The Chen–Zhang list-recovery conjecture for folded Reed–Solomon codes: a proof at output cap seven and counterexamples beyond

Scott Schubr
Luminary Oddities

November 20, 2026

Abstract

Chen and Zhang conjectured that folded Reed–Solomon codes of rate R with appropriate evaluation points, input lists of size ℓ and output cap $\ell^a - 1$ are list recoverable at every radius below $\Phi_{\ell,a}(R) = (1 - \ell^{1-a})(1 - aR/(a-1))$, the radius at which their hypercube construction stops list recovery, once the folding is large. We prove the conjecture for input-list size two and output cap seven, in the stronger average-radius form and for every choice of appropriate evaluation points: folding $s \geq 7 + \lceil 4/\eta \rceil$ suffices at all rates $R \leq 2/3 - 8\rho/9 - \eta$, and by the Chen–Zhang upper bound this radius is exact. For input-list size two with $a \geq 4$, and for every $\ell \geq 3$ with $a \geq 3$, we construct ℓ^a codewords that each have error strictly below $\Phi_{\ell,a}(R)$, at every rate in an explicit interval $(0, R_0^*(\ell, a))$, in every such code of large folding and length, and with high probability in random linear codes over every field with at least ℓ elements. Together with the case $(\ell, a) = (2, 2)$ proved by Chen and Zhang, this decides the conjecture for input-list size two and for every exponent $a \geq 3$: it holds at $(\ell, a) = (2, 2)$ and $(2, 3)$ at every rate, and every other case fails, with explicit failing rates filling $(0, R_0^*(\ell, a))$. Both directions are governed by one linear program. A configuration of messages has a certificate cost: the least total dimension of nonnegative subspace weights that bound the ℓ largest fibers of every linear quotient at once. Dual kernel patterns bound it from below, and the hypercube pattern has value exactly the conjectured slope $a(\ell^a - \ell)/(a-1)$. Every eight-point configuration over every field has cost at most nine, the slope for $(\ell, a) = (2, 3)$, and folded-Wronskian rank bounds turn this into the coding theorem. Independent coordinate squares sharing one origin carry kernel patterns of value $(\ell - 1)(2\ell t + c)$, which exceeds the slope exactly in the refuted range; injective padding blocks and a degree schedule convert this excess into equal individual errors. For $\ell = 2$ the squares have exact cost $4t + c$, and for $a \geq 4$ every linear code of rate below $2/B(2, a)$ admits the corresponding average-radius obstruction.

Contents

1 Introduction **2**
1.1 Folded Reed–Solomon codes and the conjecture 2
1.2 Results 3
1.3 One linear program for both directions 5
1.4 Prior work and credits 6

2 Fiber certificates and kernel patterns **7**

3 The eight-point theorem **9**
3.1 Affine tools . . . 9
3.2 Affine dimensions at most four . . . 10
3.3 Dependency supports in affine dimensions five to seven . . . 12
3.4 Proof of Theorem 1.8 and the attained costs . . . 13

4 Coding consequences **14**
4.1 The folded-Wronskian budget for every set of appropriate points . . . 14
4.2 Sharpness . . . 15
4.3 Finite-folding profiles . . . 15
4.4 Multiplicity codes . . . 17

5 Independent squares and average-radius obstructions **17**
5.1 The exact cost . . . 18
5.2 A finite converse for every linear code . . . 18
5.3 Exact realization in full-length folded Reed–Solomon codes . . . 20

6 Ordinary counterexamples **21**
6.1 Padding and degree scheduling . . . 21
6.2 Block surjectivity . . . 23
6.3 Random linear codes . . . 25
6.4 An explicit cap-fifteen instance . . . 26

7 Scope **26**

1 Introduction

1.1 Folded Reed–Solomon codes and the conjecture

Let q be a prime power and let γ generate $\mathbb{F}_q^\times$. For positive integers s, n, k and points $\alpha_0, \dots, \alpha_{n-1} \in \mathbb{F}_q$, the s-folded Reed–Solomon code [10] encodes a polynomial $f \in \mathbb{F}_q[X]$ of degree less than k by the blocks

$$E_j(f) = \big(f(\alpha_j), f(\gamma\alpha_j), \dots, f(\gamma^{s-1}\alpha_j)\big) \in \mathbb{F}_q^s, \qquad 0 \le j < n. \tag{1}$$

Following [5, Definition 1.2], the points are *appropriate* if the sn elements $\gamma^i\alpha_j$ $(0 \le i < s, 0 \le j < n)$ are distinct. For $s \ge 2$ this forces every $\alpha_j \ne 0$, so $sn \le q-1$. When $k \le sn$ the encoding is injective, since a nonzero polynomial of degree less than k has fewer than sn roots. The rate is $R = k/(sn)$. The *consecutive model* takes $\alpha_j = \gamma^{js}$ with $sn \le q-1$; it is *full length* when $sn = q-1$. We write $\mathcal{P}_k = \{f \in \mathbb{F}_q[X] : \deg f < k\}$ for the message space.

An input table is a sequence $\mathcal{T} = (\mathcal{T}_j)_{j<n}$ with $\mathcal{T}_j \subseteq \mathbb{F}_q^s$ and $|\mathcal{T}_j| \le \ell$. The relative error of a message is $\mathrm{err}_{\mathcal{T}}(f) = |\{j : E_j(f) \notin \mathcal{T}_j\}|/n$. The code is (ρ, ℓ, L) *list recoverable* if for every table at most L messages have error at most ρ. It is *average-radius* (ρ, ℓ, L) list recoverable if every $L+1$ distinct messages have mean error strictly greater than ρ against every table. The average-radius property implies the ordinary one.

Fix integers $\ell, a \ge 2$, put $M = \ell^a$ and $L = M - 1$, and define

$$\Phi_{\ell,a}(R) = \frac{M-\ell}{M}\Big(1 - \frac{aR}{a-1}\Big), \qquad B = B(\ell, a) = \frac{a(M-\ell)}{a-1}. \tag{2}$$

The identity

$$M(1-\Phi_{\ell,a}(R)) = \ell + BR \tag{3}$$

says that at radius $\Phi_{\ell,a}(R)$ the M messages may together agree with the table at $\ell n + BRn$ coordinates, and we call B the *conjectured slope*.

Conjecture 1.1 (Chen–Zhang [5, Conjecture 3.6]). *Let $\ell \geq 2$ and $a \geq 2$ be integers, put $L+1 = \ell^a$, and fix $\varepsilon > 0$, a rate $R \leq (a-1)/a$ and a generator γ. There is a constant C_0 such that, if $s \geq C_0$, $(k-1)/s \geq a$ and n is sufficiently large, then every rate-R folded Reed–Solomon code with appropriate evaluation points is $(\Phi_{\ell,a}(R) - \varepsilon, \ell, L)$ list recoverable.*

Brakensiek, Chen, Dhar and Zhang [1, Conjecture 1.3] restate the conjecture with the slack in the rate: for $\rho \leq 1 - \ell/(L+1)$, rates $R \leq R^* - \varepsilon$ with $R^* = \frac{a-1}{a}(1 - \frac{\rho(L+1)}{L+1-\ell})$ should suffice. Since $\Phi_{\ell,a}$ is linear and strictly decreasing, a radius slack ε equals the rate slack $(a-1)M\varepsilon/(a(M-\ell))$, so both forms carry the same content. The radius $\Phi_{\ell,a}$ comes from the following upper bound, which we use as stated.

Theorem 1.2 (Chen–Zhang [5, Theorem 3.1]). *Let $s \geq 1$, $2 \leq \ell \leq L$, $q \geq \ell$, $m = \lceil \log_\ell(L+1) \rceil > 1$, and suppose $(k-1)/(sn) \leq (m-1)/m$ and $(k-1)/((m-1)s) \geq 1$. If an s-folded Reed–Solomon code with appropriate evaluation points is (ρ, ℓ, L) list recoverable, then*

$$\rho \leq \frac{L+1-\ell}{L+1}\left(1 - \left\lfloor \frac{m}{m-1}\left\lfloor \frac{k-1}{s} \right\rfloor \right\rfloor \frac{1}{n}\right).$$

Pairs (ℓ, a) index the table and exponents; pairs (ℓ, L) are always written with L explicit.

1.2 Results

Table 1 summarizes the status of Conjecture 1.1 established here and in the cited works.

Theorem 1.3 (Output cap seven). *Let q be a prime power, γ a generator of $\mathbb{F}_q^\times$, and $n \geq 1$, $s \geq 7$ and $1 \leq k \leq sn$ integers. Let $\alpha_0, \ldots, \alpha_{n-1}$ be appropriate evaluation points. If $0 \leq \rho < 3/4$ and*

$$\frac{k-1}{n(s-6)} < \frac{2}{3} - \frac{8\rho}{9}, \tag{4}$$

then the s-folded Reed–Solomon code with these points is average-radius $(\rho, 2, 7)$ list recoverable, and hence $(\rho, 2, 7)$ list recoverable.

By (2), $\rho < \Phi_{2,3}(R) = \frac{3}{4} - \frac{9R}{8}$ is equivalent to $R < \frac{2}{3} - \frac{8\rho}{9}$, so (4) is the conjectured rate condition up to the factor $s/(s-6)$.

Corollary 1.4 (Conjecture 1.1 at $(\ell, L) = (2, 7)$). *Conjecture 1.1 holds for $(\ell, L) = (2, 7)$, in the average-radius form, for every generator and every choice of appropriate evaluation points, and without conditions on $(k-1)/s$ or on n. Precisely, let $\varepsilon > 0$ and put*

$$C(\varepsilon) = 7 + \lceil 9/(2\varepsilon) \rceil.$$

For every rate $R \leq 2/3$ and every $s \geq C(\varepsilon)$, every rate-R s-folded Reed–Solomon code with appropriate evaluation points is average-radius $(\Phi_{2,3}(R) - \varepsilon, 2, 7)$ list recoverable. Equivalently, in the rate-slack form [1, Conjecture 1.3]: for $0 \leq \rho < 3/4$ and every $\eta > 0$, folding $s \geq 7 + \lceil 4/\eta \rceil$ suffices at every rate $R \leq 2/3 - 8\rho/9 - \eta$.

(ℓ, a), cap L	Status	Source
$(2,2)$, $L=3$	holds, at radius $\frac{1}{2} - \frac{sR}{s-2}$	Chen–Zhang [5, Thm. 1.8]; average-radius form in Corollary 4.3
$(2,3)$, $L=7$	holds, average-radius form, every set of appropriate points; the radius $\Phi_{2,3}$ is exact	Theorem 1.3, Corollary 1.4, Proposition 4.4, via [5, Thm. 3.1]
$(2,a)$, $a \geq 4$	fails at every rate in $(0, R_0^*)$, in ordinary and average-radius form, for every code with appropriate points and for random linear codes; the average-radius form fails in every linear code at every rate in $(0, 2/B)$	Theorems 1.5, 1.6, 1.7
(ℓ, a), $\ell \geq 3$, $a \geq 3$	fails at every rate in $(0, R_0^*)$, in ordinary and average-radius form, for every code with appropriate points and for random linear codes	Theorems 1.5, 1.6
$(\ell, 2)$, $\ell \geq 3$	the squares patterns meet the slope exactly, $C = B$	Lemma 2.9
all, $\rho = 0$	holds	Brakensiek–Chen–Dhar–Zhang [1, Thm. 1.6]; for $\ell = 2$ Chen–Cheraghchi–Si–Zhang [4]

Table 1: The Chen–Zhang conjecture at $L+1 = \ell^a$. Here $R_0^* = R_0^*(\ell, a)$ is the explicit threshold of Theorem 1.5, for example $R_0^*(2,4) = 3/196$ and $R_0^*(3,3) = 19/906$.

Theorem 1.2 shows that the radius in Corollary 1.4 cannot be increased (Proposition 4.4), so $\Phi_{2,3}$ is the exact list-recovery radius at $(\ell, L) = (2,7)$ of folded Reed–Solomon codes of large folding and length.

For the counterexamples, fix integers ℓ, a in the region

$$(\ell \geq 3 \text{ and } a \geq 3) \quad \text{or} \quad (\ell = 2 \text{ and } a \geq 4), \tag{5}$$

and put

$$M = \ell^a, \quad N = \frac{M-1}{\ell - 1}, \quad c = \begin{cases} 0, & a \text{ even}, \\ 1, & a \text{ odd}, \end{cases} \quad t = \frac{N-c}{\ell+1}, \quad d = 2t + c, \quad C = (\ell-1)(2\ell t + c). \tag{6}$$

Lemma 2.9 shows that t is a positive integer and that $C > B$ exactly on the region (5).

Theorem 1.5 (Counterexamples in folded Reed–Solomon codes)**.** *Fix (ℓ, a) in (5) and put*

$$R_0^* = R_0^*(\ell, a) = \frac{\ell C}{B(Md - C)}.$$

For every rational rate $R \in (0, R_0^*)$ there are a rational $\varepsilon = \varepsilon(\ell, a, R) > 0$ and an integer $n_0 = n_0(\ell, a, R)$ such that the following holds with $s_0 = d + 1$. For every integer $s \geq s_0$, every s-folded Reed–Solomon code of rate exactly R and length $n \geq n_0$ with appropriate evaluation points, over any field $\mathbb{F}_q$ and for any generator γ, admits a table of exactly ℓ symbols per block and M distinct messages, each satisfying

$$\mathrm{err}_{\mathcal{T}}(f) < \Phi_{\ell,a}(R) - \varepsilon.$$

These codes satisfy $(k-1)/s \geq a$, and they exist for every s and every n with $Rsn \in \mathbb{Z}$: for every prime power $q > sn$ the consecutive points are appropriate. For example $R_0^*(2,4) = 3/196$ and $R_0^*(3,3) = 19/906$.

Every indicated instance of Conjecture 1.1 therefore fails at every sufficiently small fixed rate, with its own fixed positive slack, in every code over which the conjecture quantifies once $s \geq d+1$ and $n \geq n_0$. The mean error of the M messages is then also below $\Phi_{\ell,a}(R)-\varepsilon$, so the average-radius form fails as well.

