Capacity-Edge Obstructions to Reed–Solomon Mutual Correlated Agreement over Smooth Multiplicative Domains

Przemek Chojecki
ulam.ai

June 11, 2026

Abstract

We give a self-contained disproof of the up-to-capacity mutual correlated agreement (MCA) conjecture for smooth multiplicative Reed–Solomon domains in its support-wise, line, no-slack form, at the prize rates $\rho \in \{1/2, 1/4, 1/8, 1/16\}$. The organizing mechanism is the locator identity: if many exact restricted sums of a smooth quotient Q fill the field, then the line $x^{k+a} + zx^k$ has many bad slopes at radius $1 - \rho - 1/|Q|$.

The prime-field consequences are explicit. Over BabyBear, KoalaBear, and $3 \cdot 2^{30} + 1$, for every smooth subgroup domain of size divisible by 2^{18}, the MCA error is identically 1 on intervals beginning at $1 - \rho - 2^{-18}$ for all four prize rates, with the sharper 2^{-17} gap at rates $1/2$ and $1/4$. Over the Fermat primes 17, 257, and 65537 with the full multiplicative domain, the error is at least $1 - 1/p$ at radius $1 - \rho - 1/(2\log_2 n)$ for $\rho \in \{1/2, 1/4\}$ (the pair $(17, 1/4)$ by exhaustive verification). Infinitely many prime fields also have inverse-polylogarithmic bad-slope density at the same logarithmic scale.

The worst-case list-decoding analogue also fails in the no-slack regime. At the prize rates, every power-of-two subgroup domain of order $n \geq (\log_2 q)^{1+\varepsilon}$ admits explicit received words with superpolynomially many codewords within radius $1 - \rho - (\log_2 q)^{-1-\varepsilon}$. The general divisor-level list bound is stated for arbitrary rates whenever the required divisibility condition $\rho N \in \mathbb{Z}$ holds.

The same locator framework gives generated extension-field examples. Under the tower condition $\mathrm{ord}_{md}(p) = d$, the subgroup $D \leq \mathbb{F}_{p^d}^\times$ of order md decomposes as $\bigsqcup_{i=0}^{d-1} \zeta^i H$ with $H \leq \mathbb{F}_p^\times$, and Dias da Silva–Hamidoune fills the field coordinate by coordinate. This gives error 1 for Fermat and Proth-type smooth towers and non-negligible density bounds in borderline cases such as Goldilocks.

The results are deliberately no-slack statements: they prove concrete necessary slack floors and worst-case list lower bounds. They do not assert a negative result for formulations that impose sufficient explicit slack, nondegenerate curve constraints, or protocol-specific agreement restrictions.

1 The conjecture

The Proximity Prize [1, 5, 6] concerns Reed–Solomon codes

$$\mathrm{RS}[\mathbb{F}, D, k] = \{(P(x))_{x \in D} : \deg P < k\}, \qquad n = |D|,\ \rho = k/n,$$

over *smooth* multiplicative domains. In this paper all stated counterexamples use multiplicative subgroups $D \leq \mathbb{F}^\times$ of power-of-two order; the same locator calculation also applies to multiplicative cosets after the evident rescaling, but no coset generality is needed below. Correlated-agreement theorems control, for a random z, whether closeness of $f + zg$ to the code forces closeness of f and g

individually; the *mutual* (support-wise) version asks this on the same agreement set, which is what FRI/WHIR-style extractors consume [7, 8]. Proximity gaps and (M)CA are known throughout the Johnson regime $\delta < 1 - \sqrt{\rho}$ [2], and the prize challenge is the region between Johnson and capacity $1 - \rho$. The optimistic endpoint — conjectured in various forms since proximity gaps were introduced [2], and the natural reading of the grand challenge — is:

Conjecture 1.1 (Up-to-capacity MCA; no-slack support-wise line form)**.** *Let $C = \mathrm{RS}[\mathbb{F}, D, \rho n]$ be a smooth-domain Reed–Solomon code, $\rho \in \{1/2, 1/4, 1/8, 1/16\}$. For every $\delta < 1 - \rho$,*

$$\varepsilon_{\mathrm{mca}}(C, \delta) \;\le\; \mathrm{negl}(q) \qquad \big(\textit{concretely: } \le 2^{-128} \textit{ for the prize fields}\big),$$

where $\varepsilon_{\mathrm{mca}}$ is the support-wise line-MCA error of Definition 1.3 below. List-decoding analogue: for every $\delta < 1 - \rho$, every received word has at most $\mathrm{poly}(q)$ codewords within relative distance δ.

Remark 1.2 (What exactly is being refuted)**.** The prize materials phrase the challenge as determining the largest δ with negligible MCA/list error [1, 5]; Conjecture 1.1 is the assertion that this δ reaches capacity, transcribed in the minimal no-slack, same-support, two-word (line) form. Everything below refutes *this* form, quantitatively and with explicit witnesses. If a formulation includes a slack parameter τ, a curve variant, or a different agreement notion, our results convert into necessary conditions on that formulation (Section 8): in particular any slack $\tau \le 2^{-18}$ is insufficient on BabyBear/KoalaBear domains with $2^{18} \mid n$, and $\tau \le c_\rho / \log p$ is insufficient on infinitely many smooth prime fields. We do not claim anything about slacked formulations above these floors.

Definition 1.3 (Support-wise line-MCA error)**.** For a linear code $C \subseteq \mathbb{F}^D$ and a line $u_z = f + zg$, the parameter z is *bad at radius δ* if there is $S \subseteq D$, $|S| \ge (1 - \delta)n$, and $c \in C$ with $u_z|_S = c|_S$, while no pair $c_f, c_g \in C$ has $f|_S = c_f|_S$ and $g|_S = c_g|_S$. Then

$$\varepsilon_{\mathrm{mca}}(C, \delta) = \max_{f,g} \frac{\#\{z \in \mathbb{F} : \; z \text{ bad}\}}{|\mathbb{F}|}.$$

For $A \subseteq \mathbb{F}$ and $h \ge 0$, write $h^{\wedge}A = \{a_1 + \cdots + a_h : \; a_i \in A \text{ distinct}\}$.

2 The disproof

Theorem 2.1 (Main theorem)**.** *Conjecture 1.1 is false. Specifically:*

(a) ***(Error one on an interval; deployed fields.)*** *Let p be prime, $D \le \mathbb{F}_p^\times$ a subgroup of order n, $0 < \rho \le 1/2$, $k = \rho n \in \mathbb{Z}$, and let $N \mid n$ satisfy $\rho N \in \mathbb{Z}$ and*

$$(\rho N + 1)((1 - \rho)N - 1) + 1 \ge p.$$

Then

$$\varepsilon_{\mathrm{mca}}\big(\mathrm{RS}[\mathbb{F}_p, D, k],\, \delta\big) = 1 \qquad \textit{for every } \delta \in \big[\,1 - \rho - \tfrac{1}{N},\; 1\,\big].$$

For BabyBear, KoalaBear, and $3 \cdot 2^{30} + 1$, the divisor $N = 2^{18}$ qualifies at all four prize rates, and $N = 2^{17}$ qualifies at rates $1/2$ and $1/4$: Conjecture 1.1 fails with the largest possible error, on a radius interval of length $\rho + 2^{-18}$ for all prize rates, for every smooth subgroup domain with $2^{18} \mid n$.

