Eight-point fiber certificates and binary-input list recovery of folded Reed–Solomon codes

Scott Schubr
Luminary Oddities

November 26, 2026 (edition 5)

Abstract

Chen and Zhang proved that folded Reed–Solomon codes with input lists of size ℓ and output cap L cannot be list recovered beyond a radius given by a hypercube of messages, and conjectured that this radius is attained when $L+1$ is a power of ℓ. Brakensiek, Chen, Dhar and Zhang ask in general for the optimal trade-off among radius, rate and list sizes. For input lists of size two and output caps $L = 2, \dots, 7$ we determine the exact radius: it is $1 - (2 + \kappa_L R)/(L+1)$, with $\kappa_L = 2, 4, 5, 6, 8, 9$, at every rate for $L \in \{2, 3, 5, 7\}$, at rates up to $3/10$ for $L = 4$, and up to $1/10$ for $L = 6$. Codes with any appropriate evaluation points and large folding attain this radius in the average-radius sense, and no such code of large length exceeds it. Hence, for input lists of size two, the Chen–Zhang bound is exact precisely for $L \in \{2, 3, 5, 7\}$: for $L = 4$, $L = 6$ and every $L \geq 8$ the codes fail at a strictly smaller radius at all small rates. The positive direction bounds a certificate of nonnegative subspace weights, controlling the two largest fibers of every linear quotient, for every set of at most eight messages over every field. The negative direction plants coordinate kernels by interpolation and equalizes the errors by pairing schedules.

Keywords. list recovery; folded Reed–Solomon codes; subspace designs; Chen–Zhang bound; generalized Singleton bound; fiber certificates.
MSC 2020. Primary 94B35; Secondary 94B65, 05B35, 15A03.

1 Introduction

A list-recovery input specifies a set of allowed symbols at each coordinate of a code. The objective is to bound the number of codewords that disagree with these sets on at most a prescribed fraction of coordinates. We consider folded Reed–Solomon codes and input sets of size at most two, and we determine the largest radius at which such codes are list recoverable with output cap L for every $L \leq 7$, at all rates for $L = 2, 3, 5, 7$ and at small rates for $L = 4, 6$. This edition adds the output caps two to six, the exact radii at the caps two to seven and the classification of the caps at which the Chen–Zhang bound is tight (Theorems 1.5, 1.7 and 1.8, Sections 6–8), and proves the cap-seven theorem of edition 4 for all appropriate evaluation points.

1.1 Folded Reed–Solomon codes and the question

Let q be a prime power and let γ generate $\mathbb{F}_q^\times$. For integers $s, n, k \geq 1$ and $\alpha_0, \dots, \alpha_{n-1} \in \mathbb{F}_q$, the s-folded Reed–Solomon code [9] encodes $f \in \mathcal{P}_k = \{f \in \mathbb{F}_q[X] : \deg f < k\}$ by the blocks

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

Following Chen and Zhang [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 all $\alpha_j \ne 0$, hence $sn \le q-1$. The *consecutive* points $\alpha_j = \gamma^{js}$ with $sn \le q-1$ are appropriate. For $k \le sn$ the encoding is injective and the rate is $R = k/(sn)$.

A *table* is a sequence $A = (A_0, \dots, A_{n-1})$ of sets $A_j \subseteq \mathbb{F}_q^s$ with $|A_j| \le 2$; *binary input* refers to this size two, not to the field. The error of a message is $\mathrm{err}_A(f) = |\{j : E_j(f) \notin A_j\}|/n$. The code is $(\rho, 2, L)$ *list recoverable* if for every table at most L messages have error at most ρ. It is *average-radius* $(\rho, 2, L)$ list recoverable if every $L+1$ distinct messages have mean error greater than ρ against every table. The average-radius property implies the ordinary one.

Chen and Zhang proved the following upper bound for every input-list size.

Theorem 1.1 (Chen–Zhang [5, Theorem 3.1])**.** *Let $s \ge 1$, $2 \le \ell \le L$, $q \ge \ell$, and $\mu = \lceil \log_\ell(L+1) \rceil > 1$. Suppose $(k-1)/(sn) \le (\mu-1)/\mu$ and $(k-1)/((\mu-1)s) \ge 1$. If an s-folded Reed–Solomon code with appropriate evaluation points is (ρ, ℓ, L) list recoverable, then*

$$\rho \le \frac{L+1-\ell}{L+1}\Big(1 - \Big\lfloor \frac{\mu}{\mu-1} \Big\lfloor \frac{k-1}{s} \Big\rfloor \Big\rfloor \frac{1}{n}\Big).$$

For $\ell = 2$ and $L \ge 2$ put $\mu = \mu_L = \lceil \log_2(L+1) \rceil$ and

$$\Phi_L(R) = \frac{L-1}{L+1}\Big(1 - \frac{\mu R}{\mu-1}\Big) = 1 - \frac{2 + B_L R}{L+1}, \qquad B_L = \frac{(L-1)\mu}{\mu-1}. \tag{2}$$

Theorem 1.1 says that, up to $O(1/n)$, no rate-R folded Reed–Solomon code with appropriate points is list recoverable beyond $\Phi_L(R)$ [5, Theorem 1.7]. Chen and Zhang conjectured that this bound is almost tight when $L+1$ is a power of ℓ [5, Conjecture 3.6], in the sense that radius $\Phi_L(R) - \varepsilon$ is attained for large folding and length, and proved the case $\ell = 2$, $L = 3$ [5, Theorem 1.8]. They ask whether the conjecture holds and, if it fails, what the correct tight bound is [5, Section 4, item 2]; this question concerns the powers $L + 1 = \ell^a$. The previous edition of this article proved the case $\ell = 2$, $L = 7$ for consecutive points (Theorem 1.6 below). Brakensiek, Chen, Dhar and Zhang proved the zero-error case $\rho = 0$ at the powers $L + 1 = \ell^a$ [1, Theorem 1.6] and pose the general question.

Question 1.2 ([1, Section 1.3, Open Question 1])**.** *Beyond the zero-error regime and the case $(\ell, L) = (2, 3)$, what is the optimal trade-off among the radius ρ, the rate R, the input-list size ℓ and the output cap L for list recovery of folded Reed–Solomon codes?*

For $\ell = 2$, Chen and Zhang's question at the powers $L+1 = 4$ and 8 is settled by [5, Theorem 1.8] and by Theorem 1.7 at $L = 7$, and at the powers $L + 1 = 2^a \ge 16$ their bound is not attained (Theorem 1.8(b)). This article answers Question 1.2 for $\ell = 2$ at the caps $L \in \{2, 4, 5, 6\}$ as well: at every rate for $L \in \{2, 5\}$, at every rate $R \le 3/10$ for $L = 4$, and at every rate $R \le 1/10$ for $L = 6$. Together with $L \in \{3, 7\}$ this gives the exact radius for every $L \le 7$ on these ranges of rates. Theorem 1.1 supplies the Chen–Zhang bound at every cap, so comparing it with the exact radii extends Chen and Zhang's tightness question to the caps that are not powers; Theorem 1.8 decides it for $\ell = 2$ and every $L \ge 2$.

1.2 Fiber certificates

Consider M candidate messages as points in the vector space $\mathcal{P}_k$. At a fixed folded coordinate, evaluation is linear. Its kernel partitions the messages into fibers, one for each folded symbol, and a table allowing two symbols can capture at most the total population of the two largest fibers.

It remains to control these populations simultaneously at all coordinates. A bound chosen separately for each coordinate need not interact with the global polynomial rank budget. We instead attach to the message configuration a fixed collection of nonnegative subspace weights. The same weights then apply to every evaluation kernel. Summing the resulting inequalities reduces the agreement count to the established folded-Wronskian bounds for intersections with these subspaces.

Here is the geometric statement. Let S be a finite set of distinct points over a field, and let $V = \mathrm{dir}(S)$ be the span of its pairwise differences. For $K \le V$, write $b_2(S/K)$ for the sum of the two largest populations of affine K-cosets meeting S; the second population is zero if there is only one such coset.

Definition 1.3. A certificate for S is a finite family of subspaces $W \le V$ and rational weights $y_W \ge 0$ such that

$$b_2(S/K) \le 2 + \sum_W y_W \dim(K \cap W) \qquad (K \le V). \tag{3}$$

Its cost is $\sum_W y_W \dim W$. The family and weights may depend on S, but are fixed independently of K. Let $\mathcal{C}(S)$ be the infimum of these costs, and for $M \ge 3$ let $\mathcal{C}_M$ be the supremum of $\mathcal{C}(S)$ over all sets S of M distinct points in vector spaces over arbitrary fields.

Theorem 1.4 (Eight-point certificate)**.** *Every set of eight distinct points over any field has a certificate of cost at most nine. For affine dimensions $1, \dots, 7$, respectively, sufficient costs are*

$$6, \quad 8, \quad 9, \quad 9, \quad 9, \quad 8, \quad 7.$$

For the Boolean three-cube, $\mathcal{C}(S) = 9$.

The same method determines $\mathcal{C}_M$ for every smaller M. A *square* is a set $\{0, x, y, x+y\}$ with x, y linearly independent; it is an affine parallelogram in every characteristic.

