{self-contained},$$
$$\delta_C^* \in \left[\tfrac{1}{4}, \tfrac{30663}{65536}\right], \quad \text{with the import.}$$

The present paper is therefore the minimal self-contained core plus the residual reductions needed to state the current picture; Proposition 1.2 records the compact row-determination upgrades that are better left as citations to the companion paper.

2. Definitions

Throughout, $\mathbb{F}$ is a finite field, $q = |\mathbb{F}|$, $D \subseteq \mathbb{F}$ has $|D| = n$, and $C = \mathrm{RS}[\mathbb{F}, D, k] := \{p|_D : p \in \mathbb{F}[X],\ \deg p < k\}$ with $1 \le k < n$, and write $\rho := k/n$, so C is linear of dimension k and minimum Hamming weight $n-k+1$. For $u, v \in \mathbb{F}^D$, $\mathrm{dist}(u,v)$ is the relative Hamming distance, and for a set $C' \subseteq \mathbb{F}^D$, $\mathrm{dist}(u,C') := \min_{c\in C'} \mathrm{dist}(u,c)$ and $\Lambda(C',\delta,u) := \{c \in C' : \mathrm{dist}(u,c) \le \delta\}$. For a pair $(f_1,f_2) \in \mathbb{F}^D \times \mathbb{F}^D$ the column distance to $C^{\equiv 2} := C \times C$ is $\mathrm{dist}_2\big((f_1,f_2), C^{\equiv 2}\big) := \min_{c_1,c_2\in C} \frac{1}{n}\#\{j : (f_1(j),f_2(j)) \ne (c_1(j),c_2(j))\}$. All slopes are finite: lines are $\gamma \mapsto f_1 + \gamma f_2$, $\gamma \in \mathbb{F}$.

Fix $\delta \in (0,1)$ and write $r := \lfloor \delta n \rfloor$ when an integer radius is needed. A slope γ is *δ-CA-bad* for the pair (f_1,f_2) if the point $f_1 + \gamma f_2$ is δ-close to C while the pair is δ-far in columns, $\mathrm{dist}_2\big((f_1,f_2), C^{\equiv 2}\big) > \delta$. A *proximity witness* for γ is a pair (c,S) with $c \in C$, $S \subseteq D$, $|S| \ge (1-\delta)n$, and $(f_1+\gamma f_2)|_S = c|_S$; the witness *extends mutually* if some $(c_1,c_2) \in C^{\equiv 2}$ has $f_i|_S = c_i|_S$ for $i = 1,2$, and *fails* otherwise. Following [ABF26, Defs. 4.1, 4.3], a slope γ is *δ-MCA-bad* for (f_1,f_2) if some proximity witness for γ fails. The two errors are

$$\varepsilon_{\mathrm{ca}}(C,\delta) := \max_{(f_1,f_2)} \tfrac{1}{q}\#\{\gamma \ \delta\text{-CA-bad}\}, \qquad \varepsilon_{\mathrm{mca}}(C,\delta) := \max_{(f_1,f_2)} \tfrac{1}{q}\#\{\gamma \ \delta\text{-MCA-bad}\}.$$

For the sparse mutual layer define

$$\sigma_C(\delta) := \max\big\{\#\{\delta\text{-MCA-bad } \gamma \text{ for } (\epsilon_1,\epsilon_2)\} : |\operatorname{supp}\epsilon_1 \cup \operatorname{supp}\epsilon_2| \le r\big\}.$$

Sparse pairs are δ-close in columns, since they are explained by $(0,0)$ outside at most r coordinates, so σ_C counts a purely mutual layer.

Definition 2.1. For a target $\varepsilon^* \in (0,1)$, the grand MCA threshold is $\delta_C^*(\varepsilon^*) := \sup\{\delta \in (0, 1-\rho) : \varepsilon_{\mathrm{mca}}(C,\delta) \le \varepsilon^*\}$, with $\sup\emptyset := 0$.

The restriction to sub-capacity radii matches the challenge convention of [ABF26, PP26]; at $\delta \ge 1-\rho$ every word is δ-close to C by interpolation and the threshold question changes character. We record the comparison of the two errors.

Lemma 2.2. *Every δ-CA-bad slope is δ-MCA-bad; hence $\varepsilon_{\mathrm{ca}}(C,\delta) \le \varepsilon_{\mathrm{mca}}(C,\delta)$.*

Proof. If γ is CA-bad, then $\mathrm{dist}(f_1+\gamma f_2, C) \le \delta$, so a witness (c,S) with $|S| \ge (1-\delta)n$ exists; and $\mathrm{dist}_2((f_1,f_2),C^{\equiv 2}) > \delta$ means no set of $\ge (1-\delta)n$ coordinates carries a pair explanation, in particular S does not. So γ is MCA-bad. □

We use the standard entropy estimates for binomial coefficients, with $\mathrm{H}_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$: for integers $0 < m < N$,

$$2^{N\mathrm{H}_2(m/N)}/(N+1) \;\le\; \tbinom{N}{m} \;\le\; 2^{N\mathrm{H}_2(m/N)}. \tag{1}$$

Indeed, with $p = m/N$, expanding $1 = \sum_i \binom{N}{i}p^i(1-p)^{N-i}$ gives the upper bound by keeping the term $i = m$, which equals $\binom{N}{m}2^{-N\mathrm{H}_2(p)}$; and since the term ratios $\binom{N}{i+1}p^{i+1}(1-p)^{N-i-1}/\binom{N}{i}p^i(1-p)^{N-i} = (N-i)p/((i+1)(1-p))$ exceed 1 for $i < m$ and are below 1 for $i \ge m$, the $i = m$ term is the largest of the $N+1$ terms, giving the lower bound.

3. The unsafe side

The failure mechanism has two independent parts: a pigeonhole construction of a single received word carrying an enormous list at an agreement slightly above k, and a conversion of any such list into correlated-agreement failure. Neither part uses any arithmetic property of $\mathbb{F}$ beyond its size.

Lemma 3.1 (graded prefix floor)**.** *Let $\varphi \in \mathbb{F}[X]$ have degree $c \ge 1$ and suppose the fibers of φ inside D are complete and of uniform size c: every nonempty set $\varphi^{-1}(y) \cap D$, $y \in Q := \varphi(D)$, has exactly c elements. Put $N := n/c$, let $B \subseteq \mathbb{F}$ be any subfield with $D \subseteq B$ and $\varphi \in B[X]$ (always $B = \mathbb{F}$ works), and let $1 \le K \le n$ and $\lceil K/c\rceil \le m \le N$, $w := m - \lceil K/c\rceil$. Then some B-valued word $U\colon D \to B$ satisfies*

$$\big|\Lambda\big(\mathrm{RS}[\mathbb{F}, D, K],\, 1 - \tfrac{mc}{n},\, U\big)\big| \;\ge\; \binom{N}{m}\Big/|B|^{\,w}.$$

Proof. For each m-subset $M \subseteq Q$ put $\Lambda_M := \prod_{b\in M}(\varphi - b) = \sum_{j=0}^{m}(-1)^j e_j(M)\varphi^{m-j}$, where e_j is the j-th elementary symmetric function; $\Lambda_M \in B[X]$ has degree cm and vanishes at $x \in D$ exactly when $\varphi(x) \in M$, i.e. at exactly cm points by fiber completeness. For $z \in B^w$ let $U_z := \big(\varphi^m + \sum_{j=1}^{w} z_j\varphi^{m-j}\big)\big|_D$, a B-valued word. By pigeonhole over the prefix map $M \mapsto z(M) := \big((-1)^j e_j(M)\big)_{j\le w} \in B^w$, some z^* is attained by at least $\binom{N}{m}/|B|^w$ sets M; for each such M set $c_M := U_{z^*} - \Lambda_M|_D = -\sum_{j>w}(-1)^j e_j(M)\varphi^{m-j}|_D$, a polynomial of degree at most $c(m-w-1) = c(\lceil K/c\rceil - 1) \le K-1$, so $c_M \in \mathrm{RS}[\mathbb{F}, D, K]$, and U_{z^*} agrees with c_M on the cm fiber points of M. The map $M \mapsto c_M$ is injective on the pigeonhole class: equality of words of degree $\le K-1 \le n-1$ on all of D forces equality of polynomials, and the powers φ^{m-j} have distinct degrees $c(m-j)$, so all $e_j(M) = e_j(M')$ for $j > w$; for $j \le w$ they agree through z^*; hence $\prod_{b\in M}(Y-b) = \prod_{b\in M'}(Y-b)$ and $M = M'$. □