(b) ***(Error $1-1/p$ at $1-\rho-\Theta(1/\log n)$; linear-size fields.)*** *For the Fermat primes $p = 2^M+1 \in \{17, 257, 65537\}$, the full domain $D = \mathbb{F}_p^\times$ ($n = p-1$, $q = n+1$), and $\rho \in \{1/2, 1/4\}$ — at $\rho = 1/4$ for $p \in \{257, 65537\}$, where $M \geq 8$ as Lemma 3.4 requires; the remaining pair $(p, \rho) = (17, 1/4)$ holds as well, by the exhaustive computation of appendix A —*

$$\varepsilon_{\mathrm{mca}}\Big(\mathrm{RS}[\mathbb{F}_p, D, \rho n],\ 1-\rho-\frac{1}{2\log_2 n}\Big)\ \geq\ 1-\frac{1}{p},$$

and the same at every larger radius.

(c) ***(Non-negligible error at $1-\rho-O(1/\log p)$; infinitely many fields.)*** *For each prize rate there are infinitely many primes p with power-of-two subgroups Q, $|Q| = N = \Theta_\rho(\log p)$, such that $\varepsilon_{\mathrm{mca}}(\mathrm{RS}[\mathbb{F}_p, Q, \rho N],\ 1-\rho-1/N) \geq (\log_2 p)^{-6}$, an inverse-polynomial function of the security parameter, exceeding 2^{-128} for every $p < 2^{2^{21}}$.*

(d) ***(Worst-case list bound; divisor-level universal statement.)*** *For every finite field $\mathbb{F}$ of size q, every subgroup $D \leq \mathbb{F}^\times$ of order n, every $0 < \rho < 1$ with $\rho n \in \mathbb{Z}$, and every divisor $N \mid n$ with $\rho N \in \mathbb{Z}$, there is $z \in \mathbb{F}$ such that the received word $u_z(x) = x^{k+a} + zx^k$ ($a = n/N$) has at least $\binom{N}{\rho N+1}/q$ codewords of $\mathrm{RS}[\mathbb{F}, D, \rho n]$ within distance $1-\rho-1/N$. Consequently, for each fixed prize rate $\rho \in \{1/2, 1/4, 1/8, 1/16\}$ and each fixed $\varepsilon > 0$, if n is a power of two and $n \geq (\log_2 q)^{1+\varepsilon}$, then the maximum list size at radius $1-\rho-(\log_2 q)^{-1-\varepsilon}$ is superpolynomial in q for all sufficiently large q.*

Remark 2.2 (Status and scope)**.** The theorem above is intentionally separated by strength. Parts (a), (b), and (d) are elementary consequences of the locator identity and Dias da Silva–Hamidoune. Part (c) is weaker than the natural constant-density small-subgroup conjecture, but it is unconditional: it gives inverse-polylogarithmic bad-slope density at logarithmic subgroup size. No unproved equidistribution or small-subgroup density hypothesis is used anywhere in this paper. Slacked, curve, and exact-threshold formulations are not claimed here; the results below are the no-slack obstructions and necessary slack floors such formulations must clear.

Parts (a), (b) and (d) need only the four elementary lemmas of Section 3; part (c) is the cyclotomic sieve theorem proved in Section 4. The external inputs are exactly Dias da Silva–Hamidoune, used in Lemma 3.2, and Siegel–Walfisz, used in Theorem 4.3; all reductions from those inputs to MCA/list witnesses are proved here.

3 Four lemmas

Lemma 3.1 (Quotient locator)**.** *Let $D \leq \mathbb{F}^\times$ have order n, let $N \mid n$, $a = n/N$, $Q = D^a$ (the subgroup of order N), $1 \leq k$, $a \mid k$, $k+a \leq n$, and $\ell = k/a+1 \leq N$. For the line $f = x^{k+a}$, $g = x^k$ on D, every $z \in -\ell^\wedge Q$ is bad at radius $1-\frac{k}{n}-\frac{1}{N}$. Hence $\varepsilon_{\mathrm{mca}}(\mathrm{RS}[\mathbb{F}, D, k], 1-\rho-\frac{1}{N}) \geq |\ell^\wedge Q|/q$.*

Proof. Pick $A \subseteq Q$, $|A| = \ell$, $\sum_{b\in A} b = -z$, and set $S_A = \{x \in D : x^a \in A\}$, of size $a\ell = k+a$. The locator $L_A(X) = \prod_{b\in A}(X^a - b)$ expands as $X^{k+a} + zX^k + R_A(X)$ with $\deg R_A < k$, because its second-highest coefficient is $-\sum_{b\in A} b$ in degree $a(\ell-1) = k$ and all monomial degrees are multiples of a. Vanishing of L_A on S_A gives $u_z|_{S_A} = (-R_A)|_{S_A}$, a degree-$< k$ explanation of u_z on $k+a$ points. But $g = x^k$ agrees with no degree-$< k$ polynomial on more than k points, and $|S_A| = k+a > k$. So z is bad, for every $z \in -\ell^\wedge Q$. □

Lemma 3.2 (Coverage; Dias da Silva–Hamidoune [9]). *For $A \subseteq \mathbb{F}_p$, $|A| = m$, and $1 \le r \le m$: $|r^\wedge A| \ge \min\{p,\ r(m-r)+1\}$. In particular, if $Q \le \mathbb{F}_p^\times$ has order N, $\rho \le 1/2$, $\rho N \in \mathbb{Z}$, and*

$$(\rho N + 1)\big((1-\rho)N - 1\big) + 1 \ge p,$$

then $(\rho N+1)^\wedge Q = \mathbb{F}_p$. The simpler sufficient condition $\rho(1-\rho)N^2 \ge p$ implies this exact condition, since the left side equals $\rho(1-\rho)N^2 + (1-2\rho)N$.