Theorem 1.5 (Certificates of at most eight points)**.** *For every $M \in \{3, \dots, 8\}$ and every set of M distinct points over any field there is a certificate of cost at most κ_{M-1}, where*

$$(\kappa_2, \kappa_3, \kappa_4, \kappa_5, \kappa_6, \kappa_7) = (2, 4, 5, 6, 8, 9).$$

These costs are attained over every field: for $M = 3, \dots, 8$ respectively by three affinely independent points, a square, a square with one further independent direction, a square with two further independent directions, two squares sharing a vertex and spanning four dimensions, and the Boolean three-cube. Thus $\mathcal{C}_{L+1} = \kappa_L$ for $2 \le L \le 7$.

1.3 Coding results

The certificate costs translate into list-recovery radii through the folded-Wronskian budget. In the consecutive model the cap-seven statement reads as follows.

Theorem 1.6 (Binary-input list recovery)**.** *Let $n \ge 1$, $s \ge 7$, and $1 \le k \le sn$ be integers. Let $q > sn$ be a prime power and γ a generator of $\mathbb{F}_q^\times$. Encode each polynomial $f \in \mathbb{F}_q[X]$ of degree less than k as*

$$\mathrm{Enc}(f)_j = (f(\gamma^{js}), \dots, f(\gamma^{js+s-1})), \qquad 0 \le j < n.$$

If $0 \le \rho < 3/4$ and

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

then this code is average-radius $(\rho, 2, 7)$ list recoverable.

Proposition 2.2 proves the same statement for every set of appropriate evaluation points and every cap $L \le 7$. For $2 \le L \le 7$ put

$$\rho_L(R) = 1 - \frac{2 + \kappa_L R}{L+1}. \tag{5}$$

Theorem 1.7 (Exact radii at caps two to seven)**.** *Let $2 \le L \le 7$ and $\mu = \lceil \log_2(L+1) \rceil$. Consider s-folded Reed–Solomon codes of rate R and length n with appropriate evaluation points, over any field and for any generator.*

(a) For every $\varepsilon > 0$ and $0 < R \le (L-1)/\kappa_L$, every such code with $s \ge L + \lceil (L-1)^2/((L+1)\varepsilon) \rceil$ is average-radius $(\rho_L(R) - \varepsilon, 2, L)$ list recoverable.

(b) If $L \in \{2, 3, 5, 7\}$, then $\rho_L = \Phi_L$, and for every $0 < R \le (\mu - 1)/\mu$ every such code with $Rn \ge \mu$ fails to be $(\rho_L(R) + 3/n, 2, L)$ list recoverable.

(c) If $L = 4$, $0 < R \le 3/10$, $s \ge 3$ and $Rn \ge 1$, every such code fails to be $(3/5 - R + 3/n, 2, 4)$ list recoverable.

(d) If $L = 6$, $0 < R \le 1/10$, $s \ge 5$, $n \ge 7$ and $Rn \ge 1$, every such code fails to be $(5/7 - 8R/7 + 4/n, 2, 6)$ list recoverable.

Consequently $\rho_L(R)$ is the exact list-recovery radius of these codes for large folding and length, in both the ordinary and the average-radius sense, at every rate $R \in (0, (\mu-1)/\mu]$ for $L \in \{2, 3, 5, 7\}$, at every rate $R \in (0, 3/10]$ for $L = 4$, and at every rate $R \in (0, 1/10]$ for $L = 6$.

L	μ	κ_L	exact radius $\rho_L(R)$	Chen–Zhang bound $\Phi_L(R)$	rates covered
2	2	2	$\frac{1}{3}(1-2R)$	$\frac{1}{3}(1-2R)$	$(0, \frac{1}{2}]$
3	2	4	$\frac{1}{2} - R$	$\frac{1}{2} - R$	$(0, \frac{1}{2}]$
4	3	5	$\frac{3}{5} - R$	$\frac{3}{5} - \frac{9}{10}R$	$(0, \frac{3}{10}]$
5	3	6	$\frac{2}{3} - R$	$\frac{2}{3} - R$	$(0, \frac{2}{3}]$
6	3	8	$\frac{5}{7} - \frac{8}{7}R$	$\frac{5}{7} - \frac{15}{14}R$	$(0, \frac{1}{10}]$
7	3	9	$\frac{3}{4} - \frac{9}{8}R$	$\frac{3}{4} - \frac{9}{8}R$	$(0, \frac{2}{3}]$

Table 1: Exact list-recovery radii of folded Reed–Solomon codes with appropriate evaluation points, input lists of size two and output cap L (Theorem 1.7). For $L = 4$ and $L = 6$, $\rho_L(R) < \Phi_L(R)$ at every positive rate, and ρ_L is the exact radius on the rates covered.

At $L = 3$, Proposition 2.2 recovers [5, Theorem 1.8] in average-radius form for every $s \ge 3$, since its condition (6) holds at $\rho = 1/2 - sR/(s-2)$; at $L = 7$ it gives Theorem 1.6 for all appropriate points. Part (b) for $L = 5$ says that the Chen–Zhang bound is exactly tight at the cap $L = 5$, where $L + 1$ is not a power of two, while parts (c) and (d) show that it is not tight at $L = 4$ and $L = 6$. The next theorem extends this dichotomy to every cap.

Theorem 1.8 (When the Chen–Zhang bound is tight)**.** *Let $L \ge 2$, $M = L + 1$ and $\mu = \lceil \log_2 M \rceil$.*

(a) If $L \in \{2, 3, 5, 7\}$, then $\Phi_L(R)$ is the exact list-recovery radius, in the sense of Theorem 1.7, at every rate $R \in (0, (\mu-1)/\mu]$.

(b) If $L = 4$, $L = 6$ or $L \geq 8$, put $t = \lfloor L/3 \rfloor$, $\omega = L - 3t$, $N = 2t + \omega$ and $\chi = 4t + \omega$. Then $\chi > B_L$. Moreover, for every rate $R \in (0, 2/(MN - \chi)]$, every s-folded Reed–Solomon code of rate R with appropriate evaluation points, $s \geq N + 1$, $n \geq M$ and $Rn \geq 1$ contains M distinct messages and a table of exactly two symbols per block against which every one of these messages has error less than

$$1 - \frac{2 + \chi R}{M} + \frac{2\chi + M}{Mn} = \Phi_L(R) - \frac{(\chi - B_L)R}{M} + \frac{2\chi + M}{Mn}.$$

In particular, if also $n \geq 2(2\chi + M)/((\chi - B_L)R)$, the code is not $(\Phi_L(R) - (\chi - B_L)R/(2M), 2, L)$ list recoverable.

Thus, for input lists of size two, the Chen–Zhang bound is the exact radius at small rates precisely for $L \in \{2, 3, 5, 7\}$. For $L+1 = 2^a$ with $a \geq 4$, part (b) recovers, with a shorter construction, the failure of Conjecture 3.6 of [5] established in the consolidated record [10, Theorem 1.5]; for every other $L \geq 8$ it shows that the Chen–Zhang bound of Theorem 1.1 is not the answer to Question 1.2 at small rates.

Remark 1.9 (Zero error and the generalized Singleton bound). At $\rho = 0$, Theorem 1.7(a) gives average-radius $(0, 2, L)$ list recovery at every rate below $(L - 1)/\kappa_L$, that is 1/2, 3/5 and 2/3 for $L = 2$, 4 and 5. These exceed the rate $1-1/\log_2(L+1)$ that the entropy method of Brakensiek, Chen, Dhar and Zhang [1, Theorem 3.1] supplies for subspace-design codes at these caps, approximately 0.369, 0.569 and 0.613. Chen, Cheraghchi, Si and Zhang note after their Theorem 1.2 that the negative result of [5] rules out $(0, \ell, \ell^a - 1)$ list recovery at rates above $(a - 1)/a$ [4]. A $(0, 2, L)$ list recoverable code is $(0, 2, L')$ list recoverable for every $L' \geq L$, so $(0, 2, 2)$ and $(0, 2, 5)$ list recovery are ruled out above 1/2 and 2/3 by the cases $L' = 3$ and $L' = 7$. Hence, for input lists of size two, the zero-error rate threshold of these codes with large folding is exactly 1/2 at $L = 2$ and exactly 2/3 at $L = 5$, and it lies in $[3/5, 2/3]$ at $L = 4$. At $L = 2$ the radius $\rho_2(R) = (1 - 2R)/3$ equals the generalized Singleton bound $(L + 1 - \ell - LR)/(L + 1)$ for list recovery: by Brakensiek, Chen, Putterman and Zhang [3, Theorem 3.2], no code with at least $|\Sigma|^{Rn+5L}$ codewords over an alphabet Σ is (ρ, ℓ, L) list recoverable at any ρ at or above this bound. Folded Reed–Solomon codes with large folding therefore attain the optimal radius for $\ell = L = 2$.