Theorem 3.2 (deep-point conversion)**.** *Let $C = \mathrm{RS}[\mathbb{F}, D, k]$, $q > n$, let $\delta \in (0,1)$ satisfy $\lfloor \delta n\rfloor \le n - k - 1$, and let $\eta \in (0,1)$. If $\varepsilon_{\mathrm{ca}}(C,\delta) \le \eta\,\frac{1}{k}\big(1 - \frac{n}{q}\big)$, then every received word $U\colon D \to \mathbb{F}$ satisfies $\big|\Lambda\big(\mathrm{RS}[\mathbb{F}, D, k+1], \delta, U\big)\big| \le q\,\varepsilon_{\mathrm{ca}}(C,\delta)/(1-\eta)$.*

Proof. Put $\varepsilon := \varepsilon_{\mathrm{ca}}(C,\delta)$ and $a := n - \lfloor \delta n\rfloor \ge k+1$, and let $P_1, \dots, P_L \in \mathbb{F}[X]_{<k+1}$ be distinct polynomials whose restrictions lie in $\Lambda(\mathrm{RS}[\mathbb{F}, D, k+1], \delta, U)$; each agrees with U on a set S_i of at least a points, distances being integral. Let $\Omega := \mathbb{F} \setminus D$, of size $q-n$, and for $\alpha \in \Omega$ define the simple-pole pair $f_\alpha(x) := U(x)/(x-\alpha)$, $g_\alpha(x) := -1/(x-\alpha)$ for $x \in D$. For every i and every $x \in S_i$, $f_\alpha(x) + P_i(\alpha)g_\alpha(x) = (P_i(x) - P_i(\alpha))/(x-\alpha)$, the restriction of a polynomial of degree less than k; so the point at slope $P_i(\alpha)$ agrees with a codeword of C on S_i, hence is δ-close to C. The pair is δ-far from $C^{\equiv 2}$: if $G \in \mathbb{F}[X]_{<k}$ agreed with g_α on more than k points of D, then $(X-\alpha)G + 1$, of degree at most k, would have more than k roots while taking value 1 at α; so any pair explanation on $\ge a \ge k+1$ points is impossible. Therefore each distinct value among $P_1(\alpha), \dots, P_L(\alpha)$ is a δ-CA-bad slope, and, writing $M(\alpha)$ for the number of distinct values, $M(\alpha) \le \varepsilon q$ for every $\alpha \in \Omega$.

It remains to pick a good α. For $i \ne j$ the nonzero polynomial $P_i - P_j$ has degree at most k, hence at most k roots, so the number of colliding pairs summed over $\alpha \in \Omega$ is at most $k\binom{L}{2}$; fix α whose collision count is at most $k\binom{L}{2}/(q-n)$. If the fibers of $i \mapsto P_i(\alpha)$ have sizes $m_1, \dots, m_{M(\alpha)}$, then $\sum_r m_r = L$ and $\sum_r m_r^2 = L + 2\sum_r \binom{m_r}{2} \le L + kL(L-1)/(q-n)$, so Cauchy–Schwarz

gives $L^2 \le M(\alpha)\sum_r m_r^2$, i.e. $M(\alpha) \ge L(q-n)/(q-n+k(L-1)) \ge L(q-n)/(q-n+kL)$. Combining, $\varepsilon q(q-n+kL) \ge L(q-n)$, i.e. $L(q-n)(1-\varepsilon qk/(q-n)) \le \varepsilon q(q-n)$; the hypothesis gives $\varepsilon qk/(q-n) \le \eta < 1$, whence $L \le \varepsilon q/(1-\eta)$. □

Theorem 3.3 (cap criterion)**.** *In the setting of Lemma 3.1 with $K = k+1$ and $q > n$: if $\binom{N}{m} > |B|^w\big(\frac{q}{k}+1\big)$, then for every $\delta \in [1-\frac{mc}{n}, 1-\rho)$,*

$$\varepsilon_{\mathrm{mca}}(C,\delta) \;\ge\; \varepsilon_{\mathrm{ca}}(C,\delta) \;>\; \frac{1}{2k}\Big(1-\frac{n}{q}\Big).$$

Proof. Every $\delta < 1-\rho$ has $\lfloor \delta n \rfloor \le n-k-1$, since $\delta n < n-k$ and distances are integral; so Theorem 3.2 applies at every radius in the stated range. The word U of Lemma 3.1 has $\big|\Lambda(\mathrm{RS}[\mathbb{F}, D, k+1], \delta, U)\big| > \frac{q}{k}+1 > \frac{q-n}{k}$ at every $\delta \ge 1-\frac{mc}{n}$, because the $\binom{N}{m}/|B|^w$ listed codewords agree with U on $mc \ge (1-\delta)n$ points. If $\varepsilon_{\mathrm{ca}}(C,\delta) \le \frac{1}{2k}(1-\frac{n}{q})$, then Theorem 3.2 with $\eta = \frac{1}{2}$ bounds that list by $2q\,\varepsilon_{\mathrm{ca}}(C,\delta) \le \frac{q-n}{k}$, a contradiction. Lemma 2.2 transfers the bound to $\varepsilon_{\mathrm{mca}}$. □

Corollary 3.4 (ordinary locator cap; top of the plain-CA band)**.** *Let $D \subseteq \mathbb{F}$ be any set of size n, let $C = \mathrm{RS}[\mathbb{F}, D, k]$ with $\rho = k/n \in \{\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}\}$, $k \le 2^{40}$ and $n \ge 2^{15}$, and assume $n < q < 2^{256}$. Define α_ρ and $s_\rho = \lceil \alpha_\rho n \rceil$ as in Theorem 1.1. Then, for every $\delta \in [1-\rho-s_\rho/n, 1-\rho)$,*

$$\varepsilon_{\mathrm{mca}}(C,\delta) \ge \varepsilon_{\mathrm{ca}}(C,\delta) > \frac{1}{2k}\Big(1-\frac{n}{q}\Big).$$

In particular, if $q \ge 2^{128}$, then $\varepsilon_{\mathrm{ca}}(C,\delta) > 2^{-128}$ throughout this interval.

Proof. Apply Lemma 3.1 and Theorem 3.3 with the identity map $\varphi = X$, so $c = 1$, $N = n$, $B = \mathbb{F}$, $K = k+1$, $m = k+s_\rho$, and $w = s_\rho - 1$; here $k+1 \le m \le n$ because $s_\rho \ge 1$ and $\rho + \alpha_\rho + 2^{-15} < 1$ in all four cases. The cap criterion becomes

$$\binom{n}{k+s_\rho} > q^{s_\rho - 1}\Big(\frac{q}{k}+1\Big).$$

It is enough to verify this with q replaced by 2^{256}. Since $k \ge n/16 \ge 2^{11}$, we have $\log_2(q/k+1) < 256$, while (1) gives

$$\log_2 \binom{n}{k+s_\rho} \ge n\mathrm{H}_2\Big(\rho + \frac{s_\rho}{n}\Big) - \log_2(n+1).$$

Because $s_\rho/n \in [\alpha_\rho, \alpha_\rho + 2^{-15}]$, the following lower bounds hold on the relevant interval:

ρ	α_ρ	$\min \mathrm{H}_2(\rho + s_\rho/n)$	$\min \mathrm{H}_2(\rho + s_\rho/n) - 256\alpha_\rho$
$\frac{1}{2}$	1/300	0.9999	> 0.146
$\frac{1}{4}$	3/1000	0.8159	> 0.047
$\frac{1}{8}$	41/20000	0.5492	> 0.024
$\frac{1}{16}$	3/2500	0.3419	> 0.034.

Thus $n\mathrm{H}_2(\rho + s_\rho/n) - \log_2(n+1) > 256 s_\rho$ for every $n \ge 2^{15}$, with the tightest case still having more than 500 bits of slack at $n = 2^{15}$. This proves the criterion and hence the displayed lower bound. Finally, if $q \ge 2^{128}$ then $n \le 16k \le 2^{44}$, so $n/q < 2^{-84}$ and $\frac{1}{2k}(1-n/q) > 2^{-42} > 2^{-128}$. □

Corollary 3.5 (universal cap on the challenge box)**.** *Let $D \subseteq \mathbb{F}^\times$ be a coset of a cyclic subgroup of even order $n \ge 2^{15}$, let $\rho \in \{\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}\}$ and $n < q < 2^{256}$, and set $g := g_\rho$ as in Theorem 1.1. Then $\varepsilon_{\mathrm{mca}}(C,\delta) > \frac{1}{2k}(1-\frac{n}{q})$ for every $\delta \in [1-\rho-g, 1-\rho)$.*

Proof. Since n is even and $n \mid q-1$, the field has odd characteristic and -1 is the element of order 2 in the subgroup H with $D = \alpha H$; so $\varphi := X^2$ has fibers $\{x, -x\}$ inside D, complete and of size 2. Apply Lemma 3.1 and Theorem 3.3 with $c = 2$, $B = \mathbb{F}$, $K = k+1$ and $m := \lceil (k+1+gn)/2 \rceil$; then $2m \ge k+gn$, so $[1-\rho-g, 1-\rho) \subseteq [1-\frac{2m}{n}, 1-\rho)$, and $w = m - \lceil (k+1)/2 \rceil \le (gn+2)/2$, and