Lemma 3.3 (Monotonicity). *$\varepsilon_{\mathrm{mca}}(C,\delta)$ is nondecreasing in δ, and so is the maximum list size at radius δ.*

Proof. A witness set S with $|S| \ge (1-\delta)n$ also has $|S| \ge (1-\delta')n$ for $\delta' \ge \delta$, and both badness conditions depend on S only. A list at radius δ is a subset of the list at radius δ'. □

Lemma 3.4 (Fermat digit lemma). *Let $p = 2^M + 1$ be prime, $M = 2^t \ge 4$, and $Q = \langle 2\rangle \le \mathbb{F}_p^\times$, of order $N = 2M$, so $Q = \{\pm 2^j : 0 \le j < M\}$. Then for $r = M+1$ and (if $M \ge 8$) for $r = M/2+1$,*

$$r^\wedge Q = \mathbb{F}_p \setminus \{0\}.$$

Proof. An r-subset of Q is a pair $J^+, J^- \subseteq \{0,\dots,M-1\}$ with $|J^+|+|J^-| = r$ and sum $s = \sum_j c_j 2^j$, $c_j = \mathbf{1}[j \in J^+] - \mathbf{1}[j \in J^-] \in \{-1,0,1\}$; positions in $J^+ \cap J^-$ contribute matched zero pairs. A digit vector of support w is realizable by an r-subset iff $w \le r$, $w \equiv r \pmod 2$, and $(r-w)/2 \le M - w$.

0 is excluded: r is odd in both cases ($M, M/2$ even), so w is odd, so s is a nonzero integer with $|s| \le 2^M - 1 < p$.

Everything else is hit: given $y \in \mathbb{F}_p \setminus \{0\}$, choose the lift $s \equiv y \pmod p$ with $1 \le |s| \le 2^{M-1}$ (possible since $p = 2^M+1$). For $r = M+1$: if $|s| = 2^{M-1}$, the single digit at $M-1$ has $w = 1$, odd, done. Otherwise take the binary digits of $|s|$ (with the sign of s), supported in $\{0,\dots,M-2\}$, of weight $w_1 \le M-1$. If $w_1 \not\equiv r \pmod 2$ then $w_1 \le M-2$ (since $w_1 = M-1$ forces $s = \pm(2^{M-1}-1)$, whose weight $M-1 \equiv M+1 \pmod 2$), and rewriting the top digit $\pm 2^h \mapsto \pm(2^{h+1} - 2^h)$ into the free slot $h+1 \le M-1$ raises the weight by one. In all cases $1 \le w \le M-1 = 2M-r$, the parity matches, and padding completes the subset. For $r = M/2+1$: use the nonadjacent form (NAF) of s. Since $|s| \le 2^{M-1}$, no NAF digit occurs in position M or higher: if the top digit occurred in position $M' \ge M$, nonadjacency would let the lower tail cancel at most $2^{M'-2} + 2^{M'-4} + \cdots < 2^{M'}/3$, leaving magnitude $> \frac{2}{3}2^{M'} \ge \frac{2}{3}2^M > 2^{M-1}$. Thus the support lies in $\{0,\dots,M-1\}$ and has weight $w_1 \le \lceil M/2 \rceil = M/2$. If the parity is wrong, then the support is not the singleton $\{M-1\}$ (that case has odd weight, matching r, because $M/2$ is even). Hence some occupied position $h < M-1$ has an unoccupied successor $h+1$, by nonadjacency; rewriting $\pm 2^h$ as $\pm(2^{h+1} - 2^h)$ raises the weight by one, keeps all positions in range, and gives $w \le M/2 + 1 = r$ with the required odd parity. Padding by opposite pairs is then possible since $w \le r \le M-1$. □

4 The cyclotomic sieve theorem

This section proves part (c) of Theorem 2.1. Throughout, $\mathrm{H}(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy and

$$\gamma_\rho = \tfrac{1}{2}\big(\mathrm{H}(x_\rho) + x_\rho\big), \qquad x_\rho = \min\{2\rho,\ 2/3\},$$

so that

$$\gamma_{1/2} = \tfrac{1}{2}\log_2 3 \approx 0.7925, \quad \gamma_{1/4} = 0.75, \quad \gamma_{1/8} \approx 0.5306, \quad \gamma_{1/16} \approx 0.3343.$$

Fix a power of two $N = 2^s \geq 8$ and let $\zeta = \zeta_N \in \mathbb{Q}(\zeta_N)$ be a primitive N-th root of unity. The field $K = \mathbb{Q}(\zeta_N)$ has degree $\varphi(N) = N/2$, its ring of integers is $\mathbb{Z}[\zeta]$ with power basis $1, \zeta, \ldots, \zeta^{N/2-1}$, and $\zeta^{N/2} = -1$. For a subset $A \subseteq \mathbb{Z}/N$ put $\sigma_A = \sum_{a \in A} \zeta^a \in \mathbb{Z}[\zeta]$. Pairing the exponents into opposite pairs $\{j,\, j + N/2\}$ for $0 \leq j < N/2$ and using $\zeta^{j+N/2} = -\zeta^j$,

$$\sigma_A = \sum_{j=0}^{N/2-1} c_j(A)\, \zeta^j, \qquad c_j(A) = \mathbf{1}[j \in A] - \mathbf{1}[j + \tfrac{N}{2} \in A] \ \in \{-1, 0, 1\}. \tag{1}$$

Since $1, \zeta, \ldots, \zeta^{N/2-1}$ are linearly independent over $\mathbb{Q}$, the algebraic value σ_A is determined by, and determines, the digit vector $c(A)$.

Lemma 4.1 (Exact-support value family)**.** *Let $r \geq 1$ and let w satisfy*

$$1 \leq w \leq \min\{r,\ N/2\}, \qquad w \equiv r \pmod 2, \qquad \frac{r-w}{2} \leq \frac{N}{2} - w.$$

Then the set

$$V_{r,w} = \Big\{ \textstyle\sum_j c_j \zeta^j : \ c \in \{-1,0,1\}^{N/2},\ |\operatorname{supp} c| = w \Big\}$$

consists of $\binom{N/2}{w} 2^w$ pairwise distinct nonzero elements of $\mathbb{Z}[\zeta]$, and every $v \in V_{r,w}$ equals σ_A for some $A \subseteq \mathbb{Z}/N$ with $|A| = r$.