1.4 Prior work, scope and route

Chen and Zhang [5, Conjecture 3.6 and Theorem 3.7] proposed the power-of-input-list tradeoff and proved the input-two, output-three case. Brakensiek, Chen, Dhar and Zhang [1, Theorem 1.6] proved the zero-error case at all powers $L + 1 = \ell^a$, and in their October 11, 2026 version identify the case $(\ell, L) = (2, 3)$ as the only positive-error case proved beyond their zero-error theorem [1, Remark 1.7]. They also attribute the binary-input zero-error case to Chen, Cheraghchi, Si and Zhang [4], whose November 23, 2026 posting proves zero-error list recovery at rates approaching $(a - 1)/a$ for $\ell = 2$ and $L = 2^a - 1$. The conjectured curve, the Boolean-cube obstruction and the polynomial rank-budget framework are prior ingredients; the folded-Wronskian transfer uses the subspace-design framework [8, 2]. The consolidated record [10], which merged edition 3 of this article with two other records, treats the conjecture at all powers $L + 1 = \ell^a$ with kernel patterns and independent squares. The appropriate-points form of the cap-seven theorem, its exactness and the eight-point theorem also appear there [10, Theorem 1.3, Corollary 1.4, Proposition 4.4 and Theorem 1.8]. The present article is self-contained, nothing in it depends on that record, and it treats every cap for input lists of size two. Recent work of Goyal, Guruswami, Sun and Wootters [7] gives threshold equivalences for optimal nested subspace-design constructions, and algorithms for locating the recovered codewords are studied in, for example, [6].

The positive direction of Theorem 1.7 follows from Theorem 1.5 and the folded-Wronskian budget (Section 2). The proof of Theorem 1.5 separates according to affine dimension, as for eight points. In small dimension, large fibers force incidences among lines and planes; in large dimension, the affine dependency space is small and its supports provide the extra subspaces of the certificate (Sections 5 and 6). For the negative direction, Section 7 plants prescribed coordinate kernels in an arbitrary folded Reed–Solomon code with appropriate points by Lagrange interpolation and a first-moment choice, so that a coordinate configuration of messages is captured in prescribed fibers; pairing schedules on the remaining blocks then equalize the individual errors. Section 8 combines both directions with Theorem 1.1.

Organization. Section 2 proves the coding transfer and records the finite-parameter refinements. Sections 3–5 contain the affine tools and the proof of Theorem 1.4. Section 6 proves Theorem 1.5, Section 7 gives the constructions, and Section 8 proves Theorems 1.7 and 1.8.

2 From certificates to folded Reed–Solomon codes

We give the standard polynomial rank-budget argument explicitly to fix its characteristic, order and finite-folding conventions. This is established subspace-design machinery [8, 2].

Lemma 2.1 (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 evaluation points; the points γ^{js} of Theorem 1.6 are appropriate because $q - 1 \geq sn$. Let $K_j \leq \mathcal{P}_k$ be the kernel of the block map E_j of (1). For $W \leq \mathcal{P}_k$ with $1 \leq u = \dim W \leq s$,*

$$\sum_{j=0}^{n-1} \dim(W \cap K_j) \leq \frac{u(k-1) - u(u-1)/2}{s-u+1} \leq \frac{u(k-1)}{s-u+1}.$$

Proof. Choose a basis $g_1, \dots, g_u$ of distinct degrees $d_b < k$ by degree elimination. The polynomial

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

is nonzero: its coefficient in degree $\sum_b d_b$ is a product of the nonzero leading coefficients and the Vandermonde determinant in the elements γ^{d_b}. These are distinct because appropriate points with $s \geq 2$ are sn distinct nonzero elements, so γ has order $q - 1 \geq sn \geq k > d_b \geq 0$. Because the degrees are distinct, $\deg D = \sum_b d_b \leq u(k-1) - u(u-1)/2$.

Put $h_j = \dim(W \cap K_j)$. Change basis so the first h_j polynomials vanish on block j. For every $0 \leq t \leq s - u$, every entry $g_b(\gamma^{a+t}\alpha_j)$ of those columns at $X = \gamma^t \alpha_j$ has $a + t \leq s - 1$ and vanishes. Each such column is divisible by $X - \gamma^t \alpha_j$, so the determinant has root multiplicity at least h_j there. A basis change multiplies D by a nonzero scalar. 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 $(s - u + 1) \sum_j h_j \leq \deg D \leq u(k-1) - u(u-1)/2$. □

Proposition 2.2 (Transfer at output cap L)**.** *Let $2 \leq L \leq 7$, let γ generate $\mathbb{F}_q^\times$, let $s \geq L$ and $1 \leq k \leq sn$, and let $\alpha_0, \dots, \alpha_{n-1}$ be appropriate evaluation points. If $\rho \geq 0$ and*

$$2 + \kappa_L \frac{k-1}{n(s-L+1)} < (L+1)(1-\rho), \tag{6}$$

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

Proof. Put $r = (k-1)/(n(s-L+1))$. A nonzero polynomial of degree less than $k \le sn$ cannot vanish at the sn distinct points $\gamma^i \alpha_j$, so the encoding is injective. Let S consist of $L+1$ distinct messages and put $V = \operatorname{dir}(S)$, so $\dim V \le L \le s$. By Theorem 1.5 (Theorem 1.4 for $L = 7$), S has a certificate (y_W) of cost at most κ_L; discard weights on the zero subspace, which contribute to neither side of (3). For each support $W \le V$ we have $1 \le \dim W \le L$, and Lemma 2.1 gives

$$\sum_{j=0}^{n-1} \dim(W \cap K_j) \le \frac{(k-1)\dim W}{s - \dim W + 1} \le rn \dim W.$$

At block j two messages have equal symbols exactly when their difference lies in $K_j \cap V$, so the evaluation fibers on S are the affine $(K_j \cap V)$-cosets, and a table of two symbols captures at most $b_2(S/(K_j \cap V))$ messages there. Since $(K_j \cap V) \cap W = K_j \cap W$ for $W \le V$, summing (3) over the blocks bounds the total number of agreements of S by

$$2n + \sum_W y_W \sum_j \dim(K_j \cap W) \le 2n + rn \sum_W y_W \dim W \le n(2 + \kappa_L r) < n(L+1)(1-\rho).$$

Hence the mean error of the $L+1$ messages exceeds ρ. □

Proof of Theorem 1.6. The points γ^{js} are appropriate, and for $L = 7$ condition (6) with $\kappa_7 = 9$ reads $2 + 9(k-1)/(n(s-6)) < 8(1-\rho)$, which is (4). Proposition 2.2 applies. □

Corollary 2.3 (Asymptotic form)**.** *Fix $0 \le \rho < 3/4$, set $B = 2/3 - 8\rho/9$, and take $0 < \eta < B$. Under the remaining hypotheses of Theorem 1.6, rate $R = k/(sn) \le B - \eta$ and folding $s \ge 7 + \lceil 12/\eta \rceil$ suffice.*

Proof. Here $R \le B \le 2/3$, and

$$r < \frac{Rs}{s-6} = R + \frac{6R}{s-6} < R + \eta \le B.$$

The integer and field constraints still apply, and the strict inequality $r < B$ is condition (4). □

Corollary 2.4 (Radius form at caps two to seven)**.** *Let $2 \le L \le 7$, $\varepsilon > 0$ and $0 < R \le (L-1)/\kappa_L$. Every rate-R s-folded Reed–Solomon code with appropriate evaluation points and $s \ge L + \lceil (L-1)^2/((L+1)\varepsilon) \rceil$ is average-radius $(\rho_L(R) - \varepsilon, 2, L)$ list recoverable.*

Proof. Put $\rho = \rho_L(R) - \varepsilon$. If $\rho < 0$ there is nothing to prove, since mean errors are nonnegative. Otherwise $(L+1)(1-\rho) = 2 + \kappa_L R + (L+1)\varepsilon$ by (5). With $r = (k-1)/(n(s-L+1))$ and $k = Rsn$,

$$r < \frac{Rs}{s-L+1} = R + \frac{R(L-1)}{s-L+1},$$

and $\kappa_L R \le L - 1$ gives $\kappa_L(r - R) < (L-1)^2/(s-L+1) < (L+1)\varepsilon$, because $s - L + 1 \ge 1 + \lceil (L-1)^2/((L+1)\varepsilon) \rceil$. Thus (6) holds, and Proposition 2.2 applies. □

For $L = 7$ the folding threshold is $7 + \lceil 9/(2\varepsilon) \rceil$, and in the rate-slack form of Corollary 2.3 the same computation gives $s \ge 7 + \lceil 4/\eta \rceil$.

2.1 The Chen–Zhang bound in simplified form

Lemma 2.5. *Let $L \geq 2$ and $\mu = \lceil \log_2(L+1) \rceil$. If an s-folded Reed–Solomon code with appropriate evaluation points, rate $R \leq (\mu-1)/\mu$ and length n with $Rn \geq \mu$ is $(\rho, 2, L)$ list recoverable, then $\rho < \Phi_L(R) + 3/n$.*

Proof. We check the hypotheses of Theorem 1.1 with $\ell = 2$. Here $\mu \geq 2$ since $L+1 \geq 3$; $(k-1)/(sn) < R \leq (\mu-1)/\mu$; and $k = Rsn \geq \mu s$ gives $k - 1 \geq (\mu-1)s$. Put $\nu_0 = \lfloor (k-1)/s \rfloor \geq (k-s)/s = Rn - 1$. Then

$$\Big\lfloor \frac{\mu}{\mu-1} \nu_0 \Big\rfloor > \frac{\mu(Rn-1)}{\mu-1} - 1 \geq \frac{\mu Rn}{\mu-1} - 3,$$

since $\mu/(\mu-1) \leq 2$. Theorem 1.1 gives $\rho < \frac{L-1}{L+1}(1 - \frac{\mu R}{\mu-1} + \frac{3}{n}) \leq \Phi_L(R) + \frac{3}{n}$. □

Remark 2.6. By Lemma 2.5, the radius of Corollaries 2.3 and 2.4 at $L = 7$ cannot be increased: $\Phi_7(R) = 3/4 - 9R/8 = \rho_7(R)$. Theorem 1.7 records the same exactness at $L = 2, 3, 5$ and, at small rates, at $L = 4, 6$.