Theorem 1.6 (Random linear codes)**.** *Let (ℓ, a) lie in (5), let $q \geq \ell$ be a prime power and let $R \in (0, R_0^*)$ be rational. There are $\varepsilon > 0$ and s_0, depending only on ℓ, a, q, R, such that for every $s \geq s_0$ a uniformly random $\mathbb{F}_q$-linear code of rate R over the alphabet $\mathbb{F}_q^s$ is, with probability $1-o(1)$ as $n \to \infty$, not $(\Phi_{\ell,a}(R) - \varepsilon, \ell, \ell^a - 1)$ list recoverable.*

Theorem 1.7 (Average-radius obstruction in every linear code)**.** *Let $a \geq 4$, $M = 2^a$, and let t, c, d, C be as in (6) with $\ell = 2$. For every rational R with $0 < R < 2/B(2,a)$ there are $\varepsilon > 0$ and n_0, depending only on a and R, such that every $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq (\mathbb{F}_q^s)^n$ of rate exactly R and length $n \geq n_0$, over every finite field and with every folding $s \geq 1$, contains M distinct codewords and a table of exactly two symbols per coordinate against which their mean error is at most $\Phi_{2,a}(R) - \varepsilon$. In particular such codes are not average-radius $(\Phi_{2,a}(R) - \varepsilon, 2, 2^a - 1)$ list recoverable. For $a = 4$ the interval is $0 < R < 3/28$.*

1.3 One linear program for both directions

Let S be a set of M distinct messages, viewed as points of the message space. At a block with kernel K, the fibers of the evaluation map on S are the affine K-cosets meeting S, and a table of ℓ symbols captures at most the ℓ largest of them. A *certificate* (Definition 2.1) is a family of nonnegative subspace weights y_W, chosen once for S, that bounds these captures for every kernel simultaneously:

$$b_\ell(S/K) \leq \ell + \sum_W y_W \dim(K \cap W) \qquad (K \leq \operatorname{dir} S).$$

Its cost is $\sum_W y_W \dim W$, and $\kappa_\ell(S)$ denotes the least cost. Folded-Wronskian rank bounds [9] show that the block kernels of a folded Reed–Solomon code meet every fixed u-dimensional subspace in total dimension at most about Rnu. Summing a certificate over the blocks bounds the total capture by $\ell n + Rn\kappa_\ell(S)$. By (3), the inequality $\kappa_\ell(S) \leq B$ for all M-point configurations therefore proves the conjecture at (ℓ, a) in average-radius form (Corollary 4.3).

The dual objects are *kernel patterns* (Definition 2.2): nonnegative weights x_K on subspaces with $\sum_K x_K \dim(K \cap W) \leq \dim W$ for every W, of value $\sum_K x_K(b_\ell(S/K) - \ell)$. Weak duality bounds $\kappa_\ell(S)$ below by every such value. Two observations connect them with codes:

- The hypercube A^a with its a coordinate hyperplanes carries a kernel pattern of value exactly B (Example 2.5). This is the dual form of the Chen–Zhang construction, so $\kappa_\ell(S) \leq B$ is the strongest inequality the method can use.
- The block kernels of an actual code, normalized by its rank budget, form a kernel pattern, and the best table captures exactly its value (Lemma 2.6).

For $(\ell, a) = (2, 3)$ we prove $\kappa_2(S) \leq 9 = B$ for every eight-point configuration over every field (Theorem 1.8), which yields Theorem 1.3. For (5), independent coordinate squares sharing one origin carry kernel patterns supported on their coordinate axes of value $C > B$ (Proposition 2.8).

Sections 5 and 6 realize these axis kernels as block kernels of actual codes, in the proportion allowed by the rank budget, and pad the remaining blocks so that every message has the same error. At $a = 2$ and at $(\ell, a) = (2, 3)$ the squares value equals B, in agreement with the positive results there.

Theorem 1.8 (Eight-point certificate)**.** *Every set S of eight distinct points over any field satisfies $\kappa_2(S) \le 9$. For affine dimensions $1, \dots, 7$, respectively,*

$$\kappa_2(S) \le 6, \quad 8, \quad 9, \quad 9, \quad 9, \quad 8, \quad 7,$$

and each of these values is attained: in dimensions 1, 2 and 4 over every field with at least 8, 3 and 3 elements, respectively, and in dimensions 3, 5, 6 and 7 over every field. The Boolean three-cube has $\kappa_2(S) = 9$. Hence $\sup_S \kappa_2(S) = 9 = B(2, 3)$.

Theorem 1.9 (Independent squares)**.** *Let $\ell \ge 2$, $t \ge 1$ and $c \ge 0$ be integers, let F be a field with at least ℓ elements and let $A \subseteq F$ have ℓ elements, including 0. For independent vectors $p_0, \dots, p_{2t+c-1}$, the configuration of t squares $A \times A$ in the coordinate planes $\operatorname{span}(p_{2h}, p_{2h+1})$ and c lines Ap_i $(i \ge 2t)$, all sharing the origin, has $M = 1 + t(\ell^2 - 1) + c(\ell - 1)$ points and*

$$\kappa_\ell(S) \ge (\ell - 1)(2\ell t + c).$$

For $\ell = 2$, over every field, equality holds: $\kappa_2(S) = 4t + c$.

1.4 Prior work and credits

Folded Reed–Solomon codes were introduced by Guruswami and Rudra [10]. Chen and Zhang [5] proved that every folded Reed–Solomon code with appropriate evaluation points attains a relaxed generalized Singleton bound, established the hypercube upper bound (Theorem 1.2), stated Conjecture 1.1, and proved its case $(\ell, L) = (2, 3)$ [5, Theorems 1.8 and 3.7]. Their method and ours rest on the subspace-design property of folded Reed–Solomon codes and on the folded Wronskian determinant of Guruswami and Kopparty [9]. Brakensiek, Chen, Dhar and Zhang [1] proved the zero-error case $\rho = 0$ for all parameters [1, Theorem 1.6] by discrete Brascamp–Lieb inequalities and reformulated the conjecture as [1, Conjecture 1.3]; they attribute the zero-error case with $\ell = 2$ to Chen, Cheraghchi, Si and Zhang [4], and in the October 2026 version [1, Remark 1.7] identify $(\ell, L) = (2, 3)$, that is $(\ell, a) = (2, 2)$, as the only case with positive error proved beyond their zero-error theorem. The cap-seven theorem is the first positive-error case of the conjecture beyond $(\ell, L) = (2, 3)$, and the counterexamples of this paper are new.

The black-box route from explicit codes to random linear codes uses the subspace-design transfer of Brakensiek, Chen, Dhar and Zhang [2] and the local-equivalence and sharp-threshold theorems of Levi, Mosheiff and Shagrithaya [11] (Remark 6.11); our random-code theorem has a direct proof. The universal shortening converse of Section 5 follows the grid and support constructions of Chen and Zhang [5, Section 3.1] and of Li and Shagrithaya [12], with a sparser message set. Average-radius recovery is the average-weight notion of [11, Definition 2.1]; Goyal and Guruswami analyse list decoding and list recovery of random linear codes by counting partition-induced local profiles [7]. Complementary directions include the structure theorems and fast algorithms of Goyal and Guruswami [6], the threshold equivalences of Goyal, Guruswami, Sun and Wootters [8], and the tight generalized Singleton bound and capacity limitations of Brakensiek, Chen, Putterman and Zhang [3], whose optimal radius we compare with in Proposition 6.4.

Organization. Section 2 sets up certificates and kernel patterns. Section 3 proves Theorem 1.8. Section 4 proves Theorem 1.3 and Corollary 1.4, sharpness, and finite-folding and multiplicity-code versions. Section 5 proves Theorem 1.9 and Theorem 1.7 and realizes the squares exactly in full-length codes. Section 6 proves Theorems 1.5 and 1.6. Section 7 summarizes the scope.

2 Fiber certificates and kernel patterns

Let F be a field and S a finite set of $M \geq 2$ distinct points of an F-vector space. Its direction space $V = \mathrm{dir}(S)$ is the span of the differences of its points. Translating one point to the origin, we view $S \subseteq V$. For $K \leq V$, the *K-fibers* of S are the nonempty sets $S \cap (v + K)$. For $\ell \geq 1$, let $b_\ell(S/K)$ be the sum of the ℓ largest fiber sizes, where absent fibers count zero. Thus $b_\ell(S/0) = \min(\ell, M)$ and $b_\ell(S/V) = M$.

Definition 2.1 (Certificate)**.** A *certificate* for (S, ℓ) is a finitely supported family of real weights $y_W \geq 0$ on subspaces $W \leq V$ such that

$$b_\ell(S/K) \leq \ell + \sum_W y_W \dim(K \cap W) \qquad \text{for every } K \leq V. \tag{7}$$

Its cost is $\mathrm{cost}(y) = \sum_W y_W \dim W$. The weights depend on S and are fixed independently of K. Let $\kappa_\ell(S)$ be the infimum of the costs.

Definition 2.2 (Kernel pattern)**.** A *kernel pattern* on V is a finitely supported family of real weights $x_K \geq 0$ on subspaces $K \leq V$ such that

$$\sum_K x_K \dim(K \cap W) \leq \dim W \qquad \text{for every } W \leq V. \tag{8}$$

Its value for (S, ℓ) is $\mathrm{val}_\ell(x) = \sum_K x_K (b_\ell(S/K) - \ell)$.

Lemma 2.3 (Duality)**.** *Every kernel pattern and every certificate satisfy* $\mathrm{val}_\ell(x) \leq \mathrm{cost}(y)$*; hence* $\mathrm{val}_\ell(x) \leq \kappa_\ell(S)$*. If F is finite, then $\kappa_\ell(S)$ is a minimum and equals the maximum value of a kernel pattern.*

Proof. By (7), nonnegativity and (8),

$$\sum_K x_K (b_\ell(S/K) - \ell) \leq \sum_K x_K \sum_W y_W \dim(K \cap W) = \sum_W y_W \sum_K x_K \dim(K \cap W) \leq \sum_W y_W \dim W.$$

If F is finite, V has finitely many subspaces, and the certificate problem and the kernel-pattern problem are a finite linear program and its dual. Both are feasible: $y_V = M$ is a certificate, since $b_\ell(S/0) \leq \ell$ and $b_\ell(S/K) \leq M$ otherwise, and $x = 0$ is a pattern. Linear-programming duality gives equal attained optima. □

Lemma 2.4 (Two standard patterns)**.** *(a) If $L_1, \ldots, L_r \leq V$ are lines whose sum is direct, then $x_{L_i} = 1$ $(1 \leq i \leq r)$ is a kernel pattern.*

(b) If $e_1, \ldots, e_m$ is a basis of V, $m \geq 2$, and $H_i = \mathrm{span}(e_j : j \neq i)$, then $x_{H_i} = 1/(m-1)$ $(1 \leq i \leq m)$ is a kernel pattern.

Proof. (a) A nonzero intersection $W \cap L_i$ equals L_i. The lines contained in W have a direct sum inside W, so there are at most $\dim W$ of them. (b) Let $w = \dim W$. Then $\dim(W \cap H_i) = w - \mathbf{1}[W \not\subseteq H_i]$. The coordinate functionals restricted to W span its dual, so at least w of them are nonzero on W, that is, $W \not\subseteq H_i$ for at least w indices. Hence $\sum_i \dim(W \cap H_i) \leq mw - w = (m-1)w$. □

Example 2.5 (The hypercube pattern). Let $A \subseteq F$ have $\ell \geq 2$ elements and let $S = A^a \subseteq F^a$ in a basis $e_1, \ldots, e_a$, $a \geq 2$. The fibers modulo H_i are the ℓ layers $\{x : x_i = \alpha\}$, each of size ℓ^{a-1}, so $b_\ell(S/H_i) = M = \ell^a$. The pattern of Lemma 2.4(b) has value $a(M - \ell)/(a-1) = B(\ell, a)$. Hence $\kappa_\ell(A^a) \geq B(\ell, a)$. For the Boolean three-cube this gives $\kappa_2 \geq 9$.

The next lemma shows that an actual code's block kernels form a scaled kernel pattern and that the best table captures exactly its value.

Lemma 2.6 (Capture identity)**.** *Let $\mathcal{P}$ be an F-vector space, let $E_0, \dots, E_{n-1}$ be linear maps on $\mathcal{P}$ with kernels K_j, let $S \subseteq \mathcal{P}$ be a set of $M > \ell$ distinct points with $V = \operatorname{dir}(S)$, and suppose that for some $r > 0$*

$$\sum_{j<n} \dim(W \cap K_j) \le rn \dim W \qquad \text{for every } W \le V. \tag{9}$$

Put $x_K = |\{j : K_j \cap V = K\}|/(rn)$. Then x is a kernel pattern on V, and the largest total number of agreements of the points of S with a table of at most ℓ symbols per block is

$$\sum_{j<n} b_\ell(S/(K_j \cap V)) = n(\ell + r \operatorname{val}_\ell(x)) \le n(\ell + r\kappa_\ell(S)).$$

Proof. For $W \le V$, $\sum_K x_K \dim(K \cap W) = (rn)^{-1} \sum_j \dim(K_j \cap W) \le \dim W$. At block j the points of S with equal symbols are exactly the $(K_j \cap V)$-fibers, so ℓ symbols capture at most, and for a suitable choice exactly, $b_\ell(S/(K_j \cap V))$ points. Summing, $\sum_j (b_\ell(S/(K_j \cap V)) - \ell) = rn \operatorname{val}_\ell(x)$; the term $K = 0$ contributes zero because $M > \ell$. Lemma 2.3 gives the inequality. □

Proposition 2.7 (Certificate transfer)**.** *In the setting of Lemma 2.6, with $M > \ell$, let the encoding $f \mapsto (E_j(f))_j$ be injective and let (9) hold for every subspace $W \le \mathcal{P}$ with $1 \le \dim W \le M - 1$. Suppose $\kappa_\ell(S) \le \bar{\kappa}$ for every set S of M distinct points of $\mathcal{P}$. If $0 \le \rho$ and*

$$\ell + \bar{\kappa} r < M(1 - \rho),$$

then the code is average-radius $(\rho, \ell, M - 1)$ list recoverable.

Proof. Let S consist of M distinct messages. Its direction space has dimension at most $M-1$, so (9) holds on it. Lemma 2.6 bounds the total agreement of S with any table by $n(\ell + r\bar{\kappa}) < Mn(1 - \rho)$, so the mean error exceeds ρ. □

Independent squares. Let $\ell \ge 2$, $t \ge 1$, $c \ge 0$, let $A \subseteq F$ have ℓ elements including 0, let $p_0, \dots, p_{d-1}$ be independent with $d = 2t + c$, and put

$$S = \{0\} \cup \bigcup_{h=0}^{t-1} \{\alpha p_{2h} + \beta p_{2h+1} : (\alpha, \beta) \in A^2 \setminus \{(0,0)\}\} \cup \bigcup_{i=2t}^{d-1} \{\alpha p_i : \alpha \in A \setminus \{0\}\}. \tag{10}$$

Independence makes these $M = 1 + t(\ell^2 - 1) + c(\ell - 1)$ points distinct.