Proof. Distinctness and nonvanishing are immediate from the basis property and $w \geq 1$. Given a digit vector c of support w, build A as follows: for each j with $c_j = 1$ put $j \in A$; for each j with $c_j = -1$ put $j + N/2 \in A$; this contributes w elements and realizes the value by (1). Then choose $b = (r-w)/2$ indices j outside $\operatorname{supp} c$ — possible since $b \leq N/2 - w$ — and for each put *both* j and $j + N/2$ into A; each such opposite pair contributes $\zeta^j - \zeta^j = 0$ to the sum and 2 to the cardinality. The resulting A has $|A| = w + 2b = r$ and $\sigma_A = v$. □

Lemma 4.2 (Granularity)**.** *Write $W(w) = \binom{N/2}{w} 2^w$ and let $r = \rho N + 1$ with $0 < \rho \leq 1/2$. The admissible w in Lemma 4.1 form the set $\{w \leq \min(r, N-r) : \ w \equiv r\ (2)\}$ together with $w = r$ when $r \leq N/2$; on consecutive admissible values, W changes by a multiplicative factor at most N^2, and*

$$\max_{w \text{ admissible}} W(w) \ \geq \ 2^{\gamma_\rho N\,(1-o(1))} \qquad (N \to \infty).$$

Proof. The third condition of Lemma 4.1 reads $w \leq N - r$, giving the stated admissible range (for $\rho = 1/2$, $\min(r, N-r) = N/2 - 1$; for $\rho < 1/2$, the binding cap is $w \leq r$). Single steps satisfy $W(w+1)/W(w) = 2(N/2 - w)/(w+1) \in [2/N,\ N]$, so parity steps of two change W by a factor in $[4/N^2, N^2]$. For the maximum: the exponent of $W(xN/2)$ is $(N/2)(\mathrm{H}(x) + x)(1 + o(1))$, maximized at $x = 2/3$ when unconstrained and at the cap $x = 2\rho$ when $\rho < 1/3$; both cases give the exponent $\gamma_\rho N$ by the definition of x_ρ. □

Theorem 4.3 (Cyclotomic sieve)**.** *Fix $\rho \in \{1/2, 1/4, 1/8, 1/16\}$. For every sufficiently large X there exist a power of two*

$$N \asymp_\rho \log X, \qquad N \leq \Big(\frac{2}{\gamma_\rho} + o(1)\Big) \log_2 X,$$

and at least $\dfrac{X}{6N \log X}$ primes $p \in (X, 2X]$ with $N \mid p - 1$ such that the subgroup $Q \leq \mathbb{F}_p^\times$ of order N satisfies

$$|(\rho N + 1)^\wedge Q| \ \geq \ \frac{p}{(\log_2 p)^6}.$$

In particular there are infinitely many such primes, and for each of them

$$\varepsilon_{\mathrm{mca}}\Big(\mathrm{RS}[\mathbb{F}_p, Q, \rho N],\, 1-\rho-\tfrac{1}{N}\Big) \;\geq\; \frac{1}{(\log_2 p)^6},$$

an inverse-polynomial function of the security parameter $\lambda = \log_2 p$, hence non-negligible; it exceeds 2^{-128} whenever $\log_2 p \leq 2^{21}$.

Proof. Let $r = \rho N + 1$ throughout, and set the target $T = X/(\log_2 X)^3$.

Choice of N and w. Let N be the smallest power of two with $N \geq 16$ (so $\rho N \in \mathbb{Z}$ for every prize rate) and $\max_w W(w) \geq T$, where the maximum is over admissible w as in Lemma 4.2. The upper bound from Lemma 4.2 and minimality give $N \leq (2/\gamma_\rho + o(1)) \log_2 X$. Conversely, the trivial bound $\max_w W(w) \leq 3^{N/2}$ gives $N \geq (2/\log_2 3 - o(1)) \log_2 X$, so $N \asymp_\rho \log X$. Since W starts below T at the smallest admissible w (namely $W \leq N^2$ there) and exceeds T at the maximizer, Lemma 4.2 provides an admissible w_0 with

$$\frac{T}{N^2} \;\leq\; W := W(w_0) \;\leq\; T.$$

Let $V = V_{r,w_0} \subseteq \mathbb{Z}[\zeta_N]$ be the corresponding value family, $|V| = W$.

Primes and reduction. Let $\mathcal{P}$ be the set of primes $p \in (X, 2X]$ with $p \equiv 1 \pmod N$. Since $N \leq (\log X)^2$, the Siegel–Walfisz theorem [16] gives $|\mathcal{P}| \geq X/(3\varphi(N)\log X) \geq X/(3N \log X)$ for all large X. For $p \in \mathcal{P}$ fix a degree-one prime $\mathfrak{p}$ of $\mathbb{Z}[\zeta_N]$ above p (one exists because p splits completely, p being odd and $\equiv 1 \bmod N$), with reduction map $\theta_\mathfrak{p} : \mathbb{Z}[\zeta_N] \to \mathbb{F}_p$ sending ζ_N to an element of multiplicative order N. Then $\theta_\mathfrak{p}$ maps $\{\zeta^a : a \in \mathbb{Z}/N\}$ bijectively onto the subgroup $Q \leq \mathbb{F}_p^\times$ of order N, and by Lemma 4.1,

$$\theta_\mathfrak{p}(V) \;\subseteq\; r^{\wedge} Q.$$

Collision counting. For $p \in \mathcal{P}$ let C_p be the number of unordered pairs $\{v, v'\} \subseteq V$, $v \neq v'$, with $\theta_\mathfrak{p}(v) = \theta_\mathfrak{p}(v')$, i.e. $\mathfrak{p} \mid v - v'$. Each difference $\delta = v - v'$ is a nonzero element of $\mathbb{Z}[\zeta_N]$ whose coordinates in the power basis lie in $\{-2, \ldots, 2\}$, so every archimedean conjugate satisfies $|\sigma(\delta)| \leq N$, whence $0 < |\mathrm{N}_{K/\mathbb{Q}}(\delta)| \leq N^{N/2}$. If $\mathfrak{p} \mid \delta$ then $p \mid \mathrm{N}(\delta)$, and the number of primes exceeding X that divide a nonzero integer of absolute value at most $N^{N/2}$ is at most

$$\kappa := \frac{(N/2)\log N}{\log X} = O(\log\log X),$$

using $N = O(\log X)$. Therefore

$$\sum_{p \in \mathcal{P}} C_p \;\leq\; \binom{W}{2}\kappa \;\leq\; W^2\kappa.$$

By Markov's inequality, at least half of the primes in $\mathcal{P}$ satisfy

$$C_p \;\leq\; \frac{2W^2\kappa}{|\mathcal{P}|} \;\leq\; \frac{6\,W^2\,\kappa\,N\log X}{X} \;\leq\; W \cdot \frac{6\,\kappa\,N\log X}{(\log_2 X)^3} \;=\; W \cdot O\Big(\frac{\log\log X}{\log X}\Big) \;\leq\; \frac{W}{2}$$

for all large X, where the middle inequality uses $W \leq T = X/(\log_2 X)^3$.