2.2 Finite-folding profiles

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

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

Proposition 2.7 (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 $\max_{1 \leq d \leq \min(7,k)} \Pi_d < n(6-8\rho)$, then it is average-radius $(\rho, 2, 7)$ list recoverable.

Proof. For a fixed eight-message configuration, summing its certificate over all blocks bounds total capture by $2n + \sum_W y_W c_{\dim W}$. For affine dimensions one through four, the cost bounds and $c_u \leq u\theta_d$ give $\Pi_1, \ldots, \Pi_4$. The proper-core certificates of Lemma 5.1 contribute $c_5 + 2c_u$ for $u = 1, 2$ or $c_5 + c_u$ for $u = 3, 4$. Its full-core certificates contribute $3c_5/2$, $3c_5/2 + c_u/2$ for $u = 1, 2$, or $c_5 + 2c_2$. These are exactly the branches of Π_5. Lemma 5.2 gives the ambient weight one and the support weight $1/\max(1, u-1)$ in dimension six, and ambient weight one in dimension seven. These give Π_6, Π_7. The strict inequality therefore excludes total capture at least $8n(1-\rho)$. No monotonicity of the budgets in u is required. □

The folded-Wronskian bound of Lemma 2.1 already supplies the budgets

$$b_u = \frac{u(k-1) - u(u-1)/2}{s - u + 1}.$$

Their numerators increase and their positive denominators decrease for $u \leq k$, so b_u is nondecreasing. Substitution in the preceding profiles recovers the simpler dimension-sensitive bounds. We next improve the budgets themselves by retaining windows that cross the ends of an evaluation block.

Lemma 2.8 (Cyclic folded-Wronskian budget)**.** *Under the hypotheses of Theorem 1.6, let* $1 \le u \le \min(s,k)$*,* $\dim W = u$*, and* $h_j = \dim(W \cap K_j)$*. Then*

$$\sum_{j=0}^{n-1} h_j(s-u+h_j) \le D_u^{\mathrm{fold}} := u(k-1) - u(u-1)/2.$$

Proof. Use the folded matrix $M(X) = (g_b(\gamma^a X))_{0\le a<u,\,1\le b\le u}$ from Lemma 2.1. Its nonzero determinant $D(X)$ has degree at most D_u^{fold}. Write $\Omega = q-1$. At $X = \gamma^t$, the rows evaluate at the u distinct cyclic exponents $t, t+1, \dots, t+u-1$ modulo Ω. Partition them among the disjoint coded blocks $B_j = \{js, \dots, js+s-1\}$ and any gap. 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 count. Writing $x_+ = \max\{x, 0\}$, we obtain

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

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

If $n = 1$, then $k \le s$ makes the sole block map injective and $h_0 = 0$. Suppose $n \ge 2$. We have $\Omega \ge sn \ge 2s \ge s+u$. For a fixed length-$s$ cyclic 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 $0 \le h \le u$,

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

Sum determinant valuations at the Ω 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 an integer budget

$$c_u(D_u) = \max\left\{ H \in \mathbb{Z} : \begin{array}{l} 0 \le H \le n\min(u, \max(k-s,0)), \quad H = nm+r,\ 0 \le r < n, \\ (s-u)H + nm^2 + r(2m+1) \le D_u \end{array} \right\}. \tag{7}$$

The set contains zero. This is a finite, explicit computation. For $H = \sum h_j$, integer convexity gives $\sum h_j^2 \ge nm^2 + r(2m+1)$: transferring one unit between two entries differing 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 2.8 therefore supplies the support budgets $c_u = c_u(D_u^{\mathrm{fold}})$ in Proposition 2.7.

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

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

Their maximum is $39 < 40 = n(6-8\rho)$, giving mean capture at most $2 + 39/10 = 59/10 < 6$. The primitive-order requirement holds since $511 \ge 290$. This certifies folding 29 for these parameters. The coarser budgets b_u certify folding 30 in the earlier example. The accompanying exact-arithmetic program reproduces both comparisons.

2.3 Hasse-derivative evaluation blocks

The same certificate applies to multiplicity codes by the classical derivative Wronskian in its large-characteristic range [8, 5].

Proposition 2.9 (Multiplicity-code receiver)**.** *Let $\mathbb{F}_q$ have characteristic p, let $n \geq 1$, $s \geq 7$, $1 \leq k \leq \min(p, sn)$, and choose distinct $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$. Encode $\deg f < k$ by the Hasse-derivative blocks $(f^{[0]}(\alpha_j), \ldots, f^{[s-1]}(\alpha_j))$. For $0 \leq \rho < 3/4$, inequality (4) suffices under the present hypotheses for average-radius $(\rho, 2, 7)$ list recovery. More sharply, Proposition 2.7 applies with $c_u = c_u(D_u^{\mathrm{mult}})$, where $D_u^{\mathrm{mult}} = u(k-u)$ and c_u is given by (7).*

Proof. The block kernel consists of polynomials divisible by $(X - \alpha_j)^s$. Injectivity follows from $k \leq sn$. For $\dim W = u \leq \min(s, k)$, its ordinary derivative Wronskian is nonzero and has degree at most $u(k-u)$: eliminate leading degrees and use the Vandermonde determinant of their falling factorials. All degrees are distinct and below $k \leq p$. At a fixed α_j, Taylor elimination gives distinct orders $0 \leq \nu_1 < \cdots < \nu_u < k$, exactly $h_j = \dim(W \cap K_j)$ of which are at least s. The leading Wronskian coefficient is again a nonzero Vandermonde, so its valuation is $\sum_i \nu_i - u(u-1)/2$. The low orders are at least $0, \ldots, u - h_j - 1$ and the high ones at least $s, \ldots, s + h_j - 1$. Hence the valuation is at least $h_j(s - u + h_j)$. Summing at distinct evaluation points gives

$$\sum_j h_j(s - u + h_j) \leq u(k-u).$$

Integer convexity gives the displayed budgets. The coarse inequality $\sum_j h_j \leq u(k-1)/(s-u+1)$ also follows, so the proof of Theorem 1.6 gives its simpler sufficient condition. □

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

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

Again the maximum is $39 < 40$. This folding-28 example uses the derivative characteristic hypothesis; the folded-29 example above instead uses a primitive element of the characteristic-two field $\mathbb{F}_{512}$.

3 Affine tools

Lemma 3.1 (Selected-fiber rank bound)**.** *Let $S = \{v_1, \ldots, v_m\}$ be distinct points of affine dimension e. On $E_0 = \{c \in \mathbb{F}^m : \sum_i c_i = 0\}$ 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, B and set $c = |A| + |B|$. Let $E \leq E_0$ consist of coefficient vectors supported on $A \cup B$ with separate coefficient sums zero on A and B. With $\delta = \dim(E \cap \Lambda)$,*

$$b_2(S/K) - 2 \leq \dim K + \delta. \tag{8}$$

Proof. A proper K cannot contain all pairwise 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 $K \leq \mathrm{dir}(S)$,*

$$b_2(S/K) \leq b_2(T/(K \cap U)) + \dim K - \dim(K \cap U) + \mathbf{1}_{U \subseteq K}. \tag{9}$$

Consequently, if a certificate for the modified quantity $b_2(T/H) + \mathbf{1}_{H=U}$ has ambient coefficient at least one and cost D, then S has an ordinary 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 σ outside points and c_T core points, and let $b \in \{0, 1, 2\}$ count the fibers meeting the core. The space of coefficients with zero sum on each selected fiber has image modulo U of dimension $\sigma - (2 - b)$. Indeed a fiber not meeting the core imposes one independent zero-sum condition on its outside coefficients; a core coefficient absorbs that condition in a fiber meeting the core. Independence in V/U gives

$$\sigma - (2 - b) \le \dim K - \dim(K \cap U).$$

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, the two core fibers contribute at least two. If $U \subseteq K$, the same inequality holds with an additional one on the right. Adding proves (9). For the last assertion, add weight one on V and subtract one from the core ambient coefficient. 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 $a \ge 1$, $w \ge 0$ rational and a line $Y_1 \le U$ with*

$$b_2(T/H) + \mathbf{1}_{H=U} \le 2 + a \dim H + w \dim(H \cap Y_1), \qquad 2a + w \le m.$$

Thus a planar core together with j affine coloops has ordinary certificate cost at most $m + j$.

Proof. For a direction line Y, set $m_Y = b_2(T/Y) - 2$. Positive values occur only in pair-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 intersect in at most four points. Therefore $m_1 + m_2 \le m$. Let Y_1 maximize m_Y and set

$$\lambda = \max\left\{1, \frac{m-1}{m_1 + m_2}\right\}, \quad a = \lambda m_2, \quad w = \lambda(m_1 - m_2).$$

Then $a \ge 1$, $w \ge 0$, and $2a + w = \max\{m-1, m_1+m_2\} \le m$. For $H = Y_1$ the increment $a + w \ge m_1$; for every other line it is $a \ge m_2$. For $H = U$ the required increment is $m - 1$, and for $H = 0$ the bound is exact. Apply Lemma 3.2. □

Lemma 3.4 (Two directions)**.** *Two distinct parallel Y-lines and two distinct parallel Y'-lines, with $Y \ne Y'$, 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 2-by-2 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 $Y + Y'$, whose union has affine dimension at most three, or three lines lie in a plane and adjoining the fourth increases dimension by at most one. □

4 Eight points in affine dimensions at most four

Throughout, captures refer to $b_2(S/K)$. For dimension one, weight six on V works: the zero kernel captures two and V captures eight. Dimension two follows from Lemma 3.3, discarding its nonnegative indicator. Dimension seven will follow from affine independence in Section 5.