Proposition 2.8 (Squares pattern)**.** *For (10), the axis lines $Fp_0, \dots, Fp_{d-1}$ carry the kernel pattern of Lemma 2.4(a), of value $(\ell - 1)(2\ell t + c)$. Hence $\kappa_\ell(S) \ge (\ell - 1)(2\ell t + c)$.*

Proof. Modulo Fp_{2h}, the points of square h form the ℓ fibers $\{\alpha p_{2h} + \beta p_{2h+1} : \alpha \in A\}$, $\beta \in A$, each of size ℓ; all other points lie in singleton fibers, by independence. Thus $b_\ell(S/Fp_{2h}) = \ell^2$, and similarly for Fp_{2h+1}. Modulo Fp_i with $i \ge 2t$, the line Ap_i is a fiber of size ℓ and all other points are singletons; there are at least $\ell^2 - 1 \ge \ell - 1$ of them since $t \ge 1$, so $b_\ell(S/Fp_i) = 2\ell - 1$. The value is $2t(\ell^2 - \ell) + c(\ell - 1) = (\ell - 1)(2\ell t + c)$. □

Lemma 2.9 (Squares against the slope)**.** *Let $\ell, a \geq 2$ and use* (6)*. Then t is a positive integer, $M = 1 + t(\ell^2 - 1) + c(\ell - 1)$, and*

$$C = \frac{2\ell(M-1) - c(\ell-1)^2}{\ell+1} < 2M, \tag{11}$$

$$(C - B)(\ell+1)(a-1) = \begin{cases} [a(\ell-1) - 2\ell]M + \ell[a(\ell-1)+2], & a \text{ even}, \\ [a(\ell-1) - 2\ell]M + a(\ell-1) + \ell^2 + 1, & a \text{ odd}. \end{cases} \tag{12}$$

Consequently $C > B$ on the region (5)*, and $C = B$ for $a = 2$ and for $(\ell, a) = (2, 3)$.*

Proof. Reducing $N = 1 + \ell + \cdots + \ell^{a-1}$ modulo $\ell + 1$ gives remainder c, so t is an integer, positive since $N \geq \ell + 1$. Then $1 + t(\ell^2 - 1) + c(\ell - 1) = 1 + (\ell - 1)N = M$, and (11) and (12) follow by expansion. In (5) the coefficient $a(\ell-1)-2\ell$ is nonnegative and the remaining term is positive. For $a = 2$ the coefficient is -2, $c = 0$, $M = \ell^2$, and the even case gives $-2\ell^2+2\ell^2 = 0$. For $(\ell, a) = (2, 3)$ the odd case gives $-8 + 3 + 4 + 1 = 0$. □

By Example 2.5, $\sup_S \kappa_\ell(S) \geq B$ over ℓ^a-point configurations. Proposition 2.7 and the rank budget of Section 4 give the conjecture whenever the supremum equals B, and Lemma 2.9 with Proposition 2.8 shows that it exceeds B on (5).

3 The eight-point theorem

Throughout this section $\ell = 2$, captures refer to $b_2(S/K)$, and a *certificate* is one for $(S, 2)$.

3.1 Affine tools

Lemma 3.1 (Selected-fiber rank bound)**.** *Let $S = \{v_1, \ldots, v_m\}$ have affine dimension e. On $E_0 = \{c \in F^m : \sum_i c_i = 0\}$ define $T(c) = \sum_i c_i v_i$, and put $\Lambda = \ker T$. Then $\dim \Lambda = m - 1 - e$. If $K < V$, choose the two largest nonempty K-fibers A, A' and set $c = |A| + |A'|$. Let $E \leq E_0$ consist of coefficient vectors supported on $A \cup A'$ with separate coefficient sums zero on A and on A'. With $\delta = \dim(E \cap \Lambda)$,*

$$b_2(S/K) - 2 \leq \dim K + \delta. \tag{13}$$

Proof. A proper K cannot contain all differences, so there are at least two nonempty fibers. We have $\dim E = c - 2$ and $T(E) \leq K$. Rank–nullity gives $c - 2 = \dim T(E) + \delta \leq \dim K + \delta$. □

Lemma 3.2 (Adjoining affine coloops)**.** *Let T consist of $m \geq 3$ distinct points with direction space U. Adjoin j points so that S has affine dimension $\dim U + j$; equivalently, their homogenized vectors are independent modulo the homogeneous span of T. For $K \leq \mathrm{dir}(S)$,*

$$b_2(S/K) \leq b_2(T/(K \cap U)) + \dim K - \dim(K \cap U) + \mathbf{1}_{U \subseteq K}. \tag{14}$$

Consequently, if a certificate for the modified quantity $b_2(T/H) + \mathbf{1}_{H=U}$ $(H \leq U)$ has coefficient at least one on U and cost D, then S has a certificate of cost at most $D + j$.

Proof. Translate a core point to zero. The j outside points are then linearly independent in V/U. The case $K = V$ is immediate. Otherwise select two nonempty largest fibers, containing s outside points and c_T core points, and let $b \in \{0, 1, 2\}$ count the selected fibers meeting the core. The space of coefficients with zero sum on each selected fiber has image modulo U of dimension $s - (2 - b)$: a fiber not meeting the core imposes one independent zero-sum condition on its outside coefficients,

and a core coefficient absorbs that condition in a fiber meeting the core. Independence in V/U gives $s - (2 - b) \le \dim K - \dim(K \cap U)$. If $U \not\subseteq K$, the core occupies at least two fibers, and $c_T + 2 - b \le b_2(T/(K \cap U))$: when only one selected fiber meets it, a second nonempty core fiber contributes at least one; when neither does, two core fibers contribute at least two. If $U \subseteq K$, the same inequality holds with an additional one on the right. Adding proves (14). For the last assertion, add weight one on V and subtract one from the coefficient on U. The new coefficients are nonnegative, and the cost increases by $\dim V - \dim U = j$. □

Lemma 3.3 (Modified planar certificate)**.** *For $m \ge 3$ points T spanning an affine plane with direction U, there are rational $\alpha' \ge 1$, $w \ge 0$ and a line $L_1 \le U$ with*

$$b_2(T/H) + \mathbf{1}_{H=U} \le 2 + \alpha' \dim H + w \dim(H \cap L_1) \quad (H \le U), \qquad 2\alpha' + w \le m.$$

Thus a planar core of m points together with j affine coloops has a certificate of cost at most $m + j$, and m planar points alone have one of cost at most m.

Proof. For a direction line L, set $m_L = b_2(T/L) - 2$. Positive values occur only in difference directions, so there are finitely many. The two largest values $m_1 \ge m_2$ in distinct directions are positive, because an affine spanning triple supplies two directions with capture at least three. Two unions of two parallel lines in different directions meet in at most four points, so $m_1 + m_2 \le m$. Let L_1 maximize m_L and set

$$\lambda = \max\Big\{1, \frac{m-1}{m_1 + m_2}\Big\}, \quad \alpha' = \lambda m_2, \quad w = \lambda(m_1 - m_2).$$

Then $\alpha' \ge 1$, $w \ge 0$ and $2\alpha' + w = \max\{m - 1, m_1 + m_2\} \le m$. For $H = L_1$ the increment $\alpha' + w \ge m_1$; for every other line it is $\alpha' \ge m_2$. For $H = U$ the required increment is $m - 1$, and for $H = 0$ the bound is exact. Apply Lemma 3.2; without coloops, discard the indicator. □

Lemma 3.4 (Two directions)**.** *Two distinct parallel L-lines and two distinct parallel M-lines, with $L \ne M$, have at most four cross-intersections. If there are at least three, all four lines lie in one affine plane. If there are at least two, their affine span has dimension at most three.*

Proof. Each line pair has at most one intersection. Three edges of the bipartite two-by-two intersection graph connect its four vertices. An intersecting nonparallel pair determines a plane, and the parallel mates reached by those edges also lie in it. With two intersections, either two matched pairs span parallel planes of direction $L + M$, whose union has affine dimension at most three, or three lines lie in a plane and adjoining the fourth increases the dimension by at most one. □

3.2 Affine dimensions at most four

For dimension one, weight six on V works: the zero kernel captures two and V captures eight. Dimension two follows from Lemma 3.3 with $m = 8$ and $j = 0$. Dimension seven is treated in Lemma 3.9.

Lemma 3.5 (Dimension three)**.** *Eight distinct points of affine dimension three have a certificate of cost at most nine.*

Proof. If every line direction captures at most five, take $y_V = 3$: lines get right-hand side five and planes eight, so all kernels are covered. Otherwise choose a line direction L with capture $c_L \ge 6$. It is at most seven, because two parallel lines have affine span at most two. For a plane P not

containing L, its two selected cosets capture at most four points on the selected two L-lines and at most $8 - c_L$ outsiders:

$$b_2(S/P) \le 12 - c_L. \tag{15}$$

If $c_L = 7$ and another direction M captured at least five, the selected subsets would meet in at least four points, and Lemma 3.4 would make all eight points coplanar. Thus other lines capture at most four. Weights $y_V = 2$, $y_L = 3$ work: line L gets seven, other lines four, planes containing L nine and transverse planes six, enough by (15). The cost is nine.

If $c_L = 6$, no other line captures six, since four common selected points would again make all eight points coplanar. Suppose another direction captures five. The selected subsets, of sizes six and five, meet in three or four points. Three cross-intersections put the union of all eight points in a plane by Lemma 3.4, which is impossible. With four, the union of the two selected subsets has $6 + 5 - 4 = 7$ points, coplanar by Lemma 3.4; the eighth point is an affine coloop, and Lemma 3.3 with $m = 7$, $j = 1$ gives cost at most eight. Otherwise all other lines capture at most four; take $y_V = 2$, $y_L = 2$, of cost eight. Planes containing L get eight and transverse planes six, covering (15). Zero and full kernels satisfy every displayed certificate directly. □

Lemma 3.6 (Modified seven-point core)**.** *Seven distinct points T of affine dimension three, with direction U, admit a certificate for $b_2(T/H) + \mathbf{1}_{H=U}$ of cost at most eight and with coefficient on U at least one.*

Proof. If every line captures at most four, weight $5/2$ on U works. Otherwise a line L captures five or six. If it captures six, another line capturing at least five would have four common selected points, putting all seven points in a plane by Lemma 3.4. Thus all other lines capture at most four. Use $y_U = 2$, $y_L = 2$, of cost eight. A plane avoiding L captures at most five and gets six; a plane containing L gets eight. The modified full-kernel value eight is covered.

Suppose the largest line capture is five. If another direction captures five, the selected subsets meet in three or four points. Three would make all seven coplanar by Lemma 3.4. Four give $5 + 5 - 4 = 6$ coplanar points and one affine coloop. Lemma 3.3 with $m = 6$, $j = 1$ supplies an ordinary certificate on U with coefficient one on U and cost between six and seven: the modified planar core has cost at least $m - 1 = 5$ and the coloop adds one. Its full-kernel right-hand side is therefore at least eight, which covers the extra indicator. If L is the only direction capturing five, take $y_U = 2$, $y_L = 1$. Planes avoiding L capture at most $4 + 2 = 6$; those containing it get seven. The modified full-kernel value eight is covered by nine. All other ranks are immediate. □

Lemma 3.7 (Dimension four)**.** *Eight distinct points of affine dimension four have a certificate of cost at most nine.*

Proof. If a line direction captures at least six points, those six lie on two parallel lines and span at most a plane. Since the affine dimension is four, they span exactly a plane and the remaining two points are independent affine coloops; Lemma 3.3 with $m = 6$, $j = 2$ gives cost at most eight. Line captures seven or eight are incompatible with dimension four. If a plane direction captures at least seven points, these lie in an affine space of dimension at most three, and dimension four forces a seven-point three-dimensional core and one coloop; Lemmas 3.6 and 3.2 give cost at most nine. A plane cannot capture all eight.

We may assume that line captures are at most five and plane captures at most six. If no line captures five, $y_V = 9/4$ works: ranks one, two and three get $17/4$, $13/2$ and $35/4$. If exactly one line direction L captures five, $y_V = 2$, $y_L = 1$ works.

It remains to consider two different directions capturing five. Their selected subsets A, A' meet in $x = |A \cap A'| \in \{2, 3, 4\}$ points, since $|A| + |A'| - 8 = 2$ and Lemma 3.4 allows at most four. If

$x = 2$, their union is all eight points and Lemma 3.4 bounds its affine dimension by three. If $x = 3$, Lemma 3.4 puts the 7 points of $A \cup A'$ in a plane, and the last point raises the dimension to at most three. Both contradict the hypothesis. If $x = 4$, Lemma 3.4 puts the 6 points of $A \cup A'$ in a plane; they span it, since they lie in two directions, and dimension four forces the remaining two points to be independent affine coloops. Lemma 3.3 with $m = 6$, $j = 2$ gives cost at most eight. This exhausts the cases; zero and full kernels satisfy the stated weights. □

3.3 Dependency supports in affine dimensions five to seven

Use the notation of Lemma 3.1 with $m = 8$. Distinctness excludes a nonzero affine dependency supported on fewer than three points. Let D be the exact support of a nonzero dependency, and suppose the dependency space restricted to D is one-dimensional. Then its direction space U_D has dimension $|D| - 2$. If that dependency belongs to E, all points of D lie in $b \le 2$ selected fibers, with coefficient sum zero on each. The coefficient space on D with these zero-sum conditions has dimension $|D| - b$; its image has dimension $|D| - b - 1$ and lies in $K \cap U_D$. This image is nonzero: for $|D| = 3$, a split into two nonempty groups would create a singleton with nonzero coefficient, so $b = 1$; for $|D| \ge 4$ the dimension is at least $|D| - 3 \ge 1$. We refer to this as the *support observation*.

Lemma 3.8 (Dimension five)**.** *Every eight-point set of affine dimension five has a certificate of cost at most nine.*

Proof. Here $\dim \Lambda = 2$. Let D be the union of the supports of all dependencies, put $t = |D|$ and $U = \operatorname{dir}(D)$. All dependencies are supported on D, so $u = \dim U = t - 3$, and distinctness implies $t \ge 4$. For proper K put $h = \dim(K \cap U)$ and $\delta = \dim(E \cap \Lambda)$.

First suppose D is proper, so $u \le 4$. If $\delta > 0$ then $h \ge 1$: otherwise projection modulo K is injective on the affine span of D, and the two selected fibers contain at most two points of D, too few to support a dependency. If $\delta = 2$, all dependencies belong to E, so all of D lies in the two selected fibers. If $b \le 2$ of these meet D, the coefficient space on D with zero sums on the groups has image dimension $t - b - 2$, so $h \ge t - b - 2 \ge u - 1$. For $u = 3, 4$ these observations give $\delta \le h$; take $y_V = y_U = 1$, of cost $5 + u \le 9$. For $u = 1, 2$ they give $\delta \le 2h$; take $y_V = 1$, $y_U = 2$, of cost $5 + 2u \le 9$. Lemma 3.1 proves the inequalities for proper kernels, and the full kernel is covered because the cost is at least seven.