Conclusion. Discarding one element of each colliding pair, for these primes

$$|r^{\wedge} Q| \;\geq\; |\theta_\mathfrak{p}(V)| \;\geq\; W - C_p \;\geq\; \frac{W}{2} \;\geq\; \frac{X}{2N^2(\log_2 X)^3} \;\geq\; \frac{p}{(\log_2 p)^6}$$

for all large X, since $N^2 = O((\log_2 X)^2)$ and $p \leq 2X$. The MCA statement follows from Lemma 3.1 applied with $D = Q$ and $a = 1$ (so $\ell = r = \rho N + 1$ and $|\ell^{\wedge} Q|/p \geq (\log_2 p)^{-6}$); equivalently, from Lemma 3.1 for any larger smooth domain D with $Q \leq D \leq \mathbb{F}_p^\times$ when one exists. Finally, $(\log_2 p)^6 \leq 2^{128}$ iff $\log_2 p \leq 2^{128/6}$, and $128/6 > 21$. □

5 Proof of Theorem 2.1

(a). Let $a = n/N$ and $Q = D^a$. Then $a \mid k$ ($k/a = \rho N \in \mathbb{Z}$) and $\ell = \rho N + 1$. By Lemma 3.2, $\ell \hat{} Q = \mathbb{F}_p$, so by Lemma 3.1 every $z \in \mathbb{F}_p$ is bad at radius $1 - \rho - 1/N$ and the error there is 1; Lemma 3.3 extends this to all larger radii. Numerically, the exact DSH quantity is $(\rho N + 1)((1-\rho)N - 1) + 1$. For $N = 2^{18}$ and the smallest prize factor $\rho(1-\rho) = 15/256$, it is already larger than $15 \cdot 2^{28}$, hence exceeds BabyBear $15 \cdot 2^{27} + 1$, KoalaBear $2^{31} - 2^{24} + 1$, and $3 \cdot 2^{30} + 1 = 3221225473$. For $N = 2^{17}$, it equals 2^{32} at $\rho = 1/2$ and $3 \cdot 2^{30} + 2^{16}$ at $\rho = 1/4$, so the sharper 2^{-17} gap holds at both rates.

(b). Take $N = 2M = 2\log_2 n$, $a = n/N$, $\ell = \rho N + 1 \in \{M + 1, M/2 + 1\}$. The quotient D^a is the unique subgroup of order N, namely $\langle 2 \rangle$. By Lemma 3.4, $|\ell \hat{} Q| = p - 1$ in the five cases it covers; apply Lemmas 3.1 and 3.3. The remaining case $(p, \rho) = (17, 1/4)$, i.e. $|3 \hat{} \langle 2 \rangle| = 16$ over $\mathbb{F}_{17}$, is the exhaustively verified item V1 of appendix A.

(c). This is Theorem 4.3.

(d). For each ℓ-subset $A \subseteq Q$ ($\ell = \rho N + 1$), Lemma 3.1's computation writes $L_A = X^{k+a} + z_A X^k + R_A$ with $z_A = -\sum_{b \in A} b$. There are $\binom{N}{\ell}$ subsets and q values of z_A; fix z achieving at least the average $\binom{N}{\ell}/q$. Each matching A gives the codeword $c_A = -R_A|_D$, agreeing with u_z on the $k + a$ points of S_A, i.e. within distance $1 - \rho - 1/N$. Distinct A give distinct monic L_A (distinct root sets), hence distinct R_A as polynomials of degree $< k < n$, hence distinct codewords on the n-point domain. The radius and size claims follow. For the final prize-rate claim, let $b_\rho \in \{2, 4, 8, 16\}$ be the denominator of ρ and put $T = (\log_2 q)^{1+\varepsilon}$. For all large q, choose the largest power of two $N \le T$; then $N > T/2$, $b_\rho \mid N$, and, since n is a power of two with $n \ge T$, also $N \mid n$. Thus $\rho N \in \mathbb{Z}$, the divisor-level bound applies, and it holds at radius $1 - \rho - 1/N \le 1 - \rho - 1/T$. By monotonicity it also holds at $1 - \rho - (\log_2 q)^{-1-\varepsilon}$, where

$$\frac{1}{q}\binom{N}{\rho N + 1} \;\ge\; 2^{\mathrm{H}(\rho)N(1-o(1)) - \log_2 q} \;\ge\; 2^{\mathrm{H}(\rho)(\log_2 q)^{1+\varepsilon}(1-o(1))/2 \;-\; \log_2 q},$$

which is $q^{\omega(1)}$. □

6 Fully explicit counterexamples

Example 6.1 (BabyBear, rate 1/2, all smooth domains of size $\ge 2^{17}$)**.** $p = 15 \cdot 2^{27} + 1 = 2013265921$. Let D be the subgroup of order $n = 2^{27}$, $k = 2^{26}$, $N = 2^{17}$, $a = 2^{10}$, and consider

$$f(x) = x^{2^{26} + 2^{10}}, \qquad g(x) = x^{2^{26}}.$$

For *every* $z \in \mathbb{F}_p$ there is a 2^{17}-element subgroup computation exhibiting badness: pick any $A \subseteq Q = D^{2^{10}}$ with $|A| = 2^{16} + 1$ and $\sum A = -z$ (which exists by Lemma 3.2), and take $S_A = \{x : x^{2^{10}} \in A\}$, $|S_A| = 2^{26} + 2^{10}$. Then $f + zg$ agrees with the explicit degree-$< 2^{26}$ polynomial $-R_A$ on S_A while g has no degree-$< 2^{26}$ explanation on S_A. Hence

$$\varepsilon_{\mathrm{mca}}\big(\mathrm{RS}[\mathbb{F}_p, D, 2^{26}],\, \delta\big) = 1 \qquad \text{for all } \delta \ge \tfrac{1}{2} - 2^{-17},$$

and the same for every smooth D with $2^{17} \mid |D|$, with $k = |D|/2$. At all four prize rates the statement holds from $\delta \ge 1 - \rho - 2^{-18}$ whenever $2^{18} \mid |D|$, and at $\rho = 1/4$ the sharper 2^{-17} gap already holds whenever $2^{17} \mid |D|$. The identical computation applies to KoalaBear and $3 \cdot 2^{30} + 1$.

Example 6.2 (Fermat instance with $q = n + 1$, fully checked)**.** $p = 257$, $n = 256$, $D = \mathbb{F}_{257}^{\times}$, $\rho = 1/2$, $k = 128$, $N = 16$, $a = 16$, $Q = \langle 2 \rangle$. The line is $f = x^{144}$, $g = x^{128}$, the bad set contains

$-9^{\wedge}Q = \mathbb{F}_{257} \setminus \{0\}$ (256 of 257 parameters; 0 is the one value the construction provably cannot produce, since $0 \notin 9^{\wedge}Q$ by Lemma 3.4), and the radius is $7/16 = \frac{1}{2} - \frac{1}{16}$, far below the capacity edge $\frac{1}{2} - \frac{1}{256}$. Every ingredient of this instance — the coverage $|9^{\wedge}Q| = 256$, the locator coefficients, and the pointwise agreement on a 144-point witness set — has been verified by exact computation (appendix A). The analogous instance over 65537 ($N = 32$, radius $\frac{1}{2} - \frac{1}{32}$, 65536 bad parameters) is likewise fully verified.