Lemma 4.1 (Dimension three)**.** *Eight distinct points of affine dimension three admit 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 Y with capture $c_Y \geq 6$. It is at most seven: two parallel lines have affine span at most two. For any plane P not containing Y, its two selected cosets capture at most four points on the selected two Y-lines and at most $8 - c_Y$ outsiders. Hence

$$b_2(S/P) \leq 12 - c_Y. \tag{10}$$

If $c_Y = 7$ and another direction Y' captured at least five, the selected subsets would meet in at least four points. There are at most four cross-intersections, so Lemma 3.4 would make all eight points coplanar, a contradiction. Thus other lines capture at most four. Weights $y_V = 2$, $y_Y = 3$ work: line Y gets seven, other lines four, planes containing Y get nine, and transverse planes get six, enough by (10). Cost is nine.

If $c_Y = 6$, no other line can capture six: four common selected points would again make all eight points coplanar. If another direction captures five, the selected subsets meet in three or four points. Three intersections put their eight-point union in a plane, impossible. Four intersections give seven coplanar points plus one affine coloop, covered by Lemma 3.3 at cost at most eight. Otherwise all other lines capture at most four. Take $y_V = 2$, $y_Y = 2$, of cost eight. Planes containing Y get eight and transverse planes get six, again covering (10). Zero and full kernels satisfy every displayed certificate directly. □

Lemma 4.2 (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 Y 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. Thus all other lines capture at most four. Use $y_U = 2$, $y_Y = 2$, of cost eight. A plane avoiding Y captures at most five and gets six; a plane containing Y gets eight. The modified full-kernel value is eight and 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. Four give six coplanar points and one affine coloop. Lemma 3.3 supplies an ordinary certificate on U with ambient coefficient one and cost between six and seven: the modified planar core has cost at least $m - 1 = 5$ and adjoining the coloop adds one. Thus its full-kernel right-hand side is at least eight, covering the extra indicator as well. If Y is the only direction capturing five, take $y_U = 2$, $y_Y = 1$. Planes avoiding Y 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 4.3 (Dimension four)**.** *Eight distinct points of affine dimension four admit cost at most nine.*

Proof. If a line direction captures at least six points, six points on two parallel lines span at most a plane. The remaining two points force that plane to have dimension two and are independent affine coloops, since the total affine dimension is four. Lemma 3.3 gives cost at most eight. Line captures seven or eight are incompatible with dimension four. Similarly, if a plane direction captures at least seven points, seven lie in an affine space of dimension at most three; dimension four forces a seven-point three-dimensional core and one coloop. Lemmas 4.2 and 3.2 give cost at most nine. A plane cannot capture all eight.

We may assume line captures 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, 35/4, respectively. If just one line Y captures five, $y_V = 2$, $y_Y = 1$ works.

It remains to consider two different directions capturing five. Their selected subsets A, B meet in $t \in \{2, 3, 4\}$ points. If $t = 2$, their union is all eight and Lemma 3.4 bounds its affine dimension by three. If $t = 3$, seven points lie in a plane and the last point raises dimension to at most three. Both contradict the hypothesis. If $t = 4$, their union is six planar points; dimension four forces two independent affine coloops, already covered. This exhausts the cases; zero and full kernels satisfy the stated weights. □

5 Dependency supports in larger affine dimension

Use the notation of Lemma 3.1. Distinctness excludes a nonzero affine dependency supported on fewer than three points. We will repeatedly use the following observation, which holds for any number m of points; Lemma 5.1 applies it with $m = 8$. Let C be the exact support of a nonzero dependency, and suppose the dependency space restricted to C is one-dimensional. Then its direction space U_C has dimension $|C| - 2$. If that dependency belongs to E, all points of C lie in $b \le 2$ selected fibers, with coefficient sum zero on each. The coefficient space on C with these zero-sum conditions has dimension $|C| - b$; its image has dimension $|C| - b - 1$ and lies in $K \cap U_C$. This image is nonzero: for $|C| = 3$, a split into two nonempty groups would create a singleton with nonzero coefficient, so $b = 1$; for $|C| \ge 4$, the dimension is at least $|C| - 3 \ge 1$.

Lemma 5.1 (Dimension five)**.** *Every eight-point set of affine dimension five admits cost at most nine.*

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

First suppose C is proper, so $u \le 4$. If $\delta > 0$, then $h \ge 1$: otherwise projection modulo K is injective on the affine span of C, so the two selected fibers contain at most two core points, too few to support a dependency. If $\delta = 2$, all dependencies belong to E, so all of C lies in the two selected fibers. If $b \le 2$ of these meet C, the coefficient space on C with zero sums on the groups has image dimension $\tau - b - 2$. Thus

$$h \ge \tau - b - 2 \ge u - 1.$$

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 $C = S$. 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 must

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 with $\dim K \geq 2$, we have $\delta \leq \frac{1}{2}\dim K$. This is immediate for $\delta \leq 1$. If $\delta = 2$, all eight points occur in the selected fibers, so $\dim E = 6$ and $\dim T(E) = 4$, forcing $\dim K \geq 4$. Therefore

$$b_2(S/K) \leq 2 + \tfrac{3}{2}\dim K \qquad (\dim K \geq 2). \tag{11}$$

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 C_0, take $y_V = 3/2$, $y_{U_{C_0}} = 1/2$, of cost at most $17/2$. The observation preceding the lemma supplies a nonzero intersection for any exceptional line kernel, and (11) handles the larger proper kernels.

With two small lines, use their disjoint four-point supports C_1, C_2 and $U_i = \mathrm{dir}(C_i)$, 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

$$\delta \leq \dim(K \cap U_1) + \dim(K \cap U_2),$$

as required by Lemma 3.1. In all three full-core cases, zero and full kernels satisfy the displayed certificates directly. □

Lemma 5.2 (Dimensions $M-2$ and $M-1$)**.** *Let S consist of $M \geq 3$ distinct points. If its affine dimension is $M-2$, its dependency space is a line whose generator has support of some size $\tau \geq 3$, and S has a certificate of cost at most*

$$M - 2 + \frac{\tau - 2}{\max\{1, \tau - 3\}} \leq M.$$

If its affine dimension is $M-1$, it has a certificate of cost $M-1$. In particular, for eight points the sufficient cost is at most eight in affine dimension six and seven in dimension seven.

Proof. In affine dimension $M-2$ the dependency space has dimension one by Lemma 3.1. Let its nonzero support C have size $\tau \geq 3$; the dependencies of C are the multiples of this generator, so $U = \mathrm{dir}(C)$ has dimension $\tau - 2$. If $\delta = 1$ for a proper kernel, the observation at the start of the section gives

$$\dim(K \cap U) \geq \max\{1, \tau - 3\} =: a.$$

Thus $y_V = 1$, $y_U = 1/a$ works, with the weights added if $U = V$: for proper K Lemma 3.1 gives $b_2(S/K) - 2 \leq \dim K + \delta \leq \dim K + \dim(K \cap U)/a$, and for $\delta = 0$ ambient weight one suffices. The full kernel is covered since the cost is at least $M - 2 + 1$. The cost $M - 2 + (\tau - 2)/a$ is at most M, because $(\tau - 2)/a$ equals 1 and 2 for $\tau = 3, 4$ and is at most $3/2$ for $\tau \geq 5$.

In affine dimension $M-1$ the points are affinely independent, so $\Lambda = 0$. Lemma 3.1 gives $b_2(S/K) \leq 2 + \dim K$ for proper K. Weight one on V also covers the full kernel and has cost $M - 1$. □

Proof of Theorem 1.4. The upper bounds follow from the planar and low-dimensional arguments and Lemmas 5.1–5.2. All displayed weights are rational, nonnegative, finitely supported and fixed for S.

For sharpness let $S = \{0,1\}^3$ in a three-dimensional space. Let H_i be its three coordinate hyperplanes. Then $b_2(S/H_i) = 8$. For every W, the coordinate functionals restricted to W span W^*, so at least $\dim W$ restrictions are nonzero. Consequently

$$\sum_{i=1}^{3} \dim(W \cap H_i) \le 2 \dim W.$$

Summing any certificate's inequalities at these three kernels gives $18 \le \sum_W y_W \sum_i \dim(W \cap H_i) \le 2 \sum_W y_W \dim W$. Every certificate therefore costs at least nine, proving equality. □

6 Certificates of at most seven points

Throughout this section captures refer to $b_2(S/K)$, and $V = \mathrm{dir}(S)$. The eight-point arguments specialize directly to fewer points except in the cases $(M, e) = (6, 3)$, $(7, 3)$ and $(7, 4)$ of M points in affine dimension e; the first and last are Lemmas 6.2 and 6.3, and $(7, 3)$ is Lemma 4.2.

Lemma 6.1 (Collinear and planar sets)**.** *Let S consist of $M \ge 3$ distinct points of affine dimension e.*

(a) If $e = 1$, weight $M - 2$ on V is a certificate.