$m \le N = n/2$ since $k+gn+2 \le n$. It remains to verify the criterion. Writing $\beta := \log_2 q \le 256$, by (1) it suffices that

$$\tfrac{n}{2}\,\mathrm{H}_2(m/N) \;\ge\; 128\,gn + 512 + \log_2\!\big(\tfrac{n}{2}+1\big), \tag{2}$$

since $\beta w \le 128gn + 256$ and $\log_2(\frac{q}{k}+1) \le 256$. Here $m/N = 2m/n \in [\rho+g,\ \rho+g+2^{-13}]$ for $n \ge 2^{15}$, and on that interval the concave H_2 is at least $h(\rho) := \min\big(\mathrm{H}_2(\rho+g), \mathrm{H}_2(\rho+g+2^{-13})\big)$, which evaluates (rounding down) to $h \ge 0.9999,\ 0.8122,\ 0.5489,\ 0.3410$ at $\rho = \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}$. Both sides of (2) are linear in n up to the logarithm, with slopes $h/2$ and $128g$, and $h/2 - 128g$ equals $0.2499,\ 0.1561,\ 0.0244,\ 0.0455$ respectively, all positive; so it suffices to check (2) at $n = 2^{15}$, where the left side is at least $16384\,h \ge 8993$ (the tightest case, $\rho = \frac{1}{8}$) against a right side of $8192 + 512 + 15 = 8719$ there, and 5586 against $4096 + 527$ at $\rho = \frac{1}{16}$, and larger margins at $\rho \in \{\frac{1}{4}, \frac{1}{2}\}$; the slack of at least 274 bits makes the criterion of Theorem 3.3 strict. (All four instances were additionally verified by exact integer arithmetic at $n = 2^{15}$, $q = 2^{256} - 1$.) □

Proposition 3.6 (small fields)**.** *For every linear code $C \subsetneq \mathbb{F}^n$ and every $\delta \in (0,1)$, $\varepsilon_{\mathrm{mca}}(C,\delta) \ge 1/q$. Hence $\delta^*_C(\varepsilon^*) = 0$ whenever $\varepsilon^* < 1/q$, in particular whenever $q < 2^{128}$ at the grand target. At the boundary $q = 2^{128}$ the same construction gives $\varepsilon_{\mathrm{mca}} \ge 2^{-128}$ at every radius, which meets the threshold condition with equality and does not by itself force degeneracy.*

Proof. Pick $f_2 \notin C$, any $c_0 \in C$, $\gamma_0 \in \mathbb{F}$, and set $f_1 := c_0 - \gamma_0 f_2$. Then $f_1 + \gamma_0 f_2 = c_0$, so (c_0, D) is a proximity witness with $S = D$; but a pair explanation on $S = D$ would force $f_1, f_2 \in C$, which fails. Hence γ_0 is δ-MCA-bad for this pair at every δ, and $\varepsilon_{\mathrm{mca}}(C,\delta) \ge 1/q$. □

Remark 3.7 (other smooth domains). Lemma 3.1 and Theorem 3.3 are stated for arbitrary complete-fiber polynomial maps, so Corollary 3.5 extends beyond even-order multiplicative cosets with the identical arithmetic. (i) *Characteristic two, additive smoothness.* If $D = t + V$ is an $\mathbb{F}_2$-affine subspace of dimension $s \ge 1$ and $a \in V \setminus \{0\}$, the linearized polynomial $\varphi(x) = x^2 + ax$ satisfies $\varphi(x+a) = \varphi(x)$, so its fibers inside D are the pairs $\{x, x+a\}$, complete and of size 2; the proof of Corollary 3.5 then goes through verbatim. (ii) *Odd smooth orders.* If $3 \mid n$ (e.g. n a power of 3), take $\varphi = X^3$: the fibers are the μ_3-cosets, complete of size 3 since $\mu_3 \subseteq H$ and $3 \mid q-1$ forces characteristic $\neq 3$; the same entropy verification with $N = n/3$ yields the four gaps of Corollary 3.5 for $n \ge 2^{16}$ (checked as in the proof above, tightest margin again at $\rho = \frac{1}{8}$). (iii) Chebyshev and circle-code domains, and genus-one (ECFFT) domains, also carry complete uniform fibers and receive the same caps; see [Cho26b].

Remark 3.8 (small n and general rates). For $2^{12} \le n < 2^{15}$ the corollary's uniform gap is not claimed, but capacity is still refuted: taking $m = \lceil (k+1)/2 \rceil + 1$, so $w = 1$ and agreement $2m \ge k+3$, the criterion $\binom{n/2}{m} > q(\frac{q}{k}+1)$ holds at all four rates for $n \ge 2^{12}$ (at $\rho = \frac{1}{16}$, $n = 2^{12}$: $\log_2 \binom{2048}{130} \ge 687$ against at most 505), giving $\delta^*_C(2^{-128}) \le 1 - \rho - 3/n$ whenever $q \ge 2^{128}$. For $n < 2^{12}$ with $q \ge 2^{128}$ our method gives nothing above the safe region, and we record this corner as genuinely open. For rates outside the four challenge values, Theorem 3.3 applies unchanged; the achievable gap is governed by the criterion, asymptotically the envelope of Proposition 8.1, and is positive for every fixed $\rho \in (0,1)$ and large n. Finally, the list challenge of [ABF26] is unsafe at the same first step: Lemma 3.1 at $K = k$ produces a single word with more than $2^{-128}q$ listed codewords under the analogous criterion, with the same verification.

4. The safe side

We now prove that MCA *holds*, with essentially optimal error, deep inside the unique-decoding region — for every linear code — and that up to half the minimum distance the mutual layer costs only an explicit tangent term.

Theorem 4.1 (deep regime)**.** *Let $C \subseteq \mathbb{F}^n$ be linear with minimum weight $w_{\min}$, let $\delta \in (0,1)$, $r := \lfloor \delta n \rfloor$, and assume $3r \le w_{\min} - 1$. Then for every pair (f_1, f_2) at least one of the following holds:*

(1) *there are $c_1, c_2 \in C$ and $T \subseteq [n]$ with $|T| \le r$ and $f_i = c_i$ off T for $i = 1, 2$; or*

(2) *at most* $r+1$ *slopes* γ *have* $\operatorname{dist}(f_1+\gamma f_2, C) \le \delta$.

Consequently $\varepsilon_{\mathrm{ca}}(C,\delta) \le (r+1)/q$ *and* $\varepsilon_{\mathrm{mca}}(C,\delta) \le (r+1)/q$.

Proof. Suppose (2) fails, so there are $r+2$ distinct slopes $\gamma_0,\dots,\gamma_{r+1}$, codewords c_j, and error sets $E_j := \{i : (f_1+\gamma_j f_2)(i) \neq c_j(i)\}$ with $|E_j| \le r$. For $j \neq l$, solving the two agreements off $E_j \cup E_l$ gives $f_2 = d_{jl} := (c_j - c_l)/(\gamma_j - \gamma_l)$ and $f_1 = e_{jl} := (\gamma_j c_l - \gamma_l c_j)/(\gamma_j - \gamma_l)$ off $E_j \cup E_l$, with $d_{jl}, e_{jl} \in C$. If $r = 0$ all E_j are empty and (1) holds with $T = \emptyset$; so assume $r \ge 1$, hence at least three slopes. For any three indices j,l,m, the codeword $d_{jl} - d_{jm}$ vanishes off $E_j \cup E_l \cup E_m$, a set of size at most $3r \le w_{\min} - 1$, so $d_{jl} = d_{jm}$; chaining through shared indices, all d_{jl} equal a single $d \in C$, and likewise all e_{jl} equal a single $e \in C$. Let $T := \{i : (f_1(i), f_2(i)) \neq (e(i), d(i))\}$. If $i \notin E_j$ and $i \notin E_l$ for two distinct indices, then solving at coordinate i gives $f_2(i) = d(i)$ and $f_1(i) = e(i)$, so $i \notin T$; contrapositively each $i \in T$ lies in at least $r+1$ of the $r+2$ sets E_j, whence $(r+1)|T| \le \sum_j |E_j| \le r(r+2)$ and $|T| \le r(r+2)/(r+1) < r+1$, i.e. $|T| \le r$. This is (1) with $(c_1, c_2) = (e, d)$.