Now suppose $D = S$. Any two independent dependencies have supports whose union is all eight points, because they span Λ. Call a one-dimensional dependency subspace *small* if its support has size at most four. There are three possibilities: no small line; one small line of support size three or four; or two small lines with disjoint four-point supports. Indeed, two different small lines have union of supports all eight, hence both supports have size four and are disjoint; a combination using both has support eight, so there is no third small line.

For a proper K of dimension $\kappa' \ge 2$ we have $\delta \le \kappa'/2$. This is immediate for $\delta \le 1$. If $\delta = 2$, all eight points occur in the selected fibers, so $\dim E = 6$ and $\dim T(E) = 4$, forcing $\kappa' \ge 4$. Therefore

$$b_2(S/K) \le 2 + \tfrac{3}{2} \dim K \qquad (\dim K \ge 2). \tag{16}$$

For a line kernel, $\delta = 2$ is impossible. If $\delta = 1$, Lemma 3.1 gives capture at most four, so the dependency in E spans a small line.

With no small line, weight $3/2$ on V works, of cost $15/2$. With one small support D_0, take $y_V = 3/2$, $y_{U_{D_0}} = 1/2$, of cost at most $17/2$. The support observation supplies a nonzero intersection for any exceptional line kernel, and (16) handles the larger proper kernels.

With two small lines, use their disjoint four-point supports D_1, D_2 and $U_i = \operatorname{dir}(D_i)$, each of dimension two. Take $y_V = y_{U_1} = y_{U_2} = 1$, of cost nine. If $\delta = 2$, both dependencies belong to E,

giving nonzero intersections with both U_i. If $\delta = 1$ and its line is one of these two, one nonzero intersection suffices. Otherwise its generator uses both supports and hence all eight points; then $\dim E = 6$ and $\dim T(E) = 5$, forcing $K = V$, contrary to propriety. Thus in every proper case $\delta \le \dim(K \cap U_1) + \dim(K \cap U_2)$, as required by Lemma 3.1. In all three full-core cases, zero and full kernels satisfy the displayed certificates directly. □

Lemma 3.9 (Dimensions six and seven)**.** *In affine dimension six there is a certificate of cost at most eight; in dimension seven, of cost seven.*

Proof. In dimension six the dependency space has dimension one. Let its nonzero support D have size $t \ge 3$, so $U = \mathrm{dir}(D)$ has dimension $t-2$. If $\delta = 1$ for a proper kernel, the support observation gives $\dim(K \cap U) \ge \max\{1, t-3\} =: a'$. Thus $y_V = 1$, $y_U = 1/a'$ works and has cost $6 + (t-2)/a' \le 8$. For $\delta = 0$ ambient weight one suffices. The full kernel is covered since the cost is at least six.

In dimension seven the points are affinely independent, so $\Lambda = 0$. Lemma 3.1 gives $b_2(S/K) \le 2 + \dim K$ for proper K. Weight one on V also covers the full kernel and has cost seven. □

3.4 Proof of Theorem 1.8 and the attained costs

The upper bounds follow from Lemma 3.3 and Lemmas 3.5–3.9. All displayed weights are rational, nonnegative, finitely supported and fixed for S. The following configurations attain the seven values; each lower bound is the value of a kernel pattern from Lemma 2.4, so it holds by Lemma 2.3. Let $e_1, \dots, e_7$ be independent and $\lambda \in F \setminus \{0, 1\}$.

- *Dimension* 1*, cost* 6*:* eight collinear points ($|F| \ge 8$). The pattern $x_V = 1$ has value $8 - 2 = 6$.
- *Dimension* 2*, cost* 8*:* $\{0, 1, \lambda\}^2 \setminus \{(\lambda, \lambda)\}$ ($|F| \ge 3$). Modulo Fe_1 the fibers are the rows, of sizes $3, 3, 2$, so $b_2 = 6$, and likewise modulo Fe_2. The two lines give value $4 + 4 = 8$.
- *Dimension* 3*, cost* 9*:* the Boolean cube $\{0, 1\}^3$, by Example 2.5.
- *Dimension* 4*, cost* 9*:* $\{0, e_1, \lambda e_1, e_2, e_1 + e_2, e_3, e_4, e_3 + e_4\}$ ($|F| \ge 3$). Modulo Fe_1 the fibers $\{0, e_1, \lambda e_1\}$ and $\{e_2, e_1 + e_2\}$ give $b_2 = 5$; modulo Fe_2, Fe_3, Fe_4 the pairs $\{0, e_2\}, \{e_1, e_1 + e_2\}$; $\{0, e_3\}, \{e_4, e_3 + e_4\}$; $\{0, e_4\}, \{e_3, e_3 + e_4\}$ give $b_2 = 4$, all other fibers being singletons. The four lines give value $3 + 2 + 2 + 2 = 9$.
- *Dimension* 5*, cost* 9*:* two squares and one coloop, (10) with $\ell = 2$, $t = 2$, $c = 1$; value $4t + c = 9$ by Proposition 2.8.
- *Dimension* 6*, cost* 8*:* one square and four coloops, $t = 1$, $c = 4$; value $4 + 4 = 8$.
- *Dimension* 7*, cost* 7*:* eight affinely independent points $0, e_1, \dots, e_7$. Modulo Fe_i the fiber $\{0, e_i\}$ and a singleton give $b_2 = 3$; the seven lines give value 7.

In particular the Boolean cube has $\kappa_2 = 9$, and $\sup_S \kappa_2(S) = 9 = B(2, 3)$. □

Proposition 3.10 (Four points)**.** *Every set S of four distinct points over any field satisfies $\kappa_2(S) \le 4$, and the square $\{0, e_1, e_2, e_1 + e_2\}$ attains 4. Hence $\sup_S \kappa_2(S) = 4 = B(2, 2)$.*

Proof. Collinear points: $y_V = 2$, since $b_2(S/V) = 4$. Coplanar points spanning a plane: Lemma 3.3 with $m = 4$, $j = 0$. Affinely independent points: $\Lambda = 0$, so Lemma 3.1 gives $b_2(S/K) \le 2 + \dim K$ for proper K, and $y_V = 1$, of cost three, also covers $K = V$. For the square, both axis lines capture four, and Lemma 2.4(a) gives value $2 + 2 = 4$. □

4 Coding consequences

4.1 The folded-Wronskian budget for every set of appropriate points

The following rank bound is the folded-Wronskian argument of Guruswami and Kopparty [9], written for arbitrary appropriate points to fix its conventions.

Lemma 4.1 (Folded-Wronskian budget)**.** *Let γ generate $\mathbb{F}_q^\times$, let $s \geq 2$ and $1 \leq k \leq sn$, and let $\alpha_0, \dots, \alpha_{n-1}$ be appropriate. Let $K_j \leq \mathcal{P}_k$ be the kernel of the block map E_j of (1). For every $W \leq \mathcal{P}_k$ with $1 \leq u = \dim W \leq s$,*

$$\sum_{j<n} \dim(W \cap K_j) \leq \frac{u(k-1) - u(u-1)/2}{s-u+1} \leq \frac{u(k-1)}{s-u+1}.$$

Proof. Choose a basis $g_1, \dots, g_u$ of W with distinct degrees $d_1 < \cdots < d_u < k$, by degree elimination. The polynomial

$$D(X) = \det\bigl(g_b(\gamma^a X)\bigr)_{0 \leq a < u,\, 1 \leq b \leq u}$$

is nonzero: its coefficient of $X^{\sum_b d_b}$ is the product of the leading coefficients times the Vandermonde determinant $\det(\gamma^{ad_b})$ in the elements γ^{d_b}. These are distinct because γ has order $q-1 \geq sn \geq k > d_b \geq 0$; here $q-1 \geq sn$ because appropriate points with $s \geq 2$ are sn distinct nonzero elements. Moreover $\deg D \leq \sum_b d_b \leq u(k-1) - u(u-1)/2$.

Put $h_j = \dim(W \cap K_j)$. A change of basis of W multiplies D by a nonzero scalar, so we may assume that $g_1, \dots, g_{h_j}$ vanish at all points of block j. For $0 \leq t \leq s-u$, every entry of these columns at $X = \gamma^t \alpha_j$ is $g_b(\gamma^{a+t}\alpha_j)$ with $a + t \leq s-1$, hence zero. Each such column is divisible by $X - \gamma^t \alpha_j$, so D vanishes there to order at least h_j. The points $\gamma^t \alpha_j$ ($0 \leq t \leq s-u$, $0 \leq j < n$) are distinct, because the evaluation points are appropriate. Summing multiplicities gives $(s-u+1)\sum_j h_j \leq \deg D$. □

Proof of Theorem 1.3. The code is injective since $k \leq sn$. By Lemma 4.1, every $W \leq \mathcal{P}_k$ with $1 \leq \dim W = u \leq 7 \leq s$ satisfies $\sum_j \dim(W \cap K_j) \leq u(k-1)/(s-6) = rn\,u$ with $r = (k-1)/(n(s-6))$. Theorem 1.8 gives $\kappa_2(S) \leq 9$ for every set of eight distinct messages. By Proposition 2.7 with $\ell = 2$, $M = 8$ and $\bar{\kappa} = 9$, it suffices that $2 + 9r < 8(1-\rho)$, which is (4). □

Corollary 4.2 (Asymptotic form)**.** *Fix $0 \leq \rho < 3/4$, put $B_\rho = 2/3 - 8\rho/9$, and let $0 < \eta < B_\rho$. Under the remaining hypotheses of Theorem 1.3, rate $R = k/(sn) \leq B_\rho - \eta$ and folding $s \geq 7 + \lceil 4/\eta \rceil$ suffice for average-radius $(\rho, 2, 7)$ list recovery.*

Proof. Here $R \leq 2/3$ and $s - 6 > 4/\eta$, so

$$\frac{k-1}{n(s-6)} < \frac{Rs}{s-6} = R + \frac{6R}{s-6} \leq R + \frac{4}{s-6} < R + \eta \leq B_\rho.$$ □

Proof of Corollary 1.4. Let $R \leq 2/3$ and $\rho = \Phi_{2,3}(R) - \varepsilon$. If $\rho < 0$ the statement holds trivially, since mean errors are nonnegative. Otherwise $0 \leq \rho < 3/4$ and, by (2), with $\eta = 8\varepsilon/9$, $B_\rho = 2/3 - 8\rho/9 = R + 8\varepsilon/9 = R + \eta$. Thus $0 < \eta < B_\rho$ and $R = B_\rho - \eta$, and Corollary 4.2 applies for $s \geq 7 + \lceil 4/\eta \rceil = C(\varepsilon)$, since $4/\eta = 9/(2\varepsilon)$. The rate-slack form is Corollary 4.2 itself. □

The transfer applies at every (ℓ, a) for which the eight-point inequality has an analogue.

Corollary 4.3 (General transfer)**.** *Let $\ell, a \geq 2$, $M = \ell^a$, and suppose $\kappa_\ell(S) \leq B(\ell, a)$ for every set S of M distinct points over $\mathbb{F}_q$. Let $\varepsilon > 0$ and $R \leq (a-1)/a$. For every*

$$s \geq M - 1 + \Big\lceil \frac{(M-\ell)(M-2)}{M\varepsilon} \Big\rceil,$$

every rate-R s-folded Reed–Solomon code over $\mathbb{F}_q$ with appropriate evaluation points is average-radius $(\Phi_{\ell,a}(R) - \varepsilon, \ell, M-1)$ list recoverable. By Proposition 3.10 this applies at $(\ell, a) = (2, 2)$ over every field and gives the case $(\ell, L) = (2, 3)$ of Conjecture 1.1 in average-radius form, with $s \geq 3 + \lceil 1/\varepsilon \rceil$. At $(\ell, a) = (2, 3)$ the threshold is $7 + \lceil 9/(2\varepsilon) \rceil = C(\varepsilon)$ of Corollary 1.4.

Proof. Put $r = (k-1)/(n(s-M+2))$. For $1 \leq u \leq M-1 \leq s$, Lemma 4.1 gives $\sum_j \dim(W \cap K_j) \leq u(k-1)/(s-u+1) \leq rnu$. With $\rho = \Phi_{\ell,a}(R) - \varepsilon$, identity (3) gives $M(1-\rho) = \ell + BR + M\varepsilon$; if $\rho < 0$ there is nothing to prove. Proposition 2.7 with $\bar{\kappa} = B$ requires $B(r-R) < M\varepsilon$. Now $r < Rs/(s-M+2) = R + R(M-2)/(s-M+2)$ and $BR \leq M - \ell$ since $R \leq (a-1)/a$, so $B(r-R) < (M-\ell)(M-2)/(s-M+2) \leq M\varepsilon$ for the stated s. At $(\ell, a) = (2, 2)$, $(M-\ell)(M-2)/M = 1$; at $(\ell, a) = (2, 3)$ it is $9/2$. □

4.2 Sharpness

Proposition 4.4 (The cap-seven radius is exact)**.** *Let $s \geq 1$ and let an s-folded Reed–Solomon code with appropriate evaluation points satisfy $(k-1)/(sn) \leq 2/3$ and $k - 1 \geq 2s$. If it is $(\rho, 2, 7)$ list recoverable, then*

$$\rho \leq \frac{3}{4}\Big(1 - \Big\lfloor \frac{3}{2} \Big\lfloor \frac{k-1}{s} \Big\rfloor \Big\rfloor \frac{1}{n}\Big) \leq \Phi_{2,3}(R) + \frac{3}{2n}.$$

Consequently, for every $\varepsilon > 0$ and every such code with $n > 3/(2\varepsilon)$, the code is not $(\Phi_{2,3}(R) + \varepsilon, 2, 7)$ list recoverable. Together with Corollary 1.4, the list-recovery radius at $(\ell, L) = (2, 7)$ of folded Reed–Solomon codes with appropriate evaluation points, large folding and large length is exactly $\Phi_{2,3}(R)$ at every rate $0 < R \leq 2/3$, in both the ordinary and the average-radius sense.