(b) If S consists of $m \ge 3$ points spanning an affine plane together with $j \ge 0$ affine coloops, it has a certificate of cost at most $m + j$. In particular, if $e = 2$ it has one of cost at most M.

Proof. (a) The only kernels are 0 and the line V, with captures 2 and $M = 2 + (M - 2)$. (b) This is the final assertion of Lemma 3.3; for $j = 0$ the nonnegative indicator is discarded. □

Lemma 6.2 (Six points in affine dimension three)**.** *Six distinct points of affine dimension three have a certificate of cost at most six.*

Proof. If every line direction captures at most four points, take $y_V = 2$, of cost six. A line kernel gets right-hand side four, a plane kernel gets six, which bounds any capture of six points, and the full kernel gets eight.

Otherwise some line Y captures at least five points. The Y-cosets are affine lines parallel to Y, so at least five points lie on at most two parallel lines and hence in one affine plane Π. Since the affine dimension is three, $S \not\subseteq \Pi$, so $T = S \cap \Pi$ has exactly five points and the sixth point p lies off Π. As the affine dimension of $T \cup \{p\}$ exceeds that of T by at most one, T spans Π and p is an affine coloop. Lemma 6.1(b) with $m = 5$ and $j = 1$ gives cost at most six. □

Lemma 6.3 (Seven points in affine dimension four)**.** *Seven distinct points of affine dimension four have a certificate of cost at most eight.*

Proof. Suppose first that every line direction captures at most four points, and take $y_V = 2$, of cost eight. Line kernels get four. A plane kernel P gets six: two cosets of P lie in an affine space of dimension at most three, so they cannot contain all seven points of a four-dimensional configuration, and $b_2(S/P) \le 6$. Kernels of dimension three get eight and the full kernel ten, both at least seven.

Otherwise some line captures at least five points, which lie on at most two parallel lines and hence in an affine plane Π. If Π contained six points, the seventh would raise the affine dimension to at most three. Hence $T = S \cap \Pi$ has exactly five points, and the two remaining points raise the affine dimension from that of T, at most two, to four. So T spans Π and the remaining two points are independent affine coloops. Lemma 6.1(b) with $m = 5$ and $j = 2$ gives cost at most seven. □

Lemma 6.4 (Direct sums of lines)**.** *If $Y_1, \dots, Y_r \le V$ are lines whose sum is direct, every certificate for S has cost at least $\sum_{i=1}^{r} (b_2(S/Y_i) - 2)$.*

Proof. For $W \le V$, the lines Y_i contained in W have a direct sum inside W, so $\sum_i \dim(W \cap Y_i) \le \dim W$. Summing (3) over $K = Y_1, \dots, Y_r$ gives

$$\sum_i (b_2(S/Y_i) - 2) \le \sum_W y_W \sum_i \dim(Y_i \cap W) \le \sum_W y_W \dim W. \qquad \square$$

Proof of Theorem 1.5. Upper bounds. Let S have M points and affine dimension e, so $1 \le e \le M-1$. Lemma 6.1 gives cost at most $M-2$ for $e = 1$ and at most M for $e = 2$, and Lemma 5.2 gives at most M for $e = M-2$ and $M-1$ for $e = M-1$. For $M = 3, 4, 5$ every dimension is covered, with maxima 2, 4 and 5. For $M = 6$ the remaining dimension $e = 3$ is Lemma 6.2, so every six-point set has cost at most six. For $M = 7$ the remaining dimensions are $e = 3$, covered by Lemma 4.2, whose modified certificate is in particular an ordinary certificate of cost at most eight, and $e = 4$, covered by Lemma 6.3. The case $M = 8$ is Theorem 1.4.

Lower bounds. Let x_1, x_2, x_3, x_4 be linearly independent vectors over an arbitrary field F. In the sets below all coefficients lie in $\{0, 1\}$, so two points lie in the same coset of Fx_1 exactly when they agree in the coefficients of x_2, x_3 and x_4, and similarly for the other three lines; this holds in every characteristic.

- $\{0, x_1, x_2\}$: modulo Fx_1 and Fx_2 the captures are 3 and 3, so Lemma 6.4 gives cost at least 2.
- The square $\{0, x_1, x_2, x_1 + x_2\}$: modulo Fx_1 the fibers $\{0, x_1\}$ and $\{x_2, x_1 + x_2\}$ capture four, and likewise modulo Fx_2; cost at least 4.
- $\{0, x_1, x_2, x_1 + x_2, x_3\}$: captures $4, 4, 3$ modulo Fx_1, Fx_2, Fx_3; cost at least 5.
- $\{0, x_1, x_2, x_1 + x_2, x_3, x_4\}$: captures $4, 4, 3, 3$ modulo $Fx_1, \dots, Fx_4$; cost at least 6.
- $\{0, x_1, x_2, x_1 + x_2, x_3, x_4, x_3 + x_4\}$: captures 4 modulo each of $Fx_1, \dots, Fx_4$; cost at least 8.

Together with the Boolean cube of Theorem 1.4, these sets attain the upper bounds. $\square$

Remark 6.5. Over a field F with an element $\beta \notin \{0, 1\}$, the planar set $P_5 = \{0, x_1, \beta x_1, x_2, x_1 + x_2\}$ also has cost exactly five: modulo Fx_1 its fibers $\{0, x_1, \beta x_1\}$ and $\{x_2, x_1 + x_2\}$ capture all five points, modulo Fx_2 the fibers $\{0, x_2\}$ and $\{x_1, x_1 + x_2\}$ capture four, and Lemma 6.1(b) bounds the cost by five. Its two kernels capture more evenly than those of the square with one further direction, and Section 7 uses it at the cap $L = 4$.

7 Planted coordinate kernels and equalized errors

Throughout this section γ generates $\mathbb{F}_q^\times$, the points $\alpha_0, \dots, \alpha_{n-1}$ are appropriate, E_j is the block map of (1) on $\mathcal{P}_k$, and $k \le sn$. Let $\mathbf{e}_0, \dots, \mathbf{e}_{N-1}$ be the standard basis of $\mathbb{F}_q^N$. For a finite set $S_0 \subseteq \mathbb{F}_q^N$ and $i < N$, the *classes of S_0 modulo* $\mathbf{e}_i$ are the nonempty sets $S_0 \cap (v + \mathbb{F}_q \mathbf{e}_i)$; two points lie in the same class exactly when they agree in every coordinate other than the ith.

Lemma 7.1 (Pairing schedules)**.** *Let $g \ge 0$ and let integers $0 \le z_v \le g$, indexed by a finite set S_0, satisfy $\sum_v z_v = 2g$. There are g two-element subsets of S_0, repetitions allowed, such that every v lies in exactly z_v of them.*

Proof. Write a sequence $\pi_1, \dots, \pi_{2g}$ in which every v occupies a run of z_v consecutive positions, and form the pairs $\{\pi_i, \pi_{i+g}\}$ for $1 \le i \le g$. Positions i and $i+g$ differ by g, while a run has length at most g and so covers at most one of them. Hence every pair has two distinct elements, and v occurs in exactly z_v pairs. □

Theorem 7.2 (Planted axis schedules)**.** *Let $N \ge 1$ and $s \ge N+1$. Let $Z_0, \dots, Z_{N-1}$ be pairwise disjoint sets of blocks with $s(|Z_i|+1) \le k$ for every i, and let G be the set of the remaining g blocks. Let $S_0 \subseteq \mathbb{F}_q^N$ have $M \ge 2$ points, and for every block $j \in Z_i$ let $A_j \subseteq S_0$ be a union of at most two classes of S_0 modulo $\mathbf{e}_i$. Put $a_v = |\{j \in Z_0 \cup \cdots \cup Z_{N-1} : v \in A_j\}|$. If an integer Θ satisfies*

$$a_v \le \Theta \le a_v + g \quad (v \in S_0) \qquad \text{and} \qquad \sum_{v \in S_0} (\Theta - a_v) \le 2g, \tag{12}$$

then there are linearly independent $p_0, \dots, p_{N-1} \in \mathcal{P}_k$ and a table of exactly two symbols per block such that each of the M distinct messages $f_v = \sum_i v_i p_i$ $(v \in S_0)$ agrees with the table on at least Θ blocks.

Proof. Planting. Let $\mathcal{P}^{(i)} = \{f \in \mathcal{P}_k : E_j(f) = 0 \text{ for } j \in Z_i\}$. For $j \notin Z_i$ the map $\mathcal{P}^{(i)} \to \mathbb{F}_q^s$, $f \mapsto E_j(f)$, is onto: the $s(|Z_i|+1)$ elements $\gamma^u \alpha_{j'}$ with $u < s$ and $j' \in Z_i \cup \{j\}$ are distinct because the points are appropriate, so Lagrange interpolation gives a polynomial of degree less than $s(|Z_i|+1) \le k$ with value zero at those with $j' \in Z_i$ and arbitrary prescribed values at those with $j' = j$. Choose $p_i \in \mathcal{P}^{(i)}$ uniformly at random, independently for $i < N$. For a block j let $I_j = \{i : j \notin Z_i\}$. Then $E_j(p_i) = 0$ for $i \notin I_j$, while the vectors $E_j(p_i)$, $i \in I_j$, are independent and uniformly distributed in $\mathbb{F}_q^s$, being images of independent uniform elements under onto linear maps. Call j *bad* if these $|I_j| \le N$ vectors are linearly dependent. Exposing them one at a time, the uth lies in the span of its predecessors with probability at most q^{u-1}/q^s, so

$$\Pr[j \text{ bad}] \le \sum_{u=1}^{N} q^{u-1-s} = \frac{q^N - 1}{(q-1)q^s} < q^{N-s}.$$

Appropriate points with $s \ge 2$ are sn distinct nonzero elements, so $q > sn \ge n$, and $s \ge N+1$ gives an expected number of bad blocks below $nq^{N-s} \le n/q < 1$. Fix $p_0, \dots, p_{N-1}$ with no bad block.