For the error bounds, fix a pair. In case (2), both CA-bad and MCA-bad slopes are among the at most $r+1$ close slopes. In case (1): the pair is within column distance $r/n \le \delta$ of (c_1, c_2), so no slope is CA-bad. For MCA, write $\epsilon_i := f_i - c_i$, supported on T, and call γ *tangent* if $\epsilon_1(i) + \gamma\epsilon_2(i) = 0$ for some $i \in T$; there are at most $|T| \le r$ tangent slopes, since a coordinate with $\epsilon_2(i) \neq 0$ determines one value of γ and a coordinate with $\epsilon_2(i) = 0 \neq \epsilon_1(i)$ determines none. Let γ be non-tangent and let (c, S) be any proximity witness for $f_1 + \gamma f_2$, so $|S| \ge n - r$. The codeword $c - (c_1 + \gamma c_2)$ vanishes on $S \setminus T$, of size at least $n - 2r$, so its weight is at most $2r \le w_{\min} - 1$ and it is zero; then $(\epsilon_1 + \gamma\epsilon_2)|_S = 0$, and since γ is non-tangent this function is nonzero at every point of T, forcing $S \cap T = \emptyset$ and hence $f_i|_S = c_i|_S$: the witness extends mutually. So every MCA-bad slope is tangent, and there are at most $r \le r+1$ of them. □

Theorem 4.2 (mutual from correlated, below half the distance)**.** *Let* $C \subseteq \mathbb{F}^n$ *be linear with minimum weight* $w_{\min}$, $\delta \in (0,1)$, $r := \lfloor \delta n \rfloor$, *and assume* $2r \le w_{\min} - 1$. *Then* $\varepsilon_{\mathrm{mca}}(C,\delta) \le \max\big(\varepsilon_{\mathrm{ca}}(C,\delta),\, r/q\big)$.

Proof. Fix a pair (f_1, f_2). If $\operatorname{dist}_2((f_1,f_2), C^{\equiv 2}) > \delta$, every MCA-bad slope is CA-bad: proximity gives a witness, farness denies every pair explanation of size $\ge (1-\delta)n$, and the CA conditions are exactly these two; so the count is at most $q\,\varepsilon_{\mathrm{ca}}(C,\delta)$. If instead $\operatorname{dist}_2 \le \delta$, fix an explanation $(p_1, p_2) \in C^{\equiv 2}$ with column error set E, $|E| \le r$, and put $\epsilon_i := f_i - p_i$, supported on E. Exactly as in the proof of Theorem 4.1 — with $2r \le w_{\min} - 1$ now doing the forcing — for every non-tangent γ and every witness (c, S), the codeword $c - (p_1 + \gamma p_2)$ vanishes on $S \setminus E$ of size $\ge n - 2r$, hence is zero; then S avoids the support of $\epsilon_1 + \gamma\epsilon_2$, which is all of E, so $f_i|_S = p_i|_S$ and the witness extends. MCA-bad slopes are thus among the at most $|E| \le r$ tangent values. □

Corollary 4.3 (safe to half the distance, modulo one import)**.** *Let* $C = \mathrm{RS}[\mathbb{F}, D, k]$ *and* $\delta \le \frac{n-k}{2n}$. *Assuming the unique-decoding proximity gap of* [BCIKS20, Thm. 4.1], *namely* $\varepsilon_{\mathrm{ca}}(C,\delta) \le n/q$ *for* δ *up to half the minimum distance, we get* $\varepsilon_{\mathrm{mca}}(C,\delta) \le n/q$.

Proof. Here $w_{\min} = n - k + 1$ and $2\lfloor \delta n \rfloor \le n - k = w_{\min} - 1$, so Theorem 4.2 gives $\varepsilon_{\mathrm{mca}} \le \max(n/q, \lfloor \delta n \rfloor / q) = n/q$. □

5. Proof of Theorem 1.1

(1) is Proposition 3.6: $\varepsilon_{\mathrm{mca}}(C,\delta) \ge 1/q > 2^{-128}$ at every δ, so the supremum set is empty.

(2) By Corollary 3.4, $\varepsilon_{\mathrm{ca}}(C,\delta) > \frac{1}{2k}(1 - \frac{n}{q})$ for every $\delta \in [1-\rho-s_\rho/n, 1-\rho)$. Here $k \le 2^{40}$ gives $\frac{1}{2k} \ge 2^{-41}$, and $n \le 16k \le 2^{44}$ with $q \ge 2^{128}$ gives $1 - \frac{n}{q} > 1 - 2^{-84} > \frac{1}{2}$; so $\varepsilon_{\mathrm{ca}}(C,\delta) > 2^{-42} > 2^{-128}$ throughout the interval. By Lemma 2.2, the same interval is MCA-unsafe; hence no radius there belongs to the supremum set and $\delta^*_C(2^{-128}) \le 1 - \rho - s_\rho/n$. Finally $s_\rho/n \ge \alpha_\rho > g_\rho$, which places a nonempty CA-failing slice inside the old band $((1-\rho)/2, 1-\rho-g_\rho)$.

(3) and (4). Let $r^* := \min(\lfloor (n-k)/3 \rfloor, \lfloor 2^{-128} q \rfloor - 1)$ and suppose $r^* \ge 1$. At $\delta := r^*/n$ we have $\lfloor \delta n \rfloor = r^*$ and $3r^* \le n - k = w_{\min} - 1$, so Theorem 4.1 gives $\varepsilon_{\mathrm{mca}}(C,\delta) \le (r^*+1)/q \le 2^{-128}$, using $r^* + 1 \le \lfloor 2^{-128} q \rfloor$; also $\delta < 1 - \rho$, so δ lies in the supremum set and $\delta^* \ge r^*/n$. If $q \ge 2^{128} n$

then $\lfloor 2^{-128}q\rfloor - 1 \geq n-1 \geq \lfloor (n-k)/3\rfloor$, so $r^* = \lfloor (n-k)/3\rfloor$ and $\delta^* \geq \frac{1}{n}\lfloor (n-k)/3\rfloor \geq \frac{1-\rho}{3} - \frac{2}{3n}$; since $s_\rho/n \geq g_\rho$, the earlier ratio estimate against the weaker upper bound $1-\rho-g_\rho$ still gives a factor smaller than three. With the import, take $\delta := \frac{1}{n}\lfloor (n-k)/2\rfloor \leq \frac{n-k}{2n}$: Corollary 4.3 gives $\varepsilon_{\mathrm{mca}} \leq n/q \leq 2^{-128}$ when $q \geq 2^{128}n$, so $\delta^* \geq \frac{1-\rho}{2} - \frac{1}{2n}$, and the same comparison gives a factor smaller than two. In the thin regime $2^{128} \leq q < 2^{128}n$ only the r^* clause is claimed; as $q \downarrow 2^{128}$, r^* reaches 0 and the lower bound becomes vacuous, as stated. □

Two comments on the statement. First, the import in (3) is a published theorem, so the two-sided determination within a factor of two stands on the literature; the unconditional clause records what the present paper proves alone. Second, the case split at $q = 2^{128}$ is genuinely necessary at the stated target: below it the threshold degenerates, at it neither degeneracy nor a nontrivial safe radius follows (Proposition 3.6), and the meaningful question there is posed at a larger target, as the deployed circle-code rows already illustrate [Cho26b].

6. Refining the residual band

The main theorem gives a two-sided pincer but does not by itself determine the exact staircase. The original broad residual questions can be sharpened further. First, the top of the old plain-CA band is already unsafe by the ordinary locator floor Corollary 3.4, which is stronger than the quadratic uniform cap used only to state the smooth-domain envelope. Second, the mutual layer above plain correlated agreement is not mysterious: for column-close pairs, every extra MCA slope is forced by either a tangent coordinate or a low-weight shortening image. A second, code-agnostic formulation bounds the same extra layer by a doubled-radius pair list.

6.1. The top of the plain-CA band is already unsafe.

The gap g_ρ in Theorem 1.1 is the clean smooth-domain cap obtained from the two-fiber map X^2. The identity map gives a stronger top-edge statement for plain CA over arbitrary evaluation sets.

Corollary 6.1 (the original plain-CA band is not all safe)**.** *In the parameter box of Theorem 1.1, assume $q \geq 2^{128}$. Then*

$$\varepsilon_{\mathrm{ca}}(C,\delta) > 2^{-128} \qquad \text{for every} \qquad \delta \in \left[1-\rho-\frac{s_\rho}{n},\, 1-\rho\right).$$

Since $s_\rho/n \geq \alpha_\rho > g_\rho$, the upper slice

$$\left[1-\rho-\frac{s_\rho}{n},\, 1-\rho-g_\rho\right)$$

of the previously displayed band is already plain-CA unsafe, and hence MCA unsafe.

Proof. This is exactly Corollary 3.4, followed by the numerical estimate in the proof of Theorem 1.1(2): $k \leq 2^{40}$ and $q \geq 2^{128}$ imply $\frac{1}{2k}(1-n/q) > 2^{-128}$. □

Thus the remaining plain-CA question starts below the sharper edge $1-\rho-s_\rho/n$, not below the coarser edge $1-\rho-g_\rho$.