Proof. Apply Theorem 1.2 with $\ell = 2$, $L = 7$, $m = 3$ and $q \geq 2$. With $N = \lfloor (k-1)/s \rfloor$, we have $\lfloor \frac{3}{2} N \rfloor \geq \frac{3}{2}N - \frac{1}{2}$ and $N \geq (k-s)/s$, so the floor is at least $3k/(2s) - 2$, and $k = Rsn$ gives the second inequality. An average-radius list recoverable code is list recoverable, so the bound applies to both notions. □

4.3 Finite-folding profiles

For nonnegative support budgets $c_1, \ldots, c_{\min(7,k)}$ put $\theta_e = \max_{1 \leq u \leq e} c_u/u$ and define, when the index is available,

$$\begin{aligned}
&\Pi_1 = 6c_1, \quad \Pi_2 = 8\theta_2, \quad \Pi_3 = 9\theta_3, \quad \Pi_4 = 9\theta_4, \\
&\Pi_5 = \max\{c_5 + 2c_1,\ c_5 + 2c_2,\ c_5 + c_3,\ c_5 + c_4,\ \tfrac{3}{2}c_5,\ \tfrac{3}{2}c_5 + \tfrac{1}{2}c_1,\ \tfrac{3}{2}c_5 + \tfrac{1}{2}c_2\}, \\
&\Pi_6 = c_6 + \max_{1 \leq u \leq 6} \frac{c_u}{\max(1, u-1)}, \qquad \Pi_7 = c_7.
\end{aligned}$$

Proposition 4.5 (Support-budget transfer)**.** *Suppose a linear polynomial encoding has kernels $K_0, \ldots, K_{n-1}$, is injective on $\mathcal{P}_k$, and satisfies*

$$\sum_j \dim(W \cap K_j) \leq c_u \qquad (\dim W = u,\ 1 \leq u \leq \min(7, k)).$$

If $0 \leq \rho < 3/4$ and $\max_{1 \leq e \leq \min(7,k)} \Pi_e < n(6 - 8\rho)$, then it is average-radius $(\rho, 2, 7)$ list recoverable.

Proof. For a fixed eight-message configuration, summing its certificate over all blocks bounds the total capture by $2n + \sum_W y_W c_{\dim W}$. For affine dimensions one through four, the cost bounds and $c_u \le u\theta_e$ give $\Pi_1, \dots, \Pi_4$. The proper-core certificates of Lemma 3.8 contribute $c_5 + 2c_u$ for $u = 1, 2$ or $c_5 + c_u$ for $u = 3, 4$; its full-core certificates contribute $\frac{3}{2}c_5$, $\frac{3}{2}c_5 + \frac{1}{2}c_u$ for $u = 1, 2$, or $c_5 + 2c_2$. These are the branches of Π_5. Lemma 3.9 gives ambient weight one and support weight $1/\max(1, u-1)$ in dimension six, and ambient weight one in dimension seven; these give Π_6 and Π_7. The strict inequality excludes total capture at least $8n(1-\rho)$. No monotonicity of the budgets in u is required. □

Lemma 4.1 supplies the budgets $b_u = (u(k-1) - u(u-1)/2)/(s-u+1)$, for every set of appropriate points. In the consecutive model, windows that cross the ends of an evaluation block improve the budgets themselves.

Lemma 4.6 (Cyclic folded-Wronskian budget)**.** *In the consecutive model $\alpha_j = \gamma^{js}$ with $sn \le q-1$, $s \ge 2$ and $1 \le k \le sn$, let $1 \le u \le \min(s, k)$, $\dim W = u$ and $h_j = \dim(W \cap K_j)$. Then*

$$\sum_{j<n} h_j(s - u + h_j) \le D_u^{\mathrm{fold}} := u(k-1) - u(u-1)/2.$$

Proof. Use the matrix $\mathsf{M}(X) = (g_b(\gamma^a X))_{0\le a<u,\, 1\le b\le u}$ of Lemma 4.1; its nonzero determinant has degree at most D_u^{fold}. Write $Q = q-1$. At $X = \gamma^t$ the rows evaluate at the u distinct cyclic exponents $t, t+1, \dots, t+u-1$ modulo Q. Partition them among the disjoint blocks $B_j = \{js, \dots, js+s-1\}$ and the gap $\{sn, \dots, Q-1\}$. If $r_j(t)$ rows belong to block j, their rank is at most $\min(r_j(t), u-h_j)$, since the full block map on W has kernel dimension h_j; gap rows have rank at most their number. Writing $x_+ = \max\{x, 0\}$,

$$u - \operatorname{rank} \mathsf{M}(\gamma^t) \ge \sum_j \big(h_j + r_j(t) - u\big)_+.$$

The determinant of a polynomial square matrix vanishes to order at least its nullity at the evaluation point: constant invertible row and column operations make its last nullity-many rows zero there, so each such row is divisible by the root factor. This holds in every characteristic and pays all block deficits at a shared root before roots are summed.

If $n = 1$, then $k \le s$ makes the block map injective and $h_0 = 0$. Suppose $n \ge 2$. Then $Q \ge sn \ge 2s \ge s + u$, and for a fixed length-s block the sliding length-u window has overlap u at $s-u+1$ starts and overlap r at two starts for each $1 \le r < u$. Thus, for $0 \le h \le u$,

$$\sum_{t \bmod Q} \big(h + r_j(t) - u\big)_+ = h(s-u+1) + 2\sum_{e=1}^{h-1} e = h(s-u+h).$$

Sum the determinant valuations at the Q distinct roots γ^t, interchange the finite nonnegative sums, and use the degree bound. □

For each integer $H \ge 0$ write $m = \lfloor H/n \rfloor$ and $r = H - nm$, so $0 \le r < n$. For a numerator $D_u \ge 0$ define the integer budget

$$c_u(D_u) = \max\Big\{ H \in \mathbb{Z} : \begin{array}{l} 0 \le H \le n\min(u, \max(k-s, 0)), \\ (s-u)H + nm^2 + r(2m+1) \le D_u \end{array} \Big\}. \tag{17}$$

The set contains zero. For $H = \sum_j h_j$, integer convexity gives $\sum_j h_j^2 \ge nm^2 + r(2m+1)$: moving one unit between two entries that differ by at least two decreases their square sum. Also $h_j \le$

$\min(u, \max(k-s, 0))$, by divisibility by the block's degree-s vanishing polynomial. Lemma 4.6 therefore supplies the budgets $c_u = c_u(D_u^{\mathrm{fold}})$ in Proposition 4.5.

For $n = 10$, $s = 29$, $k = 120$, $q = 512$ and $\rho = 1/4$, in the consecutive model, these budgets and the seven profiles are

$$(4, 8, 12, 17, 22, 27, 32), \qquad (24, 32, 36, 153/4, 39, 35, 32).$$

Their maximum is $39 < 40 = n(6 - 8\rho)$, so the mean capture is at most $2 + 39/10 = 59/10 < 6 = 8(1-\rho)$. The order condition holds since $511 \geq 290$. This certifies folding 29 for these parameters, whereas the budgets b_u certify folding 30 (profile maximum $2155/54 < 40$). The accompanying program `verify_certificates.py` reproduces both comparisons in exact arithmetic, together with the folding-28 control, whose profile maximum 41 exceeds the threshold.

4.4 Multiplicity codes

The same certificate applies to multiplicity codes through the classical derivative Wronskian [9, 5].

Proposition 4.7 (Multiplicity codes)**.** *Let $\mathbb{F}_q$ have characteristic p, let $n \geq 1$, $s \geq 7$ and $1 \leq k \leq \min(p, sn)$, and choose distinct $\alpha_0, \ldots, \alpha_{n-1} \in \mathbb{F}_q$. Encode $\deg f < k$ by the Hasse-derivative blocks $(f^{[0]}(\alpha_j), \ldots, f^{[s-1]}(\alpha_j))$. For $0 \leq \rho < 3/4$, condition (4) suffices for average-radius $(\rho, 2, 7)$ list recovery. More sharply, Proposition 4.5 applies with $c_u = c_u(D_u^{\mathrm{mult}})$, where $D_u^{\mathrm{mult}} = u(k-u)$ and c_u is given by (17).*

Proof. The block kernel consists of the polynomials divisible by $(X - \alpha_j)^s$, in every characteristic, and injectivity follows from $k \leq sn$. Let $\dim W = u \leq \min(s, k)$ and choose a basis with distinct degrees $d_1 < \cdots < d_u < k$. The hypothesis $k \leq p$ enters twice. First, the ordinary derivative Wronskian $\det(g_b^{(a)})_{0 \leq a < u,\, 1 \leq b \leq u}$ has leading coefficient equal to the product of the leading coefficients times $\prod_{b<b'}(d_{b'} - d_b)$, which is nonzero in $\mathbb{F}_q$ because the d_b are distinct integers below p; its degree is at most $\sum_b d_b - u(u-1)/2 \leq u(k-u)$. Second, at a fixed α_j, Taylor elimination gives a basis with distinct orders of vanishing $0 \leq \nu_1 < \cdots < \nu_u < k$, exactly $h_j = \dim(W \cap K_j)$ of which are at least s. The lowest-order coefficient of the Wronskian at α_j is again a nonzero multiple of $\prod_{i<i'}(\nu_{i'} - \nu_i)$, nonzero since $\nu_i < p$, so the valuation at α_j equals $\sum_i \nu_i - u(u-1)/2$. The low orders are at least $0, \ldots, u - h_j - 1$ and the high ones at least $s, \ldots, s + h_j - 1$, so the valuation is at least $h_j(s - u + h_j)$. Summing over the distinct points gives $\sum_j h_j(s - u + h_j) \leq u(k-u)$. Integer convexity gives the budgets (17). The coarse inequality $\sum_j h_j \leq u(k-1)/(s-u+1)$ follows as well, so the proof of Theorem 1.3 gives condition (4). □

At $n = 10$, $s = 28$, $k = 120$, $p = q = 331$ and $\rho = 1/4$, the multiplicity budgets and profiles are

$$(4, 8, 13, 17, 22, 27, 32), \qquad (24, 32, 39, 39, 39, 35, 32),$$

with maximum $39 < 40$. This folding-28 example uses the characteristic hypothesis $k \leq p$; the folding-29 example above uses a primitive element of the characteristic-two field $\mathbb{F}_{512}$.

5 Independent squares and average-radius obstructions

In this section $\ell = 2$ and $A = \{0, 1\}$, so (10) becomes

$$S = \{0\} \;\cup\; \bigcup_{h=0}^{t-1} \{p_{2h}, p_{2h+1}, p_{2h} + p_{2h+1}\} \;\cup\; \{p_{2t}, \ldots, p_{d-1}\}, \tag{18}$$

with $t \geq 1$, $c \geq 0$, $d = 2t + c$, $M = 1 + 3t + c$ and $C = 4t + c$. The term "square" means the affine parallelogram $\{0, a, b, a + b\}$; it is valid in characteristic two.

5.1 The exact cost

Proof of Theorem 1.9. The lower bound for every ℓ is Proposition 2.8. For $\ell = 2$ write $V = U_0 \oplus \cdots \oplus U_{t-1} \oplus W_0$ with $a_h = p_{2h}$, $b_h = p_{2h+1}$ $(0 \le h < t)$, $U_h = \operatorname{span}(a_h, b_h)$ and W_0 spanned by the coloop vectors. We show that weight one on V and weight one on each U_h is a certificate, of cost $d + 2t = 4t + c$; weights add when named supports coincide, as for $t = 1$, $c = 0$, where $U_0 = V$ receives weight two.

If K is proper, the spanning property of S ensures at least two fibers. Choose the two largest, A', B', and put $r = |A'| + |B'|$. In the coefficient space F^S let E consist of the vectors supported on $A' \cup B'$ with zero coefficient sum on A' and on B'; then $\dim E = r - 2$ over every field. With $T(\lambda) = \sum_v \lambda_v v$ on the zero-sum hyperplane and $\Lambda = \ker T$, Lemma 3.1 gives

$$r - 2 \le \dim K + \dim(E \cap \Lambda). \tag{19}$$

For each square define the relation $\lambda^{(h)}$ with coefficients $1, -1, -1, 1$ at $0, a_h, b_h, a_h + b_h$. These relations lie in Λ and form a basis of it: the independent coordinates in $T(\lambda) = 0$ give $\lambda_{a_h} = \lambda_{b_h} = -\lambda_{a_h + b_h}$ and zero coefficients on the coloops, and the zero-sum condition fixes λ_0; they are independent because $a_h + b_h$ occurs in only its own relation.

If $K \cap U_h = 0$, the quotient map is injective on U_h, so $a_h, b_h, a_h + b_h$ have distinct images and the two selected fibers cannot contain all three. Every vector of E vanishes at one of these three coordinates, which occurs only in $\lambda^{(h)}$, with coefficient ± 1. Hence every vector of $E \cap \Lambda$ has zero $\lambda^{(h)}$-coefficient, and

$$\dim(E \cap \Lambda) \le |\{h : K \cap U_h \ne 0\}| \le \sum_h \dim(K \cap U_h).$$

This includes characteristic two, where $-1 = 1 \ne 0$. Together with (19) this proves (7) for every proper K, including $K = 0$. At $K = V$ the left side is $M = 1 + 3t + c$ and the right side $2 + d + 2t = 2 + 4t + c$. □

For $M = 2^a$ the profile of (6) has the following constants:

M	t	c	d	C	$B(2, a)$
4	1	0	2	4	4
8	2	1	5	9	9
16	5	0	10	20	56/3
32	10	1	21	41	75/2

5.2 A finite converse for every linear code

Let $\mathcal{C} \le (\mathbb{F}_q^s)^n$ be $\mathbb{F}_q$-linear of $\mathbb{F}_q$-dimension k and rate $R_n = k/(sn)$; linearity over $\mathbb{F}_{q^s}$ is not required. For a table $\mathcal{A} = (A_1, \ldots, A_n)$ of nonempty symbol sets and a finite set $\mathcal{S}$ of codewords, the mean error is

$$D(\mathcal{S}, \mathcal{A}) = 1 - \frac{1}{|\mathcal{S}| n} \sum_{w \in \mathcal{S}} \sum_{j=1}^{n} \mathbf{1}[w_j \in A_j].$$

Theorem 5.1 (Finite independent-square converse)**.** *Let $\mathcal{C} \le (\mathbb{F}_q^s)^n$ be $\mathbb{F}_q$-linear of dimension $k \ge d$ and put*

$$u = \Big\lfloor \frac{k - d}{s} \Big\rfloor, \qquad \mathcal{E} = \min\{2n,\ n + 2tu,\ Cu\}.$$

There are M distinct codewords $\mathcal{S} \subseteq \mathcal{C}$ and lists $A_j \subseteq \mathbb{F}_q^s$ with $1 \le |A_j| \le 2$ such that

$$\sum_{w \in \mathcal{S}} \sum_{j=1}^{n} \mathbf{1}[w_j \in A_j] \ge 2n + \mathcal{E}, \qquad \textit{hence} \qquad D(\mathcal{S}, \mathcal{A}) \le 1 - \frac{2}{M} - \frac{\mathcal{E}}{Mn}.$$

Proof. Choose disjoint sets $G_0, \dots, G_{d-1} \subseteq \{1, \dots, n\}$, each of size at most u, filling the first $2t$ to capacity before the remaining c. The total square-group and coloop-group sizes are $\Sigma_1 = \min\{n, 2tu\}$ and $\Sigma_2 = \min\{n - \Sigma_1, cu\}$. Let N_i be the subspace of codewords vanishing on G_i. Rank–nullity gives $\dim N_i \ge k - s|G_i| \ge k - su \ge d$. Inductively choose $v_i \in N_i \setminus \operatorname{span}(v_0, \dots, v_{i-1})$, possible since $i < d \le \dim N_i$. Form $\mathcal{S}$ by (18) with $p_i = v_i$; independence makes its M elements distinct.