Field	mechanism	error	radius interval ($\rho = 1/2$)	status
BabyBear, KoalaBear, $3 \cdot 2^{30}+1$	DSH ladder	1	$[1/2 - 2^{-17}, 1]$	proved
same, all four rates	DSH ladder	1	$[1 - \rho - 2^{-18}, 1]$	proved
65537 ($q = n + 1$)	Fermat digits	$\geq 1 - 2^{-16}$	$[1/2 - 2^{-5}, 1]$	proved + verified
257 ($q = n + 1$)	Fermat digits	$\geq 1 - 2^{-8}$	$[1/2 - 2^{-4}, 1]$	proved + verified
sieve primes (infinitely many)	cyclotomic sieve	$\geq (\log_2 p)^{-6}$	from $1 - \rho - \Theta(1/\log p)$	proved (Theorem 4.3)
Fermat/Proth smooth towers	scalar-coset DSH	1	$1 - \rho - 1/n$	proved (Theorem 7.3)
Goldilocks towers	box-density	$\geq \theta^d$	$1 - \rho - 1/n$	proved (Example 7.6)
prize-rate smooth codes, lists	pigeonhole	$q^{\omega(1)}$ lists	from $1 - \rho - (\log_2 q)^{-1-\varepsilon}$	proved

Table 1: The counterexample inventory. "Verified" means every quantity recomputed by exhaustive dynamic programming.

7 Extension-field towers and density variants

The prime-field quotient ladder already gives the deployed-field disproof. The following scalar-coset construction gives generated extension-field examples with error one at one symbol below capacity and explains why borderline fields such as Goldilocks still have large bad-slope density even when full restricted-sum coverage fails.

Lemma 7.1 (Scalar-coset subgroup)**.** *Let p be an odd prime, let $m \mid p-1$, put $n = md$, and assume*

$$\mathrm{ord}_{md}(p) = d.$$

Then $\mathbb{F}_{p^d}^{\times}$ contains an element ζ of order n. If $H \leq \mathbb{F}_p^{\times}$ is the subgroup of order m and $D = \langle\zeta\rangle \leq \mathbb{F}_{p^d}^{\times}$, then

$$D = \bigsqcup_{i=0}^{d-1} \zeta^i H,$$

and $1, \zeta, \ldots, \zeta^{d-1}$ is an $\mathbb{F}_p$-basis of $\mathbb{F}_{p^d}$. Conversely, an element of order n and degree d over $\mathbb{F}_p$ has $\mathrm{ord}_n(p) = d$.

Proof. The equality $\mathrm{ord}_n(p) = d$ implies $n \mid p^d - 1$, so the cyclic group $\mathbb{F}_{p^d}^{\times}$ contains an element ζ of order n. The degree of an element of order n over $\mathbb{F}_p$ is the least e with $n \mid p^e - 1$, namely $\mathrm{ord}_n(p)$; hence $\mathbb{F}_p(\zeta) = \mathbb{F}_{p^d}$ and the displayed powers of ζ form a basis. Also ζ^d has order m, so $\langle\zeta^d\rangle$ is the unique subgroup of order m and equals $H \leq \mathbb{F}_p^{\times}$. Finally, for $0 \leq i, j < d$,

$$\zeta^{i-j} \in H = \langle\zeta^d\rangle \iff d \mid i - j,$$

so the d cosets $\zeta^i H$ are disjoint and account for all md elements of D. □

Lemma 7.2 (2-adic tower criterion)**.** *Let $p \equiv 1 \pmod 4$ be prime, let $\beta = \nu_2(p-1)$, and let $m \mid p-1$ satisfy $\nu_2(m) = \beta$. If d is a power of two, then*

$$\operatorname{ord}_{md}(p) = d.$$

The 2-adic hypothesis is necessary among such towers: if $\nu_2(m) < \beta$ and $d \geq 2$ is a power of two, then $\operatorname{ord}_{md}(p) < d$.

Proof. For $p \equiv 1 \pmod 4$ and every $e \geq 1$, the standard lifting-the-exponent computation gives

$$\nu_2(p^e - 1) = \beta + \nu_2(e).$$

Indeed this is immediate for $e = 2^a$ by factoring $p^{2^{a+1}} - 1 = (p^{2^a} - 1)(p^{2^a} + 1)$ and using $p^{2^a} + 1 \equiv 2 \pmod 4$, and the odd part of e contributes no additional factor of 2.

Write $m = 2^\beta t$ with t odd and $t \mid p-1$, and write $d = 2^a$. By the Chinese remainder theorem,

$$\operatorname{ord}_{md}(p) = \operatorname{lcm}\big(\operatorname{ord}_t(p), \operatorname{ord}_{2^{\beta+a}}(p)\big).$$

Here $\operatorname{ord}_t(p) = 1$, while the displayed valuation formula shows $\operatorname{ord}_{2^{\beta+a}}(p) = 2^a = d$. This proves the criterion. If $\nu_2(m) = c < \beta$, then the same computation gives $\operatorname{ord}_{2^{c+a}}(p) = 2^{\max(0,c+a-\beta)} < 2^a$, proving the final claim. □

Theorem 7.3 (Smooth extension towers: full density)**.** *Let $p \equiv 1 \pmod 4$ be prime, let $m = 2^{\nu_2(p-1)}$, let d be a power of two, and let $D \leq \mathbb{F}_{p^d}^\times$ be the subgroup of order $n = md$ supplied by Lemmas 7.1 and 7.2. Fix $0 < \rho \leq 1/2$ with $r := \rho m \in \mathbb{Z}$, and assume*

$$\rho(1-\rho)m^2 \geq p.$$

Then, for $k = \rho n$,

$$\varepsilon_{\mathrm{mca}}\left(\mathrm{RS}[\mathbb{F}_{p^d}, D, k],\ 1 - \rho - \frac{1}{n}\right) = 1.$$

In particular, if $m^2 \geq 18p$, this holds simultaneously for all four prize rates.

Proof. Let $H \leq \mathbb{F}_p^\times$ be the subgroup of order m and write $D = \bigsqcup_{i=0}^{d-1} \zeta^i H$ with $1, \zeta, \ldots, \zeta^{d-1}$ an $\mathbb{F}_p$-basis. We prove $(k+1)^\wedge D = \mathbb{F}_{p^d}$. Take any

$$y = c_0 + c_1\zeta + \cdots + c_{d-1}\zeta^{d-1}, \qquad c_i \in \mathbb{F}_p.$$

By Lemma 3.2, $r^\wedge H = \mathbb{F}_p$ because $r(m-r) + 1 \geq p + 1$, and $(r+1)^\wedge H = \mathbb{F}_p$ because

$$(r+1)(m-r-1) + 1 = r(m-r) + (m-2r) \geq p.$$

Thus choose $T_0 \subseteq H$ with $|T_0| = r+1$ and $\sum_{t \in T_0} t = c_0$, and for $i \geq 1$ choose $T_i \subseteq H$ with $|T_i| = r$ and $\sum_{t \in T_i} t = c_i$. Then

$$A = T_0 \sqcup \zeta T_1 \sqcup \cdots \sqcup \zeta^{d-1} T_{d-1} \subseteq D$$

has size $(r+1) + (d-1)r = rd + 1 = k + 1$ and sum y. Hence $(k+1)^\wedge D = \mathbb{F}_{p^d}$. Applying Lemma 3.1 with $N = n$ and $a = 1$ gives every slope $z \in \mathbb{F}_{p^d}$ bad for $x^{k+1} + zx^k$ at radius $1 - \rho - 1/n$.