6.2. The mutual layer as a residual shortening image.

For a vector $u \in \mathbb{F}^D$ write $\mathrm{supp}(u) := \{x \in D : u(x) \neq 0\}$. Fix an integer r and a pair (f_1, f_2) that is r/n-close to $C^{\equiv 2}$. Choose one explaining pair $(p_1, p_2) \in C^{\equiv 2}$ and put

$$E := \{x \in D : (f_1(x), f_2(x)) \neq (p_1(x), p_2(x))\}, \qquad |E| \leq r,$$
$$e_i := f_i - p_i \qquad (i = 1, 2).$$

A slope is called *E-tangent* if

$$e_1(x) + \gamma e_2(x) = 0 \quad \text{for some } x \in E.$$

There are at most $|E| \leq r$ such slopes, because each coordinate with $e_2(x) \neq 0$ determines one finite value of γ, and a coordinate with $e_2(x) = 0 \neq e_1(x)$ determines none.

For this fixed explanation define $R_C(E, e_1, e_2; r)$ to be the set of slopes $\gamma \in \mathbb{F}$ for which there are a set $F_0 \subseteq D$ with $|F_0| \leq r$ and a nonzero codeword $d \in C$ such that

$$\mathrm{supp}(d) \subseteq E \cup F_0, \qquad d(x) = e_1(x) + \gamma e_2(x) \quad \text{for every } x \in E \setminus F_0.$$

Finally put

$$R_C(r) := \max_{E,e_1,e_2} |R_C(E, e_1, e_2; r)|,$$

where the maximum is over $|E| \le r$ and error pairs supported on E.

Theorem 6.2 (shortening-image reduction for the mutual layer)**.** *Let $C \subseteq \mathbb{F}^D$ be linear, let $\delta \in (0,1)$, and put $r := \lfloor \delta n \rfloor$. Then*

$$\varepsilon_{\mathrm{mca}}(C, \delta) \le \max\left(\varepsilon_{\mathrm{ca}}(C, \delta), \frac{r + R_C(r)}{q}\right).$$

If $C = \mathrm{RS}[\mathbb{F}, D, k]$, then every nonzero codeword counted in $R_C(r)$ belongs to a shortening of dimension at most

$$\max(0, 2r - (n-k)).$$

In particular $R_C(r) = 0$ whenever $2r \le n-k$, recovering the half-distance reduction Theorem 4.2.

Proof. Fix a pair (f_1, f_2). If the pair is δ-far from $C^{\equiv 2}$, then any MCA-bad slope is CA-bad by the proof of Lemma 2.2; this gives the first term.

Assume instead that the pair is δ-close, and choose (p_1, p_2) and E as above. Let γ be MCA-bad, with witness (c, S), $|S| \ge n - r$. Put $F_0 := D \setminus S$, so $|F_0| \le r$, and set

$$d := c - (p_1 + \gamma p_2) \in C.$$

On $S \setminus E$ the errors vanish and both c and $p_1 + \gamma p_2$ agree with $f_1 + \gamma f_2$, so $d = 0$ there. Hence $\mathrm{supp}(d) \subseteq E \cup F_0$. On $E \setminus F_0 = E \cap S$ we have

$$d = e_1 + \gamma e_2.$$

If γ is not E-tangent and $d = 0$, then $E \cap S = \emptyset$; consequently $S \subseteq D \setminus E$, and the original pair (p_1, p_2) explains (f_1, f_2) on S, contradicting MCA-badness. Thus every non-tangent MCA-bad slope belongs to $R_C(E, e_1, e_2; r)$, while tangent slopes contribute at most r. Taking the maximum over pairs proves the inequality.

For Reed–Solomon codes, fix E and F_0. The codewords supported in $E \cup F_0$ form a shortening on a set of size at most $2r$. Since Reed–Solomon codes are MDS, this shortening has dimension

$$\max(0, |E \cup F_0| - (n-k)) \le \max(0, 2r - (n-k)).$$

If $2r \le n - k$, every such shortening is zero, so no residual non-tangent slope exists. □

The next example shows that the shortening term is not an artifact of the proof: it appears as soon as the half-distance forcing condition fails.

Proposition 6.3 (sharpness of the half-distance wall)**.** *Let $C = \mathrm{RS}[\mathbb{F}, D, k]$ with minimum distance $d = n - k + 1$. Let*

$$\max(2, \lceil d/2 \rceil) \le r \le d - 2.$$

Then there is a pair (f_1, f_2) with $\mathrm{dist}_2((f_1, f_2), C^{\equiv 2}) \le r/n$ and a slope γ_0 that is MCA-bad at radius r/n but not CA-bad. Moreover γ_0 can be chosen non-tangent for a nearest explanation of the pair. Thus the estimate $\varepsilon_{\mathrm{mca}} \le \max(\varepsilon_{\mathrm{ca}}, r/q)$ cannot, in general, be extended beyond half the distance.

Proof. Choose disjoint sets $E, F_0 \subseteq D$ with $|E| = r$ and $|F_0| = d - r$, and put $W := E \cup F_0$, so $|W| = d$. Since C is MDS, there is a nonzero codeword $c \in C$ supported exactly on W; for Reed–Solomon codes one may take a nonzero scalar multiple of

$$\prod_{x \in D \setminus W} (X - x).$$

Let $S := D \setminus F_0$, so $|S| = n - d + r \ge n - r$ because $r \ge d/2$. Define f_1 to equal c on E and 0 off E. Choose f_2 supported on E whose restriction to E is not a scalar multiple of $c|_E$; this is possible because $|E| \ge 2$. The pair is r/n-close to $(0,0) \in C^{\equiv 2}$.

At slope $\gamma_0 = 0$, the word f_1 agrees with the codeword c on all of S: on E this is by definition, and on $S \setminus E$ both are zero. Hence (c, S) is a proximity witness. It is not a mutual witness. Indeed, any codeword agreeing with f_2 on S must be supported inside W; the shortening of

an MDS code on a minimum-weight support W is one-dimensional and spanned by c, so its restriction to E is a scalar multiple of $c|_E$, contrary to the choice of f_2. Therefore γ_0 is MCA-bad. It is not CA-bad, because the pair is already r/n-close to $C^{\equiv 2}$. Finally, relative to the nearest explanation $(0,0)$, the value $f_1 + 0 \cdot f_2$ is nonzero at every point of E, so γ_0 is non-tangent. □

6.3. **A doubled-radius pair-list formulation.** The shortening term can also be expressed without using the Reed–Solomon MDS structure. For a received pair $f = (f_1, f_2)$ and an integer s, define

$$\mathcal{L}_s^{(2)}(f) := \{(p_1, p_2) \in C^2 : \#\{x \in D : f_1(x) = p_1(x),\ f_2(x) = p_2(x)\} \geq n - s\},$$

and set

$$L_s^{(2)}(C) := \max_f |\mathcal{L}_s^{(2)}(f)|.$$

Theorem 6.4 (MCA excess is controlled by the doubled-radius pair list)**.** *Let $C \subseteq \mathbb{F}^D$ be linear, let $\delta \in (0,1)$, and put $r := \lfloor \delta n \rfloor$. Then*

$$\varepsilon_{\mathrm{mca}}(C, \delta) \leq \max\left(\varepsilon_{\mathrm{ca}}(C, \delta), \frac{1 + (r+1)L_{2r}^{(2)}(C)}{q}\right).$$

Proof. Fix a pair $f = (f_1, f_2)$. If f is δ-far from C^2 in column distance, then every MCA-bad slope is already CA-bad, so this pair contributes at most $q\varepsilon_{\mathrm{ca}}(C, \delta)$ slopes.

Suppose therefore that f is δ-close to C^2. Let B be its set of MCA-bad slopes. If $B = \emptyset$ there is nothing to prove. Choose an anchor slope $\gamma_0 \in B$ and a non-extending witness (c_0, S_0), so $|S_0| \geq n - r$ and

$$f_1 + \gamma_0 f_2 = c_0 \quad \text{on } S_0.$$

For every $\gamma \in B \setminus \{\gamma_0\}$ choose a non-extending witness (c_γ, S_γ) and define

$$p_2^{(\gamma)} := \frac{c_\gamma - c_0}{\gamma - \gamma_0}, \qquad p_1^{(\gamma)} := \frac{\gamma c_0 - \gamma_0 c_\gamma}{\gamma - \gamma_0}.$$

By linearity, $P_\gamma := (p_1^{(\gamma)}, p_2^{(\gamma)}) \in C^2$. On $S_0 \cap S_\gamma$, whose size is at least $n - 2r$, the two line equations solve back to $f_1 = p_1^{(\gamma)}$ and $f_2 = p_2^{(\gamma)}$. Hence $P_\gamma \in \mathcal{L}_{2r}^{(2)}(f)$.