At $j \in G_i$ with $i < 2t$, let i' be the partner of i and put $A_j = \{0, (v_{i'})_j\}$. The four words $0, v_i, v_{i'}, v_i + v_{i'}$ agree, since their symbols are $0, 0, (v_{i'})_j, (v_{i'})_j$; if $(v_{i'})_j = 0$ the table is a singleton and the agreements remain. At $j \in G_i$ with $i \ge 2t$, and at every remaining coordinate, put $A_j = \{0, (v_0)_j\}$; this covers the three words $0, v_i, v_0$, respectively the two words $0, v_0$. The total agreement is at least $4\Sigma_1 + 3\Sigma_2 + 2(n - \Sigma_1 - \Sigma_2) = 2n + 2\Sigma_1 + \Sigma_2$. If $n \le 2tu$ then $2\Sigma_1 + \Sigma_2 = 2n$; if $2tu < n \le du$ it is $n + 2tu$; if $n \ge du$ it is Cu. In all cases it equals $\mathcal{E}$. □

A singleton list may be padded by an unused symbol, since $q^s \ge 2$; this gives lists of exactly two symbols and cannot decrease agreement.

Corollary 5.2 (Asymptotic converse)**.** *Put $e(x) = \min\{2, 1 + 2tx, Cx\}$. If $k \ge d$, the code of Theorem 5.1 contains M distinct codewords and a table with*

$$D(\mathcal{S}, \mathcal{A}) \le 1 - \frac{2}{M} - \frac{e(R_n)}{M} + \frac{C(d/s + 1)}{Mn} \le 1 - \frac{2}{M} - \frac{e(R_n)}{M} + \frac{C(d+1)}{Mn},$$

uniformly in s and q.

Proof. The choice of u gives $0 \le R_n - u/n \le (d/s + 1)/n$, and $\mathcal{E}/n = e(u/n)$. The function e is nondecreasing and C-Lipschitz, since its three affine pieces have slopes between 0 and C. Hence $\mathcal{E}/n \ge e(R_n) - C(d/s + 1)/n$. □

Proof of Theorem 1.7. Here $t = \lfloor (M-1)/3 \rfloor$ and $c = (M-1) \bmod 3$, which agrees with (6). Write $B = B(2, a)$. Lemma 2.9 gives $C > B$ for $a \ge 4$. We also have $4t > B$: for even a, $4t = C$; for odd $a \ge 5$, $4t - B = (a-4)(M-2)/(3(a-1)) > 0$. Let $0 < R < 2/B$. Then $2 > BR$ and $CR > BR$; and $1 + 2tR > BR$, immediately if $B \le 2t$, and otherwise because $(B - 2t)R < (B - 2t)2/B = 2 - 4t/B < 1$. Thus $e(R) > BR$. Put $\varepsilon = (e(R) - BR)/(2M)$ and let $n_0 \ge \max\{d/R,\ C(d+1)/(M\varepsilon)\}$. For $n \ge n_0$ and rate exactly R we have $k = Rsn \ge d$, and by Corollary 5.2 and (3),

$$D(\mathcal{S}, \mathcal{A}) \le 1 - \frac{2 + BR}{M} - 2\varepsilon + \frac{C(d+1)}{Mn} \le \Phi_{2,a}(R) - \varepsilon.$$

For $a = 4$, $B = 56/3$ and $2/B = 3/28$. □

For $a = 4$ the obstruction is $\frac{7}{8} - \frac{5}{4}\min\{R, \frac{1}{10}\}$, whereas $\Phi_{2,4}(R) = \frac{7}{8} - \frac{7}{6}R$. At $M = 16$ the configuration has cost 20, exceeding the hypercube value $56/3$.

5.3 Exact realization in full-length folded Reed–Solomon codes

The following polynomial construction realizes prescribed axis kernels, and blocks injective on the whole configuration, exactly.

Lemma 5.3 (Polynomial realization)**.** *Fix integers $D \geq d \geq 1$ and $s \geq 1$, with $s \geq d$ if $D > d$ and $s \geq d-1$ if $D = d$. Suppose $q - 1 = Dsm$ for a positive integer m, let γ generate $\mathbb{F}_q^\times$, and use the consecutive full-length code with $n = Dm$. Put $\delta = \gamma^m$ and, for $0 \leq i < D$,*

$$P_i(Y) = \prod_{u=0}^{s-1} (Y - \delta^{si+u}), \qquad p_i(X) = P_i(X^m).$$

The polynomials $p_0, \ldots, p_{d-1}$ are independent, each of degree sm, and on $V = \operatorname{span}\{p_0, \ldots, p_{d-1}\}$

$$\ker(E_{i+Dj}|_V) = \begin{cases} \mathbb{F}_q p_i, & 0 \leq i < d, \\ \{0\}, & d \leq i < D, \end{cases} \qquad 0 \leq j < m. \tag{20}$$

Proof. The element δ has order Ds. Write $P_0(Y) = \sum_{r=0}^{s} (-1)^r e_{s,r} Y^{s-r}$. The q-binomial identity gives

$$e_{s,r} = \delta^{r(r-1)/2} \prod_{u=0}^{r-1} \frac{1 - \delta^{s-u}}{1 - \delta^{r-u}}, \qquad 0 \leq r \leq s,$$

with the empty product equal to one. Indeed the coefficients of $\prod_{u=0}^{s-1}(1 + \delta^u T)$ obey $e_{s,r} = e_{s-1,r} + \delta^{s-1} e_{s-1,r-1}$, and after removing $\delta^{r(r-1)/2}$ the displayed products satisfy the q-Pascal rule $\begin{bmatrix} s \\ r \end{bmatrix}_\delta = \begin{bmatrix} s-1 \\ r \end{bmatrix}_\delta + \delta^{s-r} \begin{bmatrix} s-1 \\ r-1 \end{bmatrix}_\delta$, whose verification reduces to $1 - \delta^s = (1 - \delta^{s-r}) + \delta^{s-r}(1 - \delta^r)$. All factors are nonzero, since their positive exponents are at most $s < Ds$, so every coefficient of P_0 is nonzero.

The parameters $\theta_i = \delta^{si}$ are D distinct elements, since δ^s has order D, and $P_i(Y) = \theta_i^s P_0(Y/\theta_i)$ has coefficient $(-1)^r e_{s,r} \theta_i^r$ at Y^{s-r}. Put $e' = d + 1$ if $D > d$ and $e' = d$ if $D = d$; then $s \geq e' - 1$. On any e' of the P_i, the coefficient rows $r = 0, \ldots, e' - 1$ form an invertible diagonal matrix times a Vandermonde matrix, so any e' of the P_i are independent. Substitution $Y = X^m$ preserves independence.

For a point of block $r = i + Dj$, $(\gamma^{s(i+Dj)+u})^m = \delta^{si+u}$, so every $P(X^m)$ takes the same block value on the m replicas of type i. A polynomial P of degree at most s vanishes at the s distinct points $\delta^{si}, \ldots, \delta^{si+s-1}$ exactly when it is a scalar multiple of P_i. For $i < d$ this gives the axis kernel on V. For $d \leq i < D$, the span of $P_0, \ldots, P_{d-1}$ meets $\mathbb{F}_q P_i$ only in zero, by the independence of any $d + 1$ of the P_i. □

Theorem 5.4 (Full-length realization)**.** *Let $t \geq 1$, $c \geq 0$, $s \geq d - 1$, $ds \mid q - 1$, $m = (q-1)/(ds)$, $n = dm$, and $sm + 1 \leq k \leq sn$. The consecutive full-length s-folded code contains the M distinct messages* (18) *and a table of exactly two symbols per block with mean error*

$$1 - \frac{8t + 3c}{Md} = 1 - \frac{2}{M} - \frac{C}{Md}.$$

For $t = 5$, $c = 0$ the mean error is $3/4$; the zero message has error zero and every other message has error $4/5$.

Proof. Apply Lemma 5.3 with $D = d$; since $k > sm$, V lies in the message space. At a square type $i < 2t$ with partner i' use $\{0, E_{i+dj}(p_{i'})\}$; the symbols are distinct by (20), and equality of evaluations is equality of all coefficients other than the ith, so the two fibers on S are exactly $\{0, p_i\}$ and $\{p_{i'}, p_i + p_{i'}\}$: four agreements. At a coloop type $i \geq 2t$ use $\{0, E_{i+dj}(p_0)\}$: the fibers are $\{0, p_i\}$

and $\{p_0\}$, three agreements. The total is $(8t+3c)m$ out of $Mn = Mdm$, and $2d+C = 8t+3c$. For $t = 5$, $c = 0$, the zero message agrees at all $10m$ blocks and each other message at the $2m$ blocks of its square. □

Proposition 5.5 (Fixed rate)**.** *Fix a rational $R_1 \in (1/d, 1)$ and an integer $s \geq d-1$. There are arbitrarily large prime powers q for which the code of Theorem 5.4 has rate exactly R_1. In particular, for every folding threshold and length threshold there is such a code with $t = 5$, $c = 0$, rate $5/48$ and mean error $3/4$ beyond both thresholds, while $\Phi_{2,4}(5/48) = 217/288 > 3/4 + 1/1000$.*

Proof. Write $R_1 = u_0/v_0$ in lowest terms, let $D' = \operatorname{lcm}(ds, v_0)$, choose a prime $\pi \nmid D'$ and put $q = \pi^{\varphi(D')h}$. Euler's theorem gives $D' \mid q-1$; set $m = (q-1)/(ds)$, $n = (q-1)/s$ and $k = R_1(q-1)$. Then $k/(sn) = R_1$, $k < sn$, and $k - sm = (R_1 - 1/d)(q-1) \geq 1$ for large h. For the last assertion choose $s \geq 9$ above the folding threshold, then h large; here $k - sm = (q-1)/240$, and $217/288 - 3/4 = 1/288$. □

Two explicit instances over prime fields, $(q, \gamma, s, m, n, k) = (541, 2, 9, 6, 60, 55)$ at rate $11/108$ and $(2161, 23, 9, 24, 240, 225)$ at rate $5/48$, have mean error $3/4$, below the hypercube radii $245/324$ and $217/288$. The accompanying files `q541_explicit_certificate.json` and `q2161_fixed_rate_certificate.json` record every polynomial, table and agreement bit, and `validate_frs_certificate.py` re-evaluates them from raw polynomial evaluations.

6 Ordinary counterexamples

Throughout this section (ℓ, a) lies in (5) and M, N, c, t, d, C, B are as in (6); blocks are indexed by r. Theorem 1.7 bounds a mean; here every message individually meets the radius. The squares (10) give unequal individual agreements, and blocks on which every selected message has a distinct symbol, scheduled by prescribed degrees, equalize them.

6.1 Padding and degree scheduling

Lemma 6.1 (Uniform subset scheduling)**.** *Let $G \geq 0$ and let nonnegative integers $(z_v)_{v \in S}$ satisfy $\sum_v z_v = \ell G$ and $\max_v z_v \leq G$. There is a multiset of G subsets of S, each of size exactly ℓ, in which v occurs exactly z_v times.*

Proof. Induct on G; at $G = 0$ all degrees vanish. If $G > 0$, at least ℓ degrees are positive, since fewer could not sum to ℓG while each is at most G. Select the ℓ largest positive degrees and decrease each by one. Every degree equal to G is selected, since otherwise at least $\ell + 1$ degrees equal G, exceeding the total. The new maximum is at most $G - 1$ and the new sum is $\ell(G-1)$. Repeated subsets are permitted; repeated elements inside a subset are not. □

Proposition 6.2 (Ordinary padding)**.** *Let $D \geq (Md - C)/\ell$ be an integer, let $s \geq d$, and let $q \geq \ell$ be a prime power with $DsM \mid q - 1$. Put $m = (q-1)/(Ds)$ and $n = Dm$, and let $sm < k \leq sn$. The consecutive full-length s-folded code of dimension k contains M distinct messages and a table of exactly ℓ symbols per block against which every message has exactly $m(\ell D + C)/M$ agreements, that is, agreement fraction $\tau_D = (\ell D + C)/(MD)$.*

Proof. Lemma 5.3 supplies independent degree-sm polynomials $p_0, \ldots, p_{d-1}$ spanning V, with kernel $\mathbb{F}_q p_i$ on special type $i < d$ and zero kernel on every other type, each type having m blocks; V lies in the message space since $k > sm$. Choose $A \subseteq \mathbb{F}_q$ of size ℓ containing $0, 1$, and let S be (10); $|S| = M$.

At special type $2h$ use the ℓ symbols $E_{2h}(\beta p_{2h+1})$, $\beta \in A$; at type $2h+1$ use $E_{2h+1}(\alpha p_{2h})$, $\alpha \in A$. The symbols are distinct because the kernel is the other axis of the square, and the selected fibers capture precisely the ℓ^2 square messages: the zero fiber is the A-axis and the others are the parallel A-lines, while no other message enters them, by coordinate independence. If $c = 1$, at the remaining axis use symbol zero and the $\ell-1$ symbols $E_i(\beta p_0)$, $\beta \in A \setminus \{0\}$: the zero fiber is the line Ap_i and each other selected fiber is the single message βp_0, so exactly $2\ell-1$ messages are captured; $t \geq 1$ ensures that p_0 belongs to a square.