Let $f = \sum_i \beta_i p_i$ with $\beta_i \in \mathbb{F}_q$. At a block $j \in Z_i$ we have $I_j = \{i' : i' \ne i\}$, since the sets $Z_{i'}$ are disjoint, so $E_j(f) = \sum_{i' \ne i} \beta_{i'} E_j(p_{i'})$ vanishes exactly when $\beta_{i'} = 0$ for all $i' \ne i$. At a block $j \in G$ we have $I_j = \{0, \dots, N-1\}$, and $E_j(f) = 0$ only if every $\beta_i = 0$. If $f = 0$ with some $\beta_i \ne 0$, choose a block $j \notin Z_i$, which exists because $s(|Z_i|+1) \le k \le sn$; then $i \in I_j$ and $\sum_{i' \in I_j} \beta_{i'} E_j(p_{i'}) = 0$ contradicts the choice. Hence $p_0, \dots, p_{N-1}$ are independent and the messages f_v are distinct.

Special blocks. At $j \in Z_i$ the preceding paragraph gives $E_j(f_v) = E_j(f_w)$ exactly when $v - w \in \mathbb{F}_q \mathbf{e}_i$, that is, when v and w lie in the same class modulo $\mathbf{e}_i$. The classes forming A_j therefore produce at most two symbols; let the table at j consist of them, completed by an arbitrary further symbol if there is only one. Every f_v with $v \in A_j$ agrees with the table at j.

Generic blocks. Put $z_v = \Theta - a_v$. By (12), $0 \le z_v \le g$ and $\sum_v z_v \le 2g$. Since $M \ge 2$, we may raise some of the z_v one unit at a time, keeping $z_v \le g$, until $\sum_v z_v = 2g$. Lemma 7.1 gives pairs $\{v_j, w_j\}$ with $v_j \ne w_j$, indexed by $j \in G$, in which every v lies exactly z_v times. At $j \in G$ the table is $\{E_j(f_{v_j}), E_j(f_{w_j})\}$; these symbols are distinct because E_j is injective on the span of the p_i. Every f_v now agrees with the table on at least $a_v + z_v \ge \Theta$ blocks. □

Proposition 7.3 (Equalized axis schedules)**.** *Let $N \ge 1$ and $s \ge N+1$. Let $S_0 \subseteq \mathbb{F}_q^N$ have $M \ge 2$ points, and for each $i < N$ let $A_i \subseteq S_0$ be a union of at most two classes of S_0 modulo $\mathbf{e}_i$. Put*

$\psi_v = |\{i : v \in A_i\}|$, $\psi_{\max} = \max_v \psi_v$, $\psi_{\min} = \min_v \psi_v$ *and* $\chi = \sum_i |A_i| - 2N$. *Let* $z \geq 0$ *be an integer with* $s(z+1) \leq k$ *and* $Nz \leq n$, *and put* $\Theta = \lfloor (2n + \chi z)/M \rfloor$. *If*

$$z\psi_{\max} \leq \Theta \qquad \text{and} \qquad \Theta - z\psi_{\min} \leq n - Nz, \tag{13}$$

then the code contains M *distinct messages and a table of exactly two symbols per block against which every one of these messages has error at most* $1 - \Theta/n$.

Proof. Choose pairwise disjoint sets $Z_0, \ldots, Z_{N-1}$ of z blocks each and put $A_j = A_i$ for $j \in Z_i$. Then $a_v = z\psi_v$ and $g = n - Nz$. By (13), $a_v \leq z\psi_{\max} \leq \Theta$ and $\Theta - a_v \leq \Theta - z\psi_{\min} \leq g$. Since $\sum_v \psi_v = \sum_i |A_i| = 2N + \chi$ and $M\Theta \leq 2n + \chi z$,

$$\sum_v (\Theta - a_v) = M\Theta - z(2N + \chi) \leq 2(n - Nz) = 2g.$$

Theorem 7.2 applies. □

Corollary 7.4 (The planar five-point schedule)**.** *Let* $s \geq 3$ *and let the code have rate* $R = k/(sn)$ *with* $Rn \geq 1$ *and* $R \leq 3/10$. *Then it contains five distinct messages and a table of exactly two symbols per block against which every one of the five messages has error at most* $3/5 - R + 14/(5n)$.

Proof. Since $q > sn \geq 3$, choose $\beta \in \mathbb{F}_q \setminus \{0, 1\}$. Take $N = 2$ and $S_0 = \{0, \mathbf{e}_0, \beta\mathbf{e}_0, \mathbf{e}_1, \mathbf{e}_0 + \mathbf{e}_1\}$, the coordinate form of the set P_5 of Remark 6.5. Modulo $\mathbf{e}_0$ the classes are $\{0, \mathbf{e}_0, \beta\mathbf{e}_0\}$ and $\{\mathbf{e}_1, \mathbf{e}_0 + \mathbf{e}_1\}$; modulo $\mathbf{e}_1$ they are $\{0, \mathbf{e}_1\}$, $\{\mathbf{e}_0, \mathbf{e}_0 + \mathbf{e}_1\}$ and $\{\beta\mathbf{e}_0\}$. Take $A_0 = S_0$ and $A_1 = \{0, \mathbf{e}_0, \mathbf{e}_1, \mathbf{e}_0 + \mathbf{e}_1\}$. Then $\psi_v = 2$ for $v \neq \beta\mathbf{e}_0$, $\psi_{\beta\mathbf{e}_0} = 1$ and $\chi = 5 + 4 - 4 = 5$.

Put $z = \lfloor k/s \rfloor - 1$. Then $z \geq 0$ because $k = Rsn \geq s$, $s(z+1) \leq k$, and $Rn - 2 \leq z \leq Rn - 1 \leq 3n/10 - 1$, so $2z \leq n$. Here $\Theta = \lfloor 2n/5 \rfloor + z$. Since z is an integer at most $2n/5 - 1$, we have $z \leq \lfloor 2n/5 \rfloor$, that is $2z \leq \Theta$; and $2z \leq 3n/5$ gives $\Theta - z = \lfloor 2n/5 \rfloor \leq n - 2z$. Proposition 7.3 applies, and every error is at most

$$1 - \frac{\lfloor 2n/5 \rfloor + z}{n} \leq 1 - \frac{2n/5 - 4/5 + Rn - 2}{n} = \frac{3}{5} - R + \frac{14}{5n}.$$ □

For the remaining caps we use squares and coordinate lines sharing the origin. Let $M \geq 5$ and write $M - 1 = 3t + \omega$ with $t \geq 1$ and $\omega \in \{0, 1, 2\}$; put $N = 2t + \omega$ and $\chi = 4t + \omega$, and let

$$\mathcal{Q}_M = \{0\} \cup \bigcup_{h<t} \{\mathbf{e}_{2h},\, \mathbf{e}_{2h+1},\, \mathbf{e}_{2h} + \mathbf{e}_{2h+1}\} \cup \{\mathbf{e}_i : 2t \leq i < N\} \subseteq \mathbb{F}_q^N, \tag{14}$$

a set of $1 + 3t + \omega = M$ points; it is the input-two family of independent squares of [10, Theorem 1.9], cited here for context, taken at every M with $\omega \in \{0, 1, 2\}$ free coordinate lines. By Lemma 6.4, applied to its N coordinate lines, its certificate cost is at least $4t + \omega = \chi$.

Corollary 7.5 (Squares schedules)**.** *Let* $M \geq 5$ *and let* t, ω, N, χ *be as above. Let* $s \geq N + 1$, $n \geq M$, *and let the code have rate* $R = k/(sn)$ *with* $Rn \geq 1$ *and* $R \leq 2/(MN - \chi)$. *Then it contains* M *distinct messages and a table of exactly two symbols per block against which every one of these messages has error less than*

$$1 - \frac{2 + \chi R}{M} + \frac{2\chi + M}{Mn}.$$

Proof. Take $S_0 = \mathcal{Q}_M$. Modulo $\mathbf{e}_{2h}$ the classes are $\{0, \mathbf{e}_{2h}\}$, $\{\mathbf{e}_{2h+1}, \mathbf{e}_{2h} + \mathbf{e}_{2h+1}\}$ and singletons, and likewise modulo $\mathbf{e}_{2h+1}$; modulo $\mathbf{e}_i$ with $i \geq 2t$ they are $\{0, \mathbf{e}_i\}$ and singletons. Let $A_{2h} = A_{2h+1}$ be the square $\{0, \mathbf{e}_{2h}, \mathbf{e}_{2h+1}, \mathbf{e}_{2h} + \mathbf{e}_{2h+1}\}$, a union of two classes in both cases, and $A_i = \{0, \mathbf{e}_i\} \cup \{\mathbf{e}_0\}$ for $i \geq 2t$. Then $\psi_0 = N$, $\psi_{\mathbf{e}_0} = 2 + \omega$, every other square point has $\psi_v = 2$, and every point $\mathbf{e}_i$ with $i \geq 2t$ has $\psi_v = 1$. So $\psi_{\max} = N$, $\psi_{\min} = 1$ if $\omega \geq 1$ and $\psi_{\min} = 2$ if $\omega = 0$, and $\sum_i |A_i| - 2N = 8t + 3\omega - 2N = \chi$.