It remains to bound how many non-anchor slopes can map to the same pair $P = (p_1, p_2) \in \mathcal{L}_{2r}^{(2)}(f)$. Let

$$E_P := \{x \in D : (f_1(x), f_2(x)) \neq (p_1(x), p_2(x))\}, \qquad t := |E_P| \leq 2r.$$

For every slope γ mapping to this same P, the corresponding witness codeword is $p_1 + \gamma p_2$, and on its witness set S_γ we need

$$(f_1 - p_1) + \gamma(f_2 - p_2) = 0.$$

Outside E_P this holds automatically. Inside E_P, a coordinate with $f_2(x) - p_2(x) \neq 0$ determines at most one value of γ, and a coordinate with $f_2(x) - p_2(x) = 0 \neq f_1(x) - p_1(x)$ determines none. Distinct finite slopes therefore have disjoint vanishing coordinate sets inside E_P.

If $t \leq r$, then $D \setminus E_P$ has size at least $n - r$ and is a mutual extension set for P. A non-extending witness must include at least one coordinate of E_P at which the displayed tangent equation vanishes, so there are at most $t \leq r$ such slopes. If $r < t \leq 2r$, a witness of size at least $n - r$ must include at least $t - r$ coordinates of E_P at which the tangent equation vanishes. By disjointness, the number of such slopes is at most

$$\frac{t}{t - r} \leq r + 1.$$

Thus each pair in the doubled-radius pair list receives at most $r + 1$ non-anchor slopes. Adding back the single anchor gives $|B| \leq 1 + (r+1)|\mathcal{L}_{2r}^{(2)}(f)|$, and the stated bound follows after maximizing over f and dividing by q. □

7. Sparse reductions for the residual band

The reductions above identify the residual mutual obstruction through shortenings and doubled-radius pair lists. We now integrate the sharper sparse form: the mutual-only layer is not merely bounded by sparse data; it is exactly the sparse layer. This is useful for threshold determination because it separates the remaining task into a plain-CA problem and a budget-restricted sparse mutual problem.

7.1. **Exact sparsification of the mutual layer.**

Lemma 7.1 (one slope per witness set)**.** *Let $C \subseteq \mathbb{F}^D$ be linear, let (g_1, g_2) be a pair, and let $S \subseteq D$ be nonempty.*

1. *If $g_1|_S \in C|_S$ and $g_2|_S \in C|_S$, no slope has a failing witness supported on S.*
2. *If $g_2|_S \in C|_S$ and $g_1|_S \notin C|_S$, then $(g_1 + \gamma g_2)|_S \notin C|_S$ for every γ, so no slope has any witness supported on S.*
3. *If $g_2|_S \notin C|_S$, then $(g_1 + \gamma g_2)|_S \in C|_S$ for at most one γ; if such a slope exists, every witness of the form (c, S) for it fails.*

In particular, each set S carries a failing witness for at most one slope; and on any proximity-witness set, $g_1|_S \in C|_S$ if and only if $g_2|_S \in C|_S$, so a witness fails exactly when $g_2|_S \notin C|_S$.

Proof. $C|_S$ is a linear subspace of $\mathbb{F}^S$, and (c, S) being a witness means exactly $(g_1+\gamma g_2)|_S \in C|_S$. The first clause is the definition of mutual extension. For the second, if $(g_1 + \gamma g_2)|_S \in C|_S$ then $g_1|_S = (g_1 + \gamma g_2)|_S - \gamma g_2|_S \in C|_S$, a contradiction. For the third, if two distinct slopes $\gamma \neq \gamma'$ both had $(g_1 + \gamma g_2)|_S, (g_1 + \gamma' g_2)|_S \in C|_S$, subtracting would give $g_2|_S \in C|_S$; and mutual extension on S requires $g_2|_S \in C|_S$, so the witness fails. The final equivalence follows because on a witness set $(g_1 + \gamma g_2)|_S \in C|_S$, so each of $g_1|_S, g_2|_S$ lies in $C|_S$ exactly when the other does. □

Theorem 7.2 (sparsification of the mutual layer)**.** *For every linear code $C \subseteq \mathbb{F}^D$ and every $\delta \in (0, 1)$,*

$$\varepsilon_{\mathrm{mca}}(C, \delta) = \max\left(\varepsilon_{\mathrm{ca}}(C, \delta), \frac{\sigma_C(\delta)}{q}\right).$$

Proof. The inequality $\geq$ follows from Lemma 2.2 and from the fact that sparse pairs are among all pairs. Conversely fix a pair (f_1, f_2). If $\mathrm{dist}_2((f_1, f_2), C^{\equiv 2}) > \delta$, then no set of at least $(1 - \delta)n$ coordinates carries a pair explanation, so every proximity witness fails; hence the MCA-bad slopes are exactly the δ-close slopes, which for a far pair are exactly the CA-bad slopes. This contributes at most $q\varepsilon_{\mathrm{ca}}(C, \delta)$ slopes.

If instead $\mathrm{dist}_2((f_1, f_2), C^{\equiv 2}) \leq \delta$, choose $(p_1, p_2) \in C^{\equiv 2}$ attaining the column distance, with column error set E of size at most r, and put $\epsilon_i := f_i - p_i$. Then $\operatorname{supp} \epsilon_1 \cup \operatorname{supp} \epsilon_2 \subseteq E$. Translation by (p_1, p_2) is a bijection between witnesses of the two pairs at each slope, via $(c, S) \mapsto (c - p_1 - \gamma p_2, S)$, and preserves failure because translation by codewords preserves membership of each restriction in $C|_S$. Hence the MCA-bad slope set of (f_1, f_2) equals that of the sparse pair (ϵ_1, ϵ_2), whose size is at most $\sigma_C(\delta)$. □

Remark 7.3. Below half the minimum distance, Theorem 7.4 gives $\sigma_C(\delta) \leq r$; thus Theorem 7.2 recovers Theorem 4.2 as an equality statement in which the tangent term is precisely the sub-half-distance sparse layer. Above half the distance, the phrase "the mutual layer breaks down" should be replaced by the exact statement "the mutual layer equals the sparse layer."

7.2. **Support thresholds, normal form, and rigidity.**

Fix a sparse pair (ϵ_1, ϵ_2) with support union E', put $e := |E'| \leq r$, and write $v_\gamma := \epsilon_1 + \gamma\epsilon_2$. Call $j \in E'$ *active* if $\epsilon_2(j) \neq 0$, and let A be the number of active coordinates. Call γ *tangent* if $v_\gamma(j) = 0$ for some $j \in E'$; there are at most e tangent slopes. If $\epsilon_2 = 0$, there are no MCA-bad slopes, so in the sequel assume $A \geq 1$.

Theorem 7.4 (support threshold)**.** *Let C be linear with minimum weight $w_{\min}$. If $e \leq w_{\min} - 1 - r$, then every δ-MCA-bad slope of (ϵ_1, ϵ_2) is tangent. In particular, sparse mass beyond the tangent count requires $e \geq w_{\min} - r$.*

Proof. Let γ be bad with failing witness (z, S), $z \in C$, $v_\gamma|_S = z|_S$, $|S| \geq n-r$. Since v_γ vanishes off E', the codeword z vanishes on $S \setminus E'$, a set of size at least $n - r - e \geq n - w_{\min} + 1$; hence $\mathrm{wt}(z) \leq w_{\min} - 1$ and $z = 0$. Then $v_\gamma|_S = 0$. If γ were not tangent, v_γ would be nonzero at every point of E', forcing $S \cap E' = \emptyset$ and $\epsilon_2|_S = 0 \in C|_S$; by Lemma 7.1 the witness would extend, a contradiction. □

For Reed–Solomon codes set $m := n - k$, so $w_{\min} = m + 1$, and assume $r \leq m - 1$; this is the sub-capacity band. Define the ambiguity family

$$\mathcal{Z} := \{z \in C : \ \mathrm{wt}(z|_{D \setminus E'}) \leq r\},$$

which contains every possible failing-witness codeword, since off E' the mismatches of v_γ against z are exactly the support of z there.

Theorem 7.5 (pinning and normal form)**.** *Let $C = \mathrm{RS}[\mathbb{F}, D, k]$, and let γ be a δ-MCA-bad slope of (ϵ_1, ϵ_2).*

(1) *There exist $z \in \mathcal{Z}$ and an active $j \in E'$ with $v_\gamma(j) = z(j)$, so that*

$$\gamma = \frac{z(j) - \epsilon_1(j)}{\epsilon_2(j)}.$$

The values pinned by $z = 0$ are exactly the tangent slopes. For fixed z, at most $A \leq e$ slopes arise this way.

(2) *Every $z \in \mathcal{Z} \setminus \{0\}$ has the normal form*

$$z = h \prod_{x \in Z} (X - x)$$

with $Z \subseteq D \setminus E'$, $|Z| \geq n - e - r$, and $\deg h \leq e + r - m - 1$. In particular $\mathcal{Z} = \{0\}$ unless $e \geq m + 1 - r$, re-proving Theorem 7.4 for Reed–Solomon codes.