Let h_v count the special types capturing v. Then

$$0 \leq h_v \leq d, \qquad \sum_{v \in S} h_v = 2t\ell^2 + c(2\ell - 1) = \ell d + C, \tag{21}$$

and v has mh_v special agreements. There are $G = (D-d)m$ generic blocks. Prescribe $z_v = m((\ell D + C)/M - h_v)$, an integer since $M \mid m$, and nonnegative because $\ell D + C \geq Md$ gives $(\ell D + C)/M \geq d \geq h_v$; the origin has $h_v = d$. For $z_v \leq G$ it suffices, as $h_v \geq 1$, that $(M-\ell)D \geq Md + C - M$. In (5) one has $d \geq 7$ and $M/\ell \geq 4$. Put $x = Md - C$; then $x \geq M(d-2) \geq 5M$ by (11), and $\ell D \geq x$ gives

$$(M-\ell)D - (Md + C - M) \geq \Big(\frac{M}{\ell} - 2\Big)x - (2C - M) \geq 10M - 3M > 0.$$

Also $D > d$, since $x \geq M(d-2) > \ell d$. Equation (21) yields $\sum_v z_v = \ell G$, and Lemma 6.1 supplies G subsets of ℓ distinct messages with these degrees. Assign them to the generic blocks; each is injective on V, so its subset gives ℓ distinct symbols capturing exactly that subset. Every message now has $mh_v + z_v = m(\ell D + C)/M$ agreements. □

The displayed estimate uses D only through $\ell D \geq Md - C$, so it holds for every real $D \geq (Md - C)/\ell$.

Corollary 6.3 (The defect-free case)**.** *Let $D \geq (Md - C)/\ell$ be an integer and let R be rational with $1/D < R < C/(BD)$. For every integer $s \geq d$ there are arbitrarily large prime powers q and consecutive full-length s-folded Reed–Solomon codes of rate exactly R, with $q = sn + 1$ and $(k-1)/s \geq a$, containing M distinct messages and a table of exactly ℓ symbols per block against which every message has error exactly $1 - \tau_D < \Phi_{\ell,a}(R)$.*

Proof. Let $R = \nu/\omega$ in lowest terms. Pick a prime $\pi \nmid DsM\omega$ and put $q = \pi^{\varphi(DsM\omega)\lambda}$; Euler's theorem gives $DsM\omega \mid q - 1$, and $q \geq \ell$ for large λ. Then $m = (q-1)/(Ds)$ is divisible by M and ω, so $k = Rsn$ is an integer, $k > sm$ since $RD > 1$, and $k < sn$. By Proposition 6.2 all M messages have error $1 - \tau_D$, and $\Phi_{\ell,a}(R) - (1 - \tau_D) = \frac{1}{M}(\frac{C}{D} - BR) > 0$. As $\lambda \to \infty$, $m \to \infty$ and $(k-1)/s > m - 1/s \to \infty$. □

Proposition 6.4 (Comparison with the optimal radius)**.** *For every rational R with $0 < R \leq 1/(Md-1)$, the codes of Proposition 6.2 at rate exactly R, with $D = \lfloor 1/R \rfloor + 1$ and the field choice of Corollary 6.3, contain M messages each of error exactly*

$$1 - \frac{\ell}{M} - \frac{C}{M(\lfloor 1/R \rfloor + 1)} \leq 1 - \frac{\ell}{M} - \frac{C}{M} \cdot \frac{R}{1+R}.$$

Compared with the optimal large-alphabet radius $(L + 1 - \ell - LR)/(L+1)$ of [3], with $L + 1 = M$, this error is smaller by at least $(C/(1+R) - (M-1))R/M > 0$.

Proof. With $D = \lfloor 1/R \rfloor + 1$ we have $RD > 1$ and $D \geq Md$, so Proposition 6.2 applies, with agreement fraction $(\ell D+C)/(MD)$ and $1/D \geq R/(1+R)$. Positivity follows from $C/(M-1) > 1+R$: by (11), $C/(M-1) \geq 4/3 - 1/(3(M-1)) \geq 4/3 - 1/45$ for $\ell = 2$, and for $\ell \geq 3$ the main term is at least $3/2$ and the subtracted term at most $(\ell-1)^2/((\ell+1)(\ell^3-1)) < 1/6$; while $Md \geq 160$ gives $R \leq 1/159$. □

As $R \to 0$ the conjectured curve, this construction and the optimal radius have slopes B/M, C/M and $(M-1)/M$. The ratio $C/(M-1) = 2\ell/(\ell+1) - c(\ell-1)^2/((\ell+1)(M-1))$ tends to $2\ell/(\ell+1)$, whereas the hypercube ratio $B/(M-1)$ tends to one.

6.2 Block surjectivity

The proof of Proposition 6.2 uses the code only through d independent codewords, equally many special blocks of each type with kernel exactly $\mathbb{F}_q p_i$ on their span, and further blocks injective on it. An *$\mathbb{F}_q$-linear code* of length n over $\mathbb{F}_q^s$ is an $\mathbb{F}_q$-subspace $\mathcal{C} \subseteq (\mathbb{F}_q^s)^n$, of rate $\dim_{\mathbb{F}_q} \mathcal{C}/(sn)$; $c_r \in \mathbb{F}_q^s$ denotes block r of a codeword c, and tables, errors and list recovery are defined as for messages.

Definition 6.5 (Block surjectivity)**.** Let $z \geq 1$ with $dz \leq n$, and fix pairwise disjoint sets $Z_0, \ldots, Z_{d-1} \subseteq \{0, \ldots, n-1\}$ of z blocks each. The code $\mathcal{C}$ has property BS_z if, for every $i < d$ and every block $r \notin Z_i$, the projection of $\mathcal{C}$ onto the blocks $Z_i \cup \{r\}$ is onto $(\mathbb{F}_q^s)^{Z_i \cup \{r\}}$. A block in none of the Z_i is *generic*.

Lemma 6.6 (Planted kernels)**.** *Let $\mathcal{C}$ have BS_z with respect to $Z_0, \ldots, Z_{d-1}$ and put $\mathcal{C}_i = \{c \in \mathcal{C} : c_r = 0 \text{ for } r \in Z_i\}$. There are $p_i \in \mathcal{C}_i$ and a set $\mathcal{B}$ of fewer than $q^{d-s}n$ bad blocks such that, whenever $n - dz \geq q^{d-s}n$, the codewords $p_0, \ldots, p_{d-1}$ are independent, and on their span V the map $c \mapsto c_r$ has kernel $\mathbb{F}_q p_i$ at every $r \in Z_i \setminus \mathcal{B}$ and kernel $\{0\}$ at every generic $r \notin \mathcal{B}$.*

Proof. Choose p_i uniformly from $\mathcal{C}_i$, independently. For $r \notin Z_i$ the map $\mathcal{C}_i \to \mathbb{F}_q^s$, $c \mapsto c_r$, is onto by BS_z, so $(p_i)_r$ is uniform. Fix r and let $J_r = \{j < d : r \notin Z_j\}$; then $|J_r| \geq d-1$ and $(p_i)_r = 0$ for the at most one $i \notin J_r$. The vectors $(p_j)_r$, $j \in J_r$, are independent and uniform; call r bad if they are linearly dependent. Adding them one at a time,

$$\Pr[r \text{ bad}] \leq \sum_{u=1}^{|J_r|} q^{u-1-s} = \frac{q^{|J_r|}-1}{(q-1)q^s} < q^{d-s}.$$

Fix an outcome with $|\mathcal{B}| < q^{d-s}n$. The coefficient map $\phi_r(c) = \sum_j c_j (p_j)_r$ has kernel $\mathbb{F}_q e_i$ at $r \in Z_i \setminus \mathcal{B}$ and kernel zero at a good generic block. If $n - dz \geq q^{d-s}n$, a good generic block exists, so the p_j are independent and the kernels of ϕ_r are the asserted kernels on V. □

Put $\tau(\xi) = (\ell + C\xi)/M$, so that $\tau(1/D) = \tau_D$.

Theorem 6.7 (Squares under block surjectivity)**.** *Let $q \geq \ell$, $s \geq 1$, and let $\mathcal{C} \subseteq (\mathbb{F}_q^s)^n$ be $\mathbb{F}_q$-linear with BS_z. Put $\xi = z/n$ and $\eta = q^{d-s}$, and suppose*

$$(Md - C)\xi + \ell\eta + \frac{M}{n} \leq \ell, \tag{22}$$

$$(Md + C - M)\xi + (M-\ell)\eta + \frac{M}{n} \leq M - \ell. \tag{23}$$

Then $\mathcal{C}$ contains M distinct codewords and a table with exactly ℓ symbols per block such that each codeword has error less than $1 - \tau(\xi) + (\ell d + C)\eta/M + 1/n$.

Proof. By (21), $\sum_v h_v = \ell d + C$ with every $h_v \geq 1$ and $h_0 = d > 1$, so $\ell d + C > M$; and $Md - C > \ell d$, as shown in the proof of Proposition 6.2. Since $(Md + C - M)\xi = (M - \ell)d\xi + (\ell d + C - M)\xi$, condition (23) gives $(M - \ell)(1 - d\xi - \eta) > 0$, that is $n - dz > \eta n$, and Lemma 6.6 supplies $p_0, \ldots, p_{d-1}$, their span V of dimension d, and $b < \eta n$ bad blocks.

Blocks. Let b_0, b_1 count the bad generic and bad special blocks. Put $m' = \min_i |Z_i \setminus \mathcal{B}| \geq z - b_1$, choose $Z_i' \subseteq Z_i \setminus \mathcal{B}$ of size m', and let W be the set of good generic blocks, $G' = |W| = n - dz - b_0$. All other blocks are discarded; a surplus good special block has kernel $\mathbb{F}_q p_i$ on V and cannot carry padding. Then

$$\ell G' + (\ell d + C)m' \geq \ell n + Cz - (\ell d + C)b. \tag{24}$$

Special blocks. Form $S \subseteq V$ and the special tables of Proposition 6.2 on the blocks Z_i'; those arguments use only independence and the kernels $\mathbb{F}_q p_i$. Codeword v has exactly $m' h_v$ agreements on $\bigcup_i Z_i'$.

Deficits. Put $T = \lfloor (\ell G' + (\ell d + C)m')/M \rfloor$ and $z_v = T - m' h_v$. Using $m' \leq z$ and $G' \geq n - dz - b$,

$$\ell G' - (Md - \ell d - C)m' \geq \ell n - (Md - C)z - \ell b > n\big(\ell - (Md - C)\xi - \ell\eta\big) \geq M$$

by (22), so $T \geq m'd + 1$ and $z_v > 0$. Similarly

$$(M - \ell)G' - (\ell d + C - M)m' > n\big(M - \ell - (Md + C - M)\xi - (M - \ell)\eta\big) \geq M$$

by (23), so $T < G' - 1 + m'$ and $z_v \leq T - m' \leq G' - 1$. The shortfall $\sigma = \ell G' - \sum_v z_v$ is an integer in $[0, M)$; increase z_v by one for σ distinct codewords. The new degrees lie in $[0, G']$ and sum to $\ell G'$.

Padding. Lemma 6.1 supplies G' subsets of size ℓ with these degrees; assign them to W, where each block is injective on V. At every discarded block use any ℓ distinct symbols.

Errors. Every $v \in S$ has at least T agreements, and by (24) and $b < \eta n$, $T > n\tau(\xi) - (\ell d + C)\eta n/M - 1$. □

Lemma 6.8 (Margins)**.** *Put $\xi_1 = \ell/(Md - C)$. For $0 \leq \xi \leq \xi_1$, $\mu_-(\xi) = \ell - (Md - C)\xi \geq 0$ and $\mu_+(\xi) = (M - \ell) - (Md + C - M)\xi > 0$, with $\mu_-(\xi) > 0$ for $\xi < \xi_1$. Moreover $d\xi_1 < 1$.*

Proof. The claims on μ_- are immediate, and $d\xi_1 < 1$ follows from $Md - C > \ell d$. The function μ_+ is linear with $\mu_+(0) > 0$, and with $D_1 = 1/\xi_1$, $\mu_+(\xi_1) = \xi_1\big((M - \ell)D_1 - (Md + C - M)\big) \geq 7M\xi_1 > 0$ by the estimate in the proof of Proposition 6.2. □

Proposition 6.9 (Folded Reed–Solomon codes have block surjectivity)**.** *Let $\mathcal{C}$ be an s-folded Reed–Solomon code of length n and dimension $k < sn$ with appropriate evaluation points. If $z \geq 1$, $dz \leq n$ and $s(z + 1) \leq k$, then $\mathcal{C}$ has BS_z with respect to every family of pairwise disjoint sets $Z_0, \ldots, Z_{d-1}$ of z blocks.*

Proof. The blocks $Z_i \cup \{r\}$ carry $s(z + 1)$ distinct unfolded points, and Lagrange interpolation provides a polynomial of degree less than $s(z + 1) \leq k$ with any prescribed values there. □

Proof of Theorem 1.5. Let $R \in (0, R_0^*)$ be rational. Since $C > B$, $BR/C < R$, and $R < R_0^*$ is equivalent to $BR/C < \xi_1$. Fix a rational ξ_* with $BR/C < \xi_* < \min\{R, \xi_1\}$, depending on (ℓ, a, R), and put $\varepsilon = (C\xi_* - BR)/(3M) > 0$. By (3), $1 - \tau(\xi_*) = \Phi_{\ell,a}(R) - 3\varepsilon$, and by Lemma 6.8, $\mu_\pm = \mu_\pm(\xi_*) > 0$. Let n_0 be the least integer exceeding

$$\ell, \quad \frac{1}{\xi_*}, \quad \frac{1}{R - \xi_*}, \quad \frac{a + 1}{R}, \quad \frac{\ell + M}{\mu_-}, \quad \frac{2M - \ell}{\mu_+}, \quad \frac{2C + \ell d + M}{M\varepsilon}.$$

Let $s \geq d+1$, $n \geq n_0$ and $k = Rsn$. The sn unfolded points are distinct, so $q \geq sn \geq n \geq \ell$ and $\eta = q^{d-s} \leq 1/n$. Put $z = \lfloor \xi_* n \rfloor$ and $\xi = z/n \in (\xi_* - 1/n, \xi_*]$. Then $z \geq 1$, $dz \leq n$, and $s(z+1) \leq s(\xi_* n + 1) \leq Rsn = k$ because $n(R - \xi_*) \geq 1$. Take $Z_i = \{iz, \dots, iz + z - 1\}$; Proposition 6.9 gives BS_z. The left side of (22) is at most $\ell - \mu_- + (\ell + M)/n \leq \ell$, and that of (23) at most $M - \ell - \mu_+ + (2M - \ell)/n \leq M - \ell$. Theorem 6.7 gives M distinct messages and a table of exactly ℓ symbols per block with errors less than

$$1 - \tau(\xi_*) + \frac{C}{Mn} + \frac{\ell d + C}{Mn} + \frac{1}{n} = \Phi_{\ell,a}(R) - 3\varepsilon + \frac{2C + \ell d + M}{Mn} < \Phi_{\ell,a}(R) - 2\varepsilon.$$

Moreover $(k-1)/s = Rn - 1/s \geq a$ because $Rn \geq a+1$, and $R < R_0^* < 2\ell/(5B) \leq 2/15 < (a-1)/a$ by (11), $Md - C \geq 5M$ and $B \geq M - \ell \geq 3\ell$. For every s and n with $Rsn \in \mathbb{Z}$, every prime power $q > sn$ and the points $\alpha_r = \gamma^{sr}$ give an appropriate code. Finally $(C, B, Md - C) = (20, 56/3, 140)$ and $(38, 36, 151)$ give $R_0^*(2,4) = 3/196$ and $R_0^*(3,3) = 19/906$. □

6.3 Random linear codes

Following [2], a uniformly random $\mathbb{F}_q$-linear code of rate $R = k/(sn)$ over $\mathbb{F}_q^s$ is the row space of a uniformly random $k \times sn$ matrix Γ over $\mathbb{F}_q$, whose columns are grouped into n consecutive blocks of s; the lengths run over n with $Rsn \in \mathbb{Z}$. Full rank holds with probability $1 - o(1)$, and conditioned on it the row space is a uniformly random k-dimensional subspace, so the statement holds equally for that model.