For the final sentence, the smallest value of $\rho(1-\rho)$ among the four prize rates is $15/256$, so $m^2 \geq 18p$ implies $\rho(1-\rho)m^2 > p$ for all four rates; it also forces $m > 18$, hence $16 \mid m$ in the smooth case, so $\rho m \in \mathbb{Z}$. □

Proposition 7.4 (Box-density extension bound)**.** *With p, m, d, D, n as in Theorem 7.3 but without the coverage inequality, let $0 < \rho \le 1/2$, $r = \rho m \in \mathbb{Z}$, $1 \le r \le m/2$, $m \ge 4$, and $k = \rho n$. Put*

$$\theta = \min\left\{1, \frac{\rho(1-\rho)m^2}{p}\right\}.$$

Then

$$\varepsilon_{\mathrm{mca}}\left(\mathrm{RS}[\mathbb{F}_{p^d}, D, k],\ 1-\rho-\frac{1}{n}\right) \ge \theta^d.$$

Proof. Use the same scalar-coset decomposition. Let

$$B = \left\{s_0 + \zeta s_1 + \cdots + \zeta^{d-1} s_{d-1} : s_0 \in (r+1)^{\wedge}H, s_i \in r^{\wedge}H \ (i \ge 1)\right\}.$$

Every element of B is a sum of $(r+1)+(d-1)r = k+1$ distinct elements of D, so $B \subseteq (k+1)^{\wedge}D$. The basis property makes the coordinate map injective, hence

$$|B| = |(r+1)^{\wedge}H|\,|r^{\wedge}H|^{d-1}.$$

By Lemma 3.2, the first factor and each remaining factor are at least θp: for r this is immediate, and for $r+1$ the identity

$$(r+1)(m-r-1)+1 = r(m-r)+(m-2r)$$

is no smaller when $r \le m/2$. Thus $|(k+1)^{\wedge}D| \ge |B| \ge (\theta p)^d = \theta^d q$. The locator obstruction Lemma 3.1 with $N = n$ gives the displayed MCA lower bound. □

Corollary 7.5 (Fermat and Proth-type towers)**.** *Let p be a Fermat prime at least 257, or more generally let $p \equiv 1 \pmod 4$ with $m = 2^{\nu_2(p-1)}$ and $m^2 \ge 18p$. For every power of two d, the smooth subgroup $D \le \mathbb{F}_{p^d}^{\times}$ of order $n = md$ satisfies, for every prize rate ρ and $k = \rho n$,*

$$\varepsilon_{\mathrm{mca}}\left(\mathrm{RS}[\mathbb{F}_{p^d}, D, k],\ 1-\rho-\frac{1}{n}\right) = 1.$$

This includes the Fermat bases $p = 257$ and $p = 65537$, and the Proth/deployed bases whose 2-part is large enough.

Proof. For Fermat primes $p \ge 257$, $m = p-1$ and $(p-1)^2 \ge 18p$. The general case is exactly Theorem 7.3. □

Example 7.6 (Goldilocks density)**.** Let

$$p = 2^{64} - 2^{32} + 1, \qquad m = 2^{32}.$$

Then $p \equiv 1 \pmod 4$, $m = 2^{\nu_2(p-1)}$, and Lemma 7.2 gives smooth towers of order $n = 2^{32}d$ in $\mathbb{F}_{p^d}$ for every power of two d. Full coverage fails at the prize rates, but Proposition 7.4 gives large density. At rate $\rho = 1/2$,

$$\theta = \frac{2^{62}}{2^{64} - 2^{32} + 1} > \frac{1}{4},$$

so

$$\varepsilon_{\mathrm{mca}}\left(\mathrm{RS}[\mathbb{F}_{p^d}, D, n/2],\ \frac{1}{2}-\frac{1}{n}\right) \ge \theta^d > 4^{-d}.$$

In particular the height-one Goldilocks field has MCA error greater than $1/4$ one symbol below capacity, and the lower bound $\theta^d > 4^{-d} = 2^{-2d}$ remains above 2^{-128} for every $d \le 64$. At rate $1/16$, $\theta > 15/256$ and $31\log_2(256/15) < 127$, so the same bound remains above 2^{-128} for $d \le 31$.

8 Scope: what is refuted, what survives

Refuted. Conjecture 1.1 in its stated form, at every prize rate, for every target $\varepsilon^* < 1$, on the deployed FFT fields (error one, on an interval), on linear-size Fermat fields (error $1 - 1/p$, verified), on generated extension-field smooth towers (error one at one symbol below capacity when the scalar-coset coverage condition holds), and even on borderline Goldilocks-type towers at non-negligible density. In the negligibility sense, with non-negligible meaning inverse-polynomial in $\lambda = \log_2 q$, the conjecture also fails on infinitely many smooth prime fields at radius $1 - \rho - O(1/\log p)$. The polynomial-list analogue fails unconditionally at the prize rates on every power-of-two subgroup domain with $n \geq (\log_2 q)^{1+\varepsilon}$ for any fixed $\varepsilon > 0$; the divisor-level version of Theorem 2.1(d) is valid for arbitrary rates whenever the chosen divisor N satisfies $\rho N \in \mathbb{Z}$.

Not refuted, and turned into floors. Any formulation with explicit slack τ: our results show such a formulation *must* take $\tau > 1/\hat{N} \asymp \sqrt{\rho(1-\rho)/p}$ on fields where the 2-part of $p - 1$ reaches $\hat{N}$ (including BabyBear, KoalaBear, and $3 \cdot 2^{30} + 1$), $\tau > c_\rho / \log p$ on the sieve fields, and $\tau > (\log_2 q)^{-1-\varepsilon}$ for the prize-rate list version whenever the domain has the corresponding dyadic divisors; above these floors the present no-slack arguments make no negative claim. The restricted-sum mechanism itself cannot certify arbitrary depths: certifying error η at $1 - \rho - 1/N$ through a quotient Q needs $\binom{N}{\rho N+1} \geq \eta q$ (the construction's bad set has size at most $|(\rho N+1)^{\wedge} Q| \leq \binom{N}{\rho N+1} \leq 2^{\mathrm{H}(\rho) N (1+o(1))}$), i.e. $N \geq \log_2(\eta q)/\mathrm{H}(\rho)\,(1 - o(1))$ — a radius gap $O(\mathrm{H}(\rho)/\log_2(\eta q))$ at best. Curve-MCA and exact slacked threshold formulations require additional constraints and analysis beyond the no-slack model studied here; protocol-level soundness of FRI/WHIR-type systems is untouched, because deployed analyses operate in the Johnson regime with margins and include protocol-specific constraints absent from this minimal no-slack definition.