We record three inequalities. First, $\chi \leq 3N \leq (M-2)N$, so $2N \leq MN - \chi$. Second, $N \geq 3$ and $\chi < 2M$, so $MN - \chi \geq M - 1$. Third,

$$(M-2)(MN-\chi) - 2(\chi + MN - M\psi_{\min}) = M\big((M-4)N - \chi + 2\psi_{\min}\big) \geq 0, \tag{15}$$

because the bracket is $3 - 5 + 2 = 0$ for $M = 5$, and for $M \geq 6$ it is at least $2N - \chi + 2 = \omega + 2$.

Put $z = \min\{\lfloor k/s \rfloor - 1, \lfloor (2n - M + 1)/(MN - \chi) \rfloor\}$. Both entries are nonnegative, because $k \geq s$ and $n \geq M$, and $s(z+1) \leq k$. Since $R \leq 2/(MN-\chi)$ and $MN - \chi \geq M - 1$,

$$\Big\lfloor \frac{2n - M + 1}{MN - \chi} \Big\rfloor > \frac{2n}{MN-\chi} - \frac{M-1}{MN-\chi} - 1 \geq Rn - 2,$$

and $\lfloor k/s \rfloor - 1 > Rn - 2$, so $z \geq Rn - 2$. Also $z \leq 2n/(MN-\chi)$, whence $Nz \leq n$ by the first inequality. With $\Theta = \lfloor (2n + \chi z)/M \rfloor \geq (2n + \chi z - M + 1)/M$, the choice of z gives $(MN - \chi)z \leq 2n - M + 1$, that is $Nz \leq \Theta$. By (15) and $z \leq 2n/(MN-\chi)$ we get $(\chi + MN - M\psi_{\min})z \leq (M-2)n$, which rearranges to $(2n + \chi z)/M - z\psi_{\min} \leq n - Nz$ and gives $\Theta - z\psi_{\min} \leq n - Nz$. Proposition 7.3 applies, and every error is at most

$$1 - \frac{\Theta}{n} \leq 1 - \frac{2n + \chi(Rn-2) - M + 1}{Mn} = 1 - \frac{2 + \chi R}{M} + \frac{2\chi + M - 1}{Mn}. \qquad \square$$

8 Proofs of Theorems 1.7 and 1.8

Lemma 8.1. *For $L \geq 3$ let $t = \lfloor L/3 \rfloor$, $\omega = L - 3t$, $\chi = 4t + \omega$, and let B_L be as in (2). Then $\chi = B_L$ for $L \in \{3, 5, 7\}$, and $\chi > B_L$ for $L \in \{4, 6\}$ and every $L \geq 8$. Moreover $\kappa_L = B_L$ for $L \in \{2, 3, 5, 7\}$.*

Proof. For $L = 3, 4, 5, 6, 7$ the pairs (χ, B_L) are $(4, 4)$, $(5, 9/2)$, $(6, 6)$, $(8, 15/2)$ and $(9, 9)$, and $\kappa_2 = 2 = B_2$. For $L \geq 8$ we have $L + 1 \geq 9$, so $\mu \geq 4$ and $B_L = (L-1)\mu/(\mu - 1) \leq 4(L-1)/3$, while $\chi = (4L - \omega)/3 \geq (4L - 2)/3$. $\square$

Proof of Theorem 1.7. Part (a) is Corollary 2.4. For part (b), Lemma 8.1 and (2) give $\rho_L = \Phi_L$, and Lemma 2.5 shows that a $(\rho_L(R) + 3/n, 2, L)$ list recoverable code would satisfy $\rho_L(R) + 3/n < \Phi_L(R) + 3/n$, which is false. For part (c), Corollary 7.4 gives five messages with error at most $3/5 - R + 14/(5n) < 3/5 - R + 3/n$, one more than the cap $L = 4$ allows. For part (d), Corollary 7.5 with $M = 7$, $t = 2$, $\omega = 0$, $N = 4$ and $\chi = 8$ applies for $R \leq 2/(28 - 8) = 1/10$, $s \geq 5$, $n \geq 7$ and $Rn \geq 1$, and gives seven messages with error less than $5/7 - 8R/7 + 23/(7n) < 5/7 - 8R/7 + 4/n$.

For the final assertion fix R in the stated range and $\varepsilon > 0$. By (a), every such code with $s \geq L + \lceil (L-1)^2/((L+1)\varepsilon) \rceil$ is average-radius, hence ordinary, $(\rho_L(R) - \varepsilon, 2, L)$ list recoverable. By (b)–(d), every such code with $s \geq 5$ and $n \geq \max\{4/\varepsilon, \mu/R\}$ has $L + 1$ messages of error at most $\rho_L(R) + \varepsilon$; it is then neither ordinary nor average-radius $(\rho_L(R) + \varepsilon, 2, L)$ list recoverable, since $L + 1$ messages of error at most ρ have mean error at most ρ. $\square$

Proof of Theorem 1.8. Part (a) is the final assertion of Theorem 1.7 together with $\rho_L = \Phi_L$ for $L \in \{2, 3, 5, 7\}$. For part (b), $M = L + 1 \geq 5$, and t, ω, N, χ agree with those of Corollary 7.5, since $M - 1 = L = 3t + \omega$. Lemma 8.1 gives $\chi > B_L$, and Corollary 7.5 gives the M messages and the table. The displayed identity is (2). If $n \geq 2(2\chi + M)/((\chi - B_L)R)$, the error term $(2\chi + M)/(Mn)$ is at most $(\chi - B_L)R/(2M)$, so all $M = L + 1$ messages have error less than $\Phi_L(R) - (\chi - B_L)R/(2M)$. □

Software and data

The verification scripts accompanying this edition are plain Python programs. `exhaustive_small_caps.py` enumerates, over $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$ and $\mathbb{F}_7$ and in the affine dimensions listed in its output, all configurations of three to eight points up to affine equivalence (cases with more than $4 \cdot 10^5$ normalized configurations are omitted), computes their certificate costs by the finite linear program of Definition 1.3, and certifies each value in exact rational arithmetic; every maximum is at most the bound of Theorem 1.5, and for each $M = 3, \ldots, 8$ that bound is reached by some enumerated configuration. `frs_schedules.py` builds explicit folded Reed–Solomon codes over prime fields, carries out the constructions of Corollaries 7.4 and 7.5 and recomputes every error from raw polynomial evaluations. `finite_profiles.py` reproduces the finite-folding profiles of Section 2 in exact arithmetic. The proofs in this article are analytic; the programs check them on finite instances.

Statements and Declarations

Funding. This research was self-funded.

Competing interests. The author owns Luminary Oddities and has no other relevant competing interests.

Data and code availability. The verification scripts cited in the text are included with this article.

Prior editions. Edition 4 of this article is available in the Luminary Research Archive, `https://research.luminaryoddities.org/eight-point-fiber-certificates-binary-input-list-recovery-folded-reed-solomon-codes/v/4`, `https://doi.org/10.5281/zenodo.24472476`.

AI assistance. OpenAI ChatGPT and Codex (earlier editions) and Anthropic Claude (this edition) assisted with derivations, proof development, computations, source checks and independent internal review. Scott Schubr directed the research and is responsible for the content.

References

[1] J. Brakensiek, Y. Chen, M. Dhar and Z. Zhang, *Combinatorial bounds for list recovery via discrete Brascamp–Lieb inequalities*, Proceedings of the 58th Annual ACM Symposium on Theory of Computing (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 the 58th Annual ACM Symposium on Theory of Computing (STOC 2026), pp. 619–630. https://doi.org/10.1145/3798129.3800778. arXiv:2510.13777v1, October 15, 2025.

[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 paper, 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*, arXiv:2611.30030v1, November 23, 2026, https://arxiv.org/abs/2611.30030v1.

[5] Y. Chen and Z. Zhang, *Explicit folded Reed–Solomon and multiplicity codes achieve relaxed generalized Singleton bounds*, Proceedings of the 57th Annual ACM Symposium on Theory of Computing (STOC 2025), pp. 1–12. https://doi.org/10.1145/3717823.3718114. Full version: arXiv:2408.15925v3, April 14, 2025; first version August 28, 2024, 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, December 8, 2025, https://arxiv.org/abs/2512.08017v1.

[7] 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.

[8] V. Guruswami and S. Kopparty, *Explicit subspace designs*, Combinatorica 36 (2016), no. 2, 161–185. https://doi.org/10.1007/s00493-014-3169-1.

[9] V. Guruswami and A. Rudra, *Explicit codes achieving list decoding capacity: error-correction with optimal redundancy*, IEEE Transactions on Information Theory 54 (2008), no. 1, 135–150. https://doi.org/10.1109/TIT.2007.911222.

[10] S. Schubr, *The Chen–Zhang list-recovery conjecture for folded Reed–Solomon codes: a proof at output cap seven and counterexamples beyond*, edition 1. Luminary Research Archive, November 2026. https://doi.org/10.5281/zenodo.24406130.