Proof. For (2), a nonzero $z \in \mathcal{Z}$ vanishes on at least $n - e - r$ points of $D \setminus E'$; collect them into Z and divide. Then $h := z / \prod_{x \in Z}(X - x)$ has degree at most $k - 1 - |Z| \leq e + r - m - 1$, which is negative when $e \leq m - r$.

For (1), let (z, S) be a failing witness for γ; as just noted, $z \in \mathcal{Z}$. Failure is inherited by supersets of S inside the agreement locus, so take S maximal: $S = D \setminus \mathrm{supp}(v_\gamma - z)$. Suppose no active coordinate is matched. Then $\mathrm{supp}(v_\gamma - z)$ consists of all active coordinates, those inactive $j \in E'$ with $\epsilon_1(j) \neq z(j)$, and $\mathrm{supp}(z) \setminus E'$, all independent of γ. On S, every point of $S \cap E'$ is inactive and matched, so $\epsilon_2|_S = 0 \in C|_S$ and $\epsilon_1|_S = z|_S \in C|_S$; off E' both ϵ_1 and, by maximality, z vanish on S. By Lemma 7.1 the witness extends, a contradiction. Thus some active coordinate is matched, giving the pinning formula. □

Theorem 7.6 (match rigidity)**.** *In the setting of Theorem 7.5, let γ be a non-tangent bad slope with maximal failing witness (z, S), $z \neq 0$, let $t \geq 1$ be its number of matched active coordinates, and let u be the number of unmatched inactive coordinates of E'. Then the closeness budget forces*

$$(A - t) + u + \mathrm{wt}\big(z|_{D \setminus E'}\big) \leq r, \qquad \textit{hence} \qquad t \geq A - e + (m + 1 - r) + u \geq A - e + m + 1 - r.$$

In particular, when every support coordinate is active ($A = e$), every non-tangent bad slope matches its witness at no fewer than $m+1-r$ coordinates, each match imposing one interpolation condition on z consistent with the single pinned value of γ.

Proof. The disagreement set of v_γ against z has size at most r and decomposes as the $A - t$ unmatched active coordinates, the u unmatched inactive coordinates, and the off-E' support of z; this is the budget identity. For the consequence, the normal form bounds the zero count: $z \neq 0$ vanishes on at least $n - e - \mathrm{wt}(z|_{D \setminus E'}) \geq n - e - r + (A - t) + u$ points off E', so $k - 1 \geq n - e - r + (A - t) + u$, i.e. $(A - t) + u \leq e + r - m - 1$. □

Remark 7.7 (the sparse value-set wall). One might hope to bound σ_C by the value sets $\{z(j) : z \in \mathcal{Z}\}$ through the pinning formula. This is vacuous once $e \geq m + 1 - r$: for any admissible zero set Z, the factor h has nonnegative degree and $z(j) = h(j) \prod_{x \in Z}(j - x)$ ranges over all

of $\mathbb{F}$. The genuine constraint is the coupling in Theorem 7.6: the same budget r pays for the off-support weight of z, the unmatched coordinates, and the t-fold interpolation consistency of z with a single slope. Bounding the number of slopes admitted by this coupled system is the sparse, budget-restricted form of the value-set frontier.

7.3. **A rider bound for the plain-CA side.**

Theorem 7.8 (rider bound below radius one half)**.** *Let $C \subseteq \mathbb{F}^D$ be linear, let $\delta \in (0, \frac{1}{2})$, put $r = \lfloor \delta n \rfloor$, and let (f_1, f_2) satisfy $\mathrm{dist}_2((f_1, f_2), C^{\equiv 2}) > \delta$. Let*

$$\mathcal{L} := \{(P_1, P_2) \in C^{\equiv 2} : \ \#\{j : (f_1(j), f_2(j)) = (P_1(j), P_2(j))\} \geq n - 2r\}.$$

Then the number of δ-CA-bad slopes is at most $1 + (r+1)|\mathcal{L}|$. Consequently

$$q\, \varepsilon_{\mathrm{ca}}(C, \delta) \leq 1 + (r+1) L_2(n - 2r),$$

where $L_2(a)$ denotes the largest interleaved pair-list size of C at column agreement a.

Proof. Let B be the bad set. If $|B| \leq 1$ there is nothing to prove. Fix $\gamma_1 \in B$ with witness codeword c_{γ_1} and agreement set S_{γ_1}, $|S_{\gamma_1}| \geq n - r$. For each $\gamma \in B \setminus \{\gamma_1\}$, with witness (c_γ, S_γ), the two equations on $S_{\gamma_1} \cap S_\gamma$, of size at least $n - 2r$, solve to

$$f_2 = P_2 := \frac{c_{\gamma_1} - c_\gamma}{\gamma_1 - \gamma}, \qquad f_1 = P_1 := c_{\gamma_1} - \gamma_1 P_2,$$

with $(P_1, P_2) \in C^{\equiv 2}$; thus every non-anchor slope rides some member of $\mathcal{L}$.

Fix one member $P = (P_1, P_2)$ and let E be its column disagreement set against (f_1, f_2). Since the pair is δ-far, $|E| \geq r + 1$. A rider γ agrees with $P_1 + \gamma P_2$ outside at most r coordinates, so it satisfies $\eta_1(j) + \gamma \eta_2(j) = 0$, where $(\eta_1, \eta_2) := (f_1 - P_1, f_2 - P_2)$ and $(\eta_1(j), \eta_2(j)) \neq (0, 0)$, at no fewer than $|E| - r$ coordinates $j \in E$; each coordinate of E admits at most one such slope. Double counting gives $\#\{\text{riders on } P\} \cdot (|E| - r) \leq |E|$, so each member carries at most $|E|/(|E| - r) \leq r + 1$ riders. □

Corollary 7.9 (doubly-sparse reduction of the sub-half CA band)**.** *In the setting of Theorem 7.8, every member of $\mathcal{L}$ certifies $\mathrm{dist}(f_i, C) \leq 2r/n$ for both i. Hence:*

1. *a δ-far pair one of whose components has $\mathrm{dist}(f_i, C) > 2\delta$ has at most one δ-CA-bad slope;*
2. *if $q\varepsilon_{\mathrm{ca}}(C, \delta) \geq 2$, the maximum is attained on pairs of the form $(c_1 + e_1, c_2 + e_2)$ with $c_i \in C$ and $\mathrm{wt}(e_i) \leq 2r$; since the CA-bad set is invariant under translation by $C^{\equiv 2}$, plain correlated agreement in this range is, up to a single slope, a problem about δ-far pairs both of whose components are $2r$-sparse.*

Proof. A member agrees with (f_1, f_2) on at least $n - 2r$ columns, so componentwise f_i is within $2r$ of $P_i \in C$. If some component is 2δ-far, then $\mathcal{L} = \emptyset$ and Theorem 7.8 gives at most one bad slope. For translation invariance, replacing (f_1, f_2) by $(f_1 - c_1, f_2 - c_2)$ shifts u_γ by the codeword $c_1 + \gamma c_2$, preserving distances to C and preserving column distance to $C^{\equiv 2}$; hence the bad set is unchanged and the maximizing far pair may be normalized to sparse components. □

Remark 7.10. When $n - 2r > \sqrt{(k-1)n}$, the pair-list $L_2(n - 2r)$ is polynomially bounded and Theorem 7.8 recovers the self-contained half-Johnson CA bound cited in Proposition 1.2. Past the Johnson radius, it converts the sub-half-radius part of the plain-CA band into an interpolation-deficient interleaved list problem for doubly sparse far pairs. The hypothesis $\delta < 1/2$ is essential in this statement; for challenge rates below $1/2$, the unresolved post-Johnson plain-CA band lies at radii at least $1/2$, so the older residual formulations of Theorems 6.2 and 6.4 must still be kept for that part.

7.4. **Conditional transfer.**

Theorem 7.11 (conditional transfer to the Johnson radius)**.** *Let $C = \mathrm{RS}[\mathbb{F}, D, k]$, let $\rho = k/n$, and let $\delta_0 \leq 1 - \sqrt{\rho} - \eta$ for some $\eta > 0$. If $\sigma_C(\delta) \leq P(n)$ for all $\delta \leq \delta_0$, then, importing the*

Johnson-regime proximity gap of [BCIKS20]*, namely* $\varepsilon_{\mathrm{ca}}(C,\delta) \le \mathrm{poly}_\eta(n)/q$ *for* $\delta \le 1-\sqrt{\rho}-\eta$*, we get*

$$\varepsilon_{\mathrm{mca}}(C,\delta) \le \frac{\max(\mathrm{poly}_\eta(n), P(n))}{q} \qquad (\delta \le \delta_0).$$

Thus the MCA safe frontier moves from one half of the minimum distance to the Johnson radius whenever the sparse mutual layer is polynomially bounded there.