Companion manuscripts. The corrected slack/entropy theory and failure-ladder calculus built on these floors are developed in [14]. The divisor-level list bound of Theorem 2.1(d), sharpened to slack two and pigeonholed over the field of definition, composes with the Crites–Stewart list-to-agreement conversion [4] into a field-size-universal challenge cap in [15], which also places the list mass directly against the survey's $\varepsilon^* |\mathbb{F}|$ budget.

Relation to prior negative results. Counterexamples to the up-to-capacity proximity-gaps conjectures of [2] were given by Diamond–Gruen and Crites–Stewart [3, 4]; near-capacity failures over prime-field multiplicative subgroups were recently established by Krachun–Kazanin–Haböck and Kambiré [12, 13]; on the list side, superpolynomial lists beyond Johnson for full-field RS go back to Ben-Sasson–Kopparty–Radhakrishnan via subspace polynomials [10] (see also [11]). The contribution here is the smooth-multiplicative mechanism — subgroup quotients of smooth domains — which yields *error-one* MCA failure on radius intervals for the actual deployed fields, exact $q = n + 1$ instances, an unconditional inverse-polylogarithmic-density theorem for the governing small-subgroup density question (Theorem 4.3; its fixed-constant-density form over arbitrary primes remains open), and the unconditional prize-rate smooth-domain list bound — together, the no-slack disproof in the setting the prize names.

A Verification record

All computations are exact (dynamic programming over residues with cardinality tracking; no sampling).

V1. *Fermat coverage.* $|(M{+}1)^{\wedge}\langle 2\rangle| = p-1$ for $p = 17, 257, 65537$, and $|(M/2{+}1)^{\wedge}\langle 2\rangle| = p-1$ for $p = 17$ ($|3^{\wedge}\langle 2\rangle| = 16$, the case of Theorem 2.1(b) not covered by Lemma 3.4), 257, and 65537; the unique missing element is 0 in every case, exactly as Lemma 3.4 predicts.

V2. *Locator end-to-end.* For $p = 257$, $A \subseteq Q$ with $|A| = 9$, $z = -\sum A$: the expanded $\prod_{b\in A}(X^{16} - b)$ has top coefficients $X^{144} + zX^{128} + (\deg < 128)$ and $x^{144} + zx^{128} = -R_A(x)$ at all 144 points of S_A.

V3. *Pigeonhole list sizes.* $p = 17$, $n = 16$, $k = 8$: the number of 9-subsets of $\mathbb{F}_{17}^{\times}$ with each prescribed sum is 672 or 673 (mean $\binom{16}{9}/17 = 672.9$), so every word $x^9 + zx^8$ has ≥ 672 codewords at distance $\leq 1 - 9/16$; the pigeonhole bound of Theorem 2.1(d) is essentially exact here.

V4. *Ladder rung.* $p = 12289$, $\rho = 1/2$: $\hat{N} = 256$ and $|129^{\wedge}Q_{256}| = 12289$ (full coverage, error 1 at $\frac{1}{2} - \frac{1}{256}$); even the unproven rung $N = 128$ covers fully, so the proved ladder is conservative.

V5. *Sieve mechanism.* $N = 16$, $r = 9$: the global cyclotomic family has exactly 3280 values (formula and enumeration agree); over primes $p \equiv 1$ (16) the sumset $|9^{\wedge}Q_{16}|$ equals $1712, 2336, 2672, 3280, 3280, 3280$ at $p = 1889, 3137, 7681, 12289, 40961, 65537$ — collision-free reduction for $p \gg 3280$, the regime driving Theorem 2.1(c).

References

[1] Ethereum Foundation, *The Proximity Prize: $1M Reed–Solomon Challenge*, 2025. https://proximityprize.org/.

[2] E. Ben-Sasson, D. Carmon, Y. Ishai, S. Kopparty, and S. Saraf, *Proximity gaps for Reed–Solomon codes*, J. ACM 70 (2023), no. 5. Preliminary version in FOCS 2020.

[3] B. E. Diamond and A. Gruen, *On the Distribution of the Distances of Random Words*, Cryptology ePrint Archive, Report 2025/2010, 2025.

[4] E. Crites and A. Stewart, *On Reed–Solomon Proximity Gaps Conjectures*, Cryptology ePrint Archive, Report 2025/2046, 2025.

[5] G. Arnon, D. Boneh, and G. Fenzi, *Open Problems in List Decoding and Correlated Agreement*, Cryptology ePrint Archive, Report 2026/680, 2026.

[6] D. Boneh, *The Proximity Prize: What It Is and What We Currently Know*, ZKProof 8 keynote transcript, 2026.

[7] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, *Fast Reed–Solomon Interactive Oracle Proofs of Proximity*, ICALP 2018.

[8] G. Arnon, A. Chiesa, G. Fenzi, and E. Yogev, *WHIR: Reed–Solomon Proximity Testing with Super-Fast Verification*, ePrint 2024/1586.

[9] J. A. Dias da Silva and Y. O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory*, Bull. London Math. Soc. 26 (1994), 140–146.

[10] E. Ben-Sasson, S. Kopparty, and J. Radhakrishnan, *Subspace polynomials and limits to list decoding of Reed–Solomon codes*, IEEE Trans. Inform. Theory 56 (2010), 113–120.

[11] V. Guruswami and A. Rudra, *Limits to list decoding Reed–Solomon codes*, IEEE Trans. Inform. Theory 52 (2006), 3642–3649.

[12] D. Krachun, S. Kazanin, and U. Haböck, *Failure of proximity gaps close to capacity*, ePrint 2026/782.

[13] A. Kambiré, *Proximity Gaps Conjecture Fails Near Capacity over Prime Fields*, arXiv:2604.09724, 2026.

[14] P. Chojecki, *Slack, Quotient Cores, and the Entropy Gap for Smooth-Domain Reed–Solomon Codes*, companion manuscript, merged corrected edition, 2026.

[15] P. Chojecki, *A Universal Field-Size Cap for Mutual Correlated Agreement on Smooth Reed–Solomon Domains*, companion manuscript, June 2026.

[16] H. Davenport, *Multiplicative Number Theory*, 3rd ed., Graduate Texts in Mathematics 74, Springer, 2000. (Siegel–Walfisz theorem, §22.)