Proof of Theorem 1.6. Choose ξ_*, ε and $\mu_\pm > 0$ as in the proof of Theorem 1.5. Let $s_0 \geq d+1$ be the least integer for which $\eta_0 = q^{d-s_0}$ satisfies $\ell\eta_0 \leq \mu_-/2$, $(M - \ell)\eta_0 \leq \mu_+/2$ and $(\ell d + C)\eta_0/M \leq \varepsilon/2$. Fix $s \geq s_0$, so $\eta = q^{d-s} \leq \eta_0$, let $k = Rsn$, $z = \lfloor \xi_* n \rfloor$, $w = s(z+1)$ and $Z_i = \{iz, \dots, iz + z - 1\}$.

Full rank. The jth row of Γ lies in the span of the earlier ones with probability at most q^{j-1-sn}, so $\Pr[\operatorname{rank}\Gamma < k] < q^{k-sn}/(q-1) \to 0$.

Block surjectivity. The projection onto $Z_i \cup \{r\}$ is onto exactly when the $k \times w$ submatrix on those columns has rank w. Here $w - k \leq s - sn(R - \xi_*) < 0$ for large n, and the w columns are independent uniform vectors in $\mathbb{F}_q^k$, so this submatrix is rank deficient with probability less than $q^{w-k}/(q-1)$. A union bound over the at most dn pairs (i, r) gives $\Pr[\mathrm{BS}_z \text{ fails}] < dn\, q^{s - sn(R - \xi_*)} \to 0$.

Conclusion. With probability $1 - o(1)$ the code has rate exactly R and BS_z. For $n \geq 2M/\mu_\pm$, the left sides of (22) and (23) are at most ℓ and $M - \ell$, and Theorem 6.7 gives M distinct codewords and a table of exactly ℓ symbols per block with errors less than

$$1 - \tau(\xi_*) + \frac{C}{Mn} + \frac{\varepsilon}{2} + \frac{1}{n} = \Phi_{\ell,a}(R) - \frac{5\varepsilon}{2} + \frac{C + M}{Mn} < \Phi_{\ell,a}(R) - \varepsilon$$

for large n. □

Remark 6.10 (Unfolded codes). The row space of Γ, read over the alphabet $\mathbb{F}_q$ with length sn, is a uniformly random $\mathbb{F}_q$-linear code of rate R. A folded table with ℓ symbols per block induces an unfolded table with at most ℓ values per coordinate, and unfolded errors are at most folded errors. With $s = s_0$, Theorem 1.6 therefore gives the same conclusion for uniformly random $\mathbb{F}_q$-linear codes over $\mathbb{F}_q$ itself, along lengths divisible by s_0, for every fixed prime power $q \geq \ell$.

Remark 6.11 (The black-box route). For large fields, $q = \Theta(sn)$, failure for random linear codes also follows from Theorem 1.5 through known transfer theorems. Brakensiek, Chen, Dhar and Zhang [2, Theorems 1.4 and 3.1] show that if random $\mathbb{F}_q$-linear codes of rate R avoid a b-local profile with high probability, then explicit folded Reed–Solomon codes with $q = \Theta(sn)$, $s \geq b(R/\varepsilon' + 1)$ and

rate $R-\varepsilon'$ avoid it as well; list recovery with output cap L corresponds to a family of local profiles on $L+1$ codewords [2]. Applied in contrapositive form to Theorem 1.5, which covers their explicit codes since it holds for all appropriate points, this shows that random linear codes of slightly larger rate contain the configurations with non-vanishing probability, and the sharp-threshold theorem of Levi, Mosheiff and Shagrithaya [11, Theorem 4.4], quoted as [2, Theorem 2.4], upgrades this to high probability at rates slightly above. Theorems 6.7 and 1.6 give a self-contained proof, valid for every code with block surjectivity, for fields of every size $q \geq \ell$, with the explicit threshold R_0^* and explicit slack.

6.4 An explicit cap-fifteen instance

Theorem 6.12. *For every integer $s \geq 10$ there are arbitrarily long consecutive full-length folded Reed–Solomon codes of exact rate $1/79$ and tables of exactly two symbols per block for which sixteen distinct messages each have relative error $55/64$. Since $\Phi_{2,4}(1/79) - 55/64 = 13/15168 > 1/10000$, these codes are not $(55/64 + 1/10000, 2, 15)$ list recoverable.*

Proof. Apply Lemma 5.3 with $D = 80$, $d = 10$ and m divisible by $84 \cdot 79$; set $n = 80m$, $k = 80sm/79$ and $V = \operatorname{span}\{p_0, \dots, p_9\}$. Then $k - sm = sm/79 \geq 1$ and $k/(sn) = 1/79$. Use the sixteen messages $S = \{0\} \cup \bigcup_{h=0}^{4} \{p_{2h}, p_{2h+1}, p_{2h} + p_{2h+1}\}$. At a block $r = i + 80j$ with $i < 10$ and partner i', the table $\{0, E_r(p_{i'})\}$ has fibers exactly $\{0, p_i\}$ and $\{p_{i'}, p_i + p_{i'}\}$. Thus the origin agrees at all $10m$ special blocks and each other message at $2m$. The remaining $70m$ blocks are injective on V; assign unordered pairs with multiplicity $m/12$ to each of the 15 pairs containing the origin and $55m/84$ to each of the 105 other pairs. These are integers, and $15m/12 + 105 \cdot 55m/84 = 70m$. The origin gains $5m/4$ and each other message $m/12 + 14 \cdot 55m/84 = 37m/4$, so every message has $45m/4$ agreements out of $80m$, an error of $55/64$. For the field, fix $s \geq 10$, put $H = 80s \cdot 84 \cdot 79$, choose a prime $\pi \nmid H$ and take $q = \pi^{\varphi(H)\lambda}$; then $m = (q-1)/(80s)$ is divisible by $84 \cdot 79$, the lengths tend to infinity with λ, and $(k-1)/s \geq 4$ for large length. Finally $\Phi_{2,4}(1/79) - 55/64 = \frac{7}{8} - \frac{7}{6 \cdot 79} - \frac{55}{64} = \frac{13}{15168}$. □

In the rate-slack form, $R^*(\rho) = \frac{3}{4}(1 - \frac{8\rho}{7})$ and $R^*(55/64 + 1/10000) - 1/79 = \frac{6}{7}(\frac{13}{15168} - \frac{1}{10000}) > \frac{1}{10000}$.

7 Scope

The results decide Conjecture 1.1 for input-list size two and for every exponent $a \geq 3$: it holds at $(\ell, a) = (2, 2)$ and $(2, 3)$ at every rate, and every other case fails, with explicit failing rates filling $(0, R_0^*(\ell, a))$. The conjecture holds at $(\ell, a) = (2, 2)$ [5] and at $(\ell, a) = (2, 3)$ (Corollary 1.4), in the average-radius form and for every set of appropriate evaluation points, with exact radius $\Phi_{2,3}$ (Proposition 4.4); the same average-radius $(\rho, 2, 7)$ theorem holds for univariate multiplicity codes in characteristic at least k (Proposition 4.7). It fails for $(2, a)$ with $a \geq 4$ and for (ℓ, a) with $\ell, a \geq 3$ at every rate in $(0, R_0^*(\ell, a))$, in every folded Reed–Solomon code with appropriate points, folding $s \geq d + 1$ and length $n \geq n_0$, and with high probability in random linear codes over every field with at least ℓ elements. The average-radius form fails for $a \geq 4$ at every rate in $(0, 2/B(2, a))$ in every linear code. In the linear-programming language of Section 2, the hypercube pattern has value exactly B, the eight-point theorem shows that $B(2, 3) = 9$ is also the largest certificate cost of eight points, and the squares patterns exceed B exactly on the region (5) and equal B at $a = 2$ and at $(\ell, a) = (2, 3)$.

Software and data

The package accompanying this paper contains: `verify_certificates.py` with its expected output `certificate_checks.json`, which reproduces the finite-folding and multiplicity profiles of Section 4 in exact rational arithmetic (`python verify_certificates.py --check`); the explicit certificates `q541_explicit_certificate.json` and `q2161_fixed_rate_certificate.json` of Section 5 with `validate_frs_certificate.py`; and `check_square_padding_frs.py`, which carries out the proof of Theorem 6.7 step by step on explicit folded Reed–Solomon codes from raw polynomial evaluations. For example, at $(\ell, a) = (3, 3)$, $s = 8$, $n = 1377$, $z = 27$ and $k = 226$, over $q = 11027$ with consecutive points and over $q = 33049$ with random appropriate points, conditions (22) and (23) hold and all 27 codewords have error 1186/1377, below $\Phi_{3,3}(k/(sn))$. The proofs in this paper are analytic; the programs check the displayed finite arithmetic and examples.

Statements

Prior versions. This paper merges and supersedes three records of the Luminary Research Archive by the author: *Eight-point fiber certificates and binary-input list recovery of folded Reed–Solomon codes*, edition 3 [13]; *Counterexamples to the fine-grained list-recovery conjecture for folded Reed–Solomon and random linear codes*, edition 2 [14]; and *Independent squares and average-radius obstructions for linear codes*, edition 2 [15].

AI assistance. OpenAI Codex and Anthropic Claude assisted with research exploration, literature retrieval, proof development and checking, computation, and manuscript preparation under the author's direction. The author is responsible for the mathematical content and its attribution.

Funding and interests. This research was self-funded. The author owns Luminary Oddities and its Research Archive.

References

[1] J. Brakensiek, Y. Chen, M. Dhar and Z. Zhang, *Combinatorial bounds for list recovery via discrete Brascamp–Lieb inequalities*, Proceedings of STOC 2026, pp. 365–376, `https://doi.org/10.1145/3798129.3800756`. Full version: arXiv:2510.13775v2, October 11, 2026, `https://arxiv.org/abs/2510.13775v2`.

[2] J. Brakensiek, Y. Chen, M. Dhar and Z. Zhang, *From random to explicit via subspace designs with applications to local properties and matroids*, Proceedings of STOC 2026, pp. 619–630, `https://doi.org/10.1145/3798129.3800778`. arXiv:2510.13777v1, October 15, 2025, `https://arxiv.org/abs/2510.13777v1`.

[3] J. Brakensiek, Y. Chen, A. Putterman and Z. Zhang, *Bounds and limitations on codes achieving list recovery capacity*, full version of the SODA 2027 extended abstract, arXiv:2607.19576v2, October 9, 2026, `https://arxiv.org/abs/2607.19576v2`.

[4] Y. Chen, M. Cheraghchi, K.-S. Si and Z. Zhang, *Evidence toward a conjecture in list recoverability of folded Reed–Solomon codes*, manuscript, 2025, as reported in [1, Section 1].

[5] Y. Chen and Z. Zhang, *Explicit folded Reed–Solomon and multiplicity codes achieve relaxed generalized Singleton bounds*, Proceedings of STOC 2025, pp. 1–12, https://doi.org/10.1145/3717823.3718114. Full version: arXiv:2408.15925v3, April 14, 2025, https://arxiv.org/abs/2408.15925v3.

[6] R. Goyal and V. Guruswami, *Structure theorems (and fast algorithms) for list recovery of subspace-design codes*, arXiv:2512.08017v1, 2025, https://arxiv.org/abs/2512.08017v1.

[7] R. Goyal and V. Guruswami, *Improved analysis of list-decodability of random linear codes: it's all about counting constraints*, Electronic Colloquium on Computational Complexity, Report TR26-074, May 12, 2026, https://eccc.weizmann.ac.il/report/2026/074/.

[8] R. Goyal, V. Guruswami, Y. Sun and M. Wootters, *Improved LCL equivalences and curve decoding alphabet sizes*, arXiv:2610.38862v1, October 28, 2026, https://arxiv.org/abs/2610.38862v1.

[9] V. Guruswami and S. Kopparty, *Explicit subspace designs*, Combinatorica 36 (2016), 161–185, https://doi.org/10.1007/s00493-014-3169-1.

[10] V. Guruswami and A. Rudra, *Explicit codes achieving list decoding capacity: error-correction with optimal redundancy*, IEEE Transactions on Information Theory 54 (2008), 135–150.

[11] M. Levi, J. Mosheiff and N. Shagrithaya, *Random Reed–Solomon codes and random linear codes are locally equivalent*, arXiv:2406.02238v7, November 14, 2025, https://arxiv.org/abs/2406.02238v7.

[12] R. Li and N. Shagrithaya, *Near-optimal list-recovery of linear code families*, APPROX/RANDOM 2025, LIPIcs 353, 53:1–53:14, https://doi.org/10.4230/LIPIcs.APPROX/RANDOM.2025.53.

[13] S. Schubr, *Eight-point fiber certificates and binary-input list recovery of folded Reed–Solomon codes*, Luminary Research Archive, edition 3, 2026-11-01, https://research.luminaryoddities.org/eight-point-fiber-certificates-binary-input-list-recovery-folded-reed-solomon-codes/v/3.

[14] S. Schubr, *Counterexamples to the fine-grained list-recovery conjecture for folded Reed–Solomon and random linear codes*, Luminary Research Archive, edition 2, 2026-11-16, https://research.luminaryoddities.org/counterexamples-fine-grained-list-recovery-conjecture-folded-reed-solomon-codes/v/2.

[15] S. Schubr, *Independent squares and average-radius obstructions for linear codes*, Luminary Research Archive, edition 2, 2026-10-27, https://research.luminaryoddities.org/independent-squares-average-radius-obstructions-linear-codes/v/2.