Proof. Immediate from Theorem 7.2 and the quoted CA input. □

8. Barriers and what remains

The pincer above is not limited by lazy constants. Each mechanism stops for a structural reason: prefix floors have an entropy envelope, the deep-point conversion has an error ceiling, and the mutual layer has a genuine half-distance wall.

Proposition 8.1 (entropy envelope for prefix floors)**.** *In the setting of Lemma 3.1, write* $\beta := \log_2|B|$*,* $A := mc$ *and* $g := (A-k)/n$*, and let* $K \le k+1$*. If* $\mathrm{H}_2(\rho+g) \le \beta\,(g-\frac{c}{n})$*, then* $\binom{N}{m} \le |B|^w$*: the pigeonhole class is not guaranteed to exceed a single codeword, and no certificate of the form of Theorem 3.3 exists at agreement* A *and scale* c*. In particular, over any field with no proper subfield containing* D *and* $q \ge 2^{128}$ *(so* $\beta \ge 128$*), a certificate at scale* c *requires* $g < \frac{1}{128} + \frac{c}{n}$*; since a useful certificate also needs* $\binom{N}{m} > \frac{q}{k} \ge 2^{88}$*, hence* $N \ge 89$ *and* $c \le n/89$*, every certified gap is below* $\frac{1}{128}+\frac{1}{89} < 2^{-5.6}$*. At the ordinary scale* $c=1$ *used in Corollary 3.4 this says the route cannot pass much beyond* $1/128$*; at the quadratic scale* $c=2$ *used in Corollary 3.5 it gives the familiar* $1/128 + 2/n$ *envelope. For deployed rows whose domains lie in small subfields (*$\beta = 31$*) the same envelope, now* $\mathrm{H}_2(\rho+g^*) = g^*\beta$*, is wider, and it is reached and saturated in* [Cho26b].

Proof. Here $w = m - \lceil K/c \rceil \ge m-(k+c)/c = (A-k-c)/c$, so by (1), $\log_2\binom{N}{m} \le \frac{n}{c}\mathrm{H}_2(A/n) \le \frac{n}{c}\cdot\beta(g-\frac{c}{n}) = \beta\frac{gn-c}{c} \le \beta w$. The instantiation takes $\beta = \log_2 q \ge 128$ and $\mathrm{H}_2 \le 1$. □

Proposition 8.2 (ceiling of the conversion)**.** *Let* δ *be as in Theorem 3.2 and* $T := \frac{1}{k}(1-\frac{n}{q})$*. If some word* u *has* $|\Lambda(\mathrm{RS}[\mathbb{F},D,k+1],\delta,u)| \ge 1+\kappa qT$ *with* $\kappa > 0$*, then* $\varepsilon_{\mathrm{ca}}(C,\delta) \ge \frac{\kappa}{\kappa+1}T$*. Conversely, no list bound, however large, certifies* $\varepsilon_{\mathrm{ca}} \ge T$ *through Theorem 3.2: the certified error tends to* T *from below as* $\kappa \to \infty$*.*

Proof. Put $x := \varepsilon_{\mathrm{ca}}(C,\delta)$; if $x \ge T$ there is nothing to prove, so let $x < T$ and $\eta := x/T < 1$. Theorem 3.2 applies with this η and yields $\kappa qT \le qx/(1-x/T)$, so $\kappa(T-x) = \kappa T(1-x/T) \le x$, i.e. $x \ge \kappa T/(\kappa+1)$. The converse is read from the same inequality. □

Remark 8.3 (why half the distance is a wall). The forcing step in Theorems 4.1 and 4.2 — a codeword vanishing outside a $2r$-set must be zero — fails precisely when $2r \ge w_{\min}$. For $C = \mathrm{RS}[\mathbb{F},D,k]$ it fails with room to spare: codewords supported inside a fixed set W with $|W| = 2r$ are evaluations of polynomials of degree $< k$ vanishing on the $n-2r$ points off W, a space of dimension exactly $\max(0, k-n+2r) = \max(0, 2r-(n-k))$. Proposition 6.3 shows that this is a real MCA obstruction, not merely a proof artifact.

The remaining tasks now have a narrower and more concrete form. The unsafe side is settled by prefix-floor certificates; the safe side is limited by two separate sparse problems.

Problem 8.4 (sparse mutual layer)**.** For $C = \mathrm{RS}[\mathbb{F},D,k]$ in the parameter box of Theorem 1.1, bound $\sigma_C(\delta)$ at target scale for

$$\frac{1-\rho}{2} < \delta < 1-\rho-\frac{s_\rho}{n}.$$

Equivalently, bound the number of slopes admitted by the budget-coupled system of Theorems 7.5 and 7.6: witnesses of the form

$$z = h\prod_{x\in Z}(X-x), \qquad \deg h \le e+r-(n-k)-1,$$

with at least $A - e + (n-k) + 1 - r$ active interpolation matches consistent with a single slope and with total closeness budget r. A polynomial bound for $\sigma_C(\delta)$ up to $1 - \sqrt{\rho} - \eta$, combined with [BCIKS20], moves the MCA safe frontier to the Johnson radius by Theorem 7.11; beyond the Johnson radius it must be combined with a plain-CA input such as Problem 8.5.

Problem 8.5 (plain CA via deficient pair lists for doubly sparse far pairs)**.** Determine $\varepsilon_{\mathrm{ca}}(C, \delta)$ in the residual plain-CA interval

$$1 - \sqrt{\rho} < \delta < 1 - \rho - \frac{s_\rho}{n}.$$

In the sub-half-radius portion of this interval, equivalently by Theorem 7.8 and Corollary 7.9, bound $L_2(n - 2\lfloor \delta n \rfloor)$ for δ-far pairs whose two components are $2\lfloor \delta n \rfloor$-sparse up to codewords. This covers the whole rate-1/2 residual CA band, but not the post-Johnson portions of the lower-rate challenge rows, which lie at radii $\geq 1/2$ and remain governed by the original plain-CA/list-size problem. The original question below the coarse cap edge $1 - \rho - g_\rho$ is already negative on its upper slice by Corollary 6.1, positive for plain CA up to the Johnson radius by [BCIKS20, BCHKS25], and open only in the displayed middle range.

Problem 8.6 (legacy residual shortening and pair-list images)**.** For $r = \lfloor \delta n \rfloor$ in the same middle interval, the older formulation is to bound the residual term $R_C(r)$ of Theorem 6.2, or equivalently the doubled-radius pair-list quantity $L^{(2)}_{2r}(C)$ of Theorem 6.4. A target-level bound

$$r + R_C(r) \leq 2^{-128} q$$

together with a solution of Problem 8.5 would close the MCA threshold in the middle band. The sparse equality Theorem 7.2 refines this legacy formulation: it says that the true mutual residue is exactly $\sigma_C(\delta)$, and Theorems 7.5 and 7.6 identify the sparse budget-restricted value-set system that must be counted.

For deployed subfield rows the residual search must also separate base-valued and genuinely extension-valued line witnesses. In the KoalaBear sextic row, $D \subseteq \mathbb{B}$ but the line field is the ambient extension $\mathbb{F}/\mathbb{B}$; the confinement lemma of [Cho26b] shows that $\mathbb{B}$-valued line words contribute bad-slope density at most $|\mathbb{B}|/|\mathbb{F}| < 2^{-154}$, far below the target 2^{-128}. Thus any target-level deployed obstruction in that row must use genuinely $\mathbb{F}$-valued line data.

Thus the current complete picture is this. Small fields are degenerate. Large fields are safe to one third of the distance by a self-contained theorem, often safe farther by the self-contained half-Johnson certificate of Proposition 1.2, and safe to one half of the distance with the single BCIKS import. They are unsafe, already for plain correlated agreement, from $1 - \rho - s_\rho/n$ to capacity; over deployed subfield rows, optimized companion floors push this unsafe frontier much farther left and print finite staircase certificates. What remains is not the original broad pair of problems, but the middle plain-CA interval of Problem 8.5 and the sparse mutual kernel of Problem 8.4, with Problem 8.6 recording the older shortening/pair-list formulation for comparison.

References

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

[BCHKS25] E. Ben-Sasson, D. Carmon, U. Haböck, S. Kopparty, and S. Saraf. On proximity gaps for Reed–Solomon codes. IACR Cryptology ePrint Archive, Report 2025/2055, 2025. 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 *Proc. 61st IEEE Symposium on Foundations of Computer Science (FOCS)*, 2020. Extended manuscript: IACR Cryptology ePrint Archive, Report 2020/654.

[Cho26a] P. Chojecki. Capacity-edge obstructions to Reed–Solomon mutual correlated agreement over smooth multiplicative domains. Manuscript, 2026.

[Cho26b] P. Chojecki. Universal field-size caps and a two-sided sandwich for mutual correlated agreement on smooth Reed–Solomon domains. Manuscript, 2026.

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

[PP26] The Proximity Prize: $1M Reed–Solomon Challenge. Preliminary release, 2026. https://proximityprize.org/.