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

Scott Schubr

October 18, 2026

Abstract

For eight distinct points over an arbitrary field, we construct a finite nonnegative rational certificate bounding the total population of the two largest fibers of every linear quotient. The certificate has intercept two and total dimension cost at most nine, and its weights are fixed independently of the quotient. This cost is attained by the Boolean three-cube. A standard folded-Wronskian argument then gives average-radius list recovery with input lists of size two and output cap seven for primitive-power folded Reed–Solomon codes whenever $(k-1)/(n(s-6)) < 2/3-8\rho/9$, with folding $s \geq 7$. The asymptotic tradeoff is the corresponding case of the existing Chen–Zhang conjecture. As supporting results, we prove that three arbitrary replacements of vertices of a Boolean four-cube preserve certificate cost at most 56/3, and exhibit an all-field family of affine dimension six attaining that cost.

Keywords. Folded Reed–Solomon codes; list recovery; affine configurations; fiber certificates; folded Wronskian.
2020 Mathematics Subject Classification. 94B35.

1 Introduction and statements

An affine configuration determines how many points can lie in the two largest fibers of a linear quotient. We seek one fixed collection of nonnegative subspace weights controlling that count for every quotient. For eight points over any field, a total dimension cost of nine suffices, and the Boolean three-cube attains this value. By affine dimension 1 through 7, the proof supplies the sufficient costs $(6, 8, 9, 9, 9, 8, 7)$. The coding consequence uses primitive-power evaluation blocks and a strict finite-parameter rate inequality. Binary input means two allowed folded symbols at a coordinate over the stated finite field.

List recovery asks how many codewords can agree on many coordinates with a table of small symbol lists. Chen and Zhang [1, Conjecture 3.6 and Theorem 3.7] identified a sharp candidate tradeoff for folded Reed–Solomon codes when the output cap plus one is a power of the input list size, and proved the binary-input, output-three case. Brakensiek, Chen, Dhar and Zhang [2, Theorem 1.6] subsequently proved the general zero-error case and developed entropy and remainder Brascamp–Lieb methods. Their version of October 11, 2026 retains the finer positive-error tradeoff as an open problem beyond the known output-three case [2, Remark 1.7 and Section 1.3].

The principal result here is a finite affine-configuration inequality supplying the eight-message, positive-error case. The proof treats arbitrary dependence coefficients over the original field. It combines elementary incidence in small affine dimension with a support analysis of the affine dependency space in large dimension. Subspace-design and local-profile methods [3, 4] provide the established coding framework.

Relation to the binary zero-error case. Chen, Cheraghchi, Si, and Zhang also studied this conjecture. Their manuscript [5] is cited by Brakensiek–Chen–Dhar–Zhang [2] as establishing the binary-input zero-error case. The conjectured tradeoff, Boolean-cube obstruction, rank-budget framework and folded-Wronskian method provide the prior framework for the positive-error eight-message consequence proved here.

Let S be a finite set of distinct points, and let $V = \mathrm{dir}(S)$ be the linear span of its pairwise differences. Translate one point to zero when viewing S inside V. For $K \le V$, let $b_2(S/K)$ be the sum of the two largest cardinalities of intersections of S with affine K-cosets. If there is only one nonempty coset, the second cardinality is zero.

Definition 1.1. A certificate for S is a finite collection of subspaces $W \le V$ and weights $y_W \in \mathbb{Q}_{\ge 0}$ such that

$$b_2(S/K) \le 2 + \sum_W y_W \dim(K \cap W) \qquad (K \le V). \tag{1}$$

Its cost is $\sum_W y_W \dim W$. The weights may depend on S, but not on K. Write $\mathcal{C}(S)$ for the infimum of certificate costs.

Theorem 1.2 (Eight-point certificate)**.** *Every set S 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, $\mathcal{C}(S) = 9$.

Theorem 1.3 (Folded Reed–Solomon consequence)**.** *Let $n \ge 1$, $s \ge 7$ and $1 \le k \le sn$ be integers, let $q > sn$ be a prime power, and let γ generate $\mathbb{F}_q^\times$. Encode $\deg f < k$ by the n folded blocks*

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

For $0 \le \rho < 3/4$, the strict condition

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

implies average-radius $(\rho, 2, 7)$ list recovery: against any table of at most two folded symbols per block, no eight distinct codewords have average agreement at least $1-\rho$. In particular the code is ordinarily $(\rho, 2, 7)$ list recoverable.

The coding statement is proved in Section 5, including all finite-parameter and multiplicative-order hypotheses. At fixed ρ, its asymptotic rate threshold is $R < 2/3 - 8\rho/9$. This is the $\ell = 2$, $L = 7$ case of the Chen–Zhang conjectured curve. For comparison, the generic entropy analysis in [2] gives the sufficient rate $(1-\rho)\log(4(1-\rho))/\log 8$ in this normalization. At $\rho = 1/4$, these thresholds are $4/9$ and approximately 0.39624. Related decoding algorithms appear in [6].

For a finite-parameter example, take $n = 10$, $s = 70$, $k = 280$, $q = 1024$ and $\rho = 1/4$, with any primitive $\gamma \in \mathbb{F}_{1024}^\times$. Then $q > sn$, the rate is $R = 2/5$, and $(k-1)/(n(s-6)) = 279/640 < 4/9$, so Theorem 1.3 applies.

Theorem 1.4 (Supporting sixteen-point results)**.** *Let C be an independent-edge affine Boolean four-cube over any field. If S consists of sixteen distinct points with $|S \cap C| \geq 13$, then S has a certificate of cost at most $56/3$.*

Moreover, let $U = \operatorname{dir}(C)$, choose thirteen vertices $T \subset C$ and $t \in T$, and choose a, b linearly independent modulo U. Then

$$S = T \cup \{t + a, t + b, t + a + b\}$$

has affine dimension six and $\mathcal{C}(S) = 56/3$.

The second family lies within the first theorem's three-replacement class. Its sharpness concerns Definition 1.1.

The independent-square construction in [7] gives a general sixteen-point certificate-cost counterexample of value twenty. The structured sixteen-point theorem above instead retains a thirteen-vertex cube core and gives its stated sharp cost. These are complementary results for the certificate problem.

Organization. The affine rank and coloop tools precede the eight-point proof in small and large affine dimensions. Section 5 supplies the complete folded-Wronskian transfer with its order, characteristic and folding hypotheses. The final section proves the structured sixteen-point bounds and sharp-family statement independently.

2 Affine tools

Lemma 2.1 (Selected-fiber rank bound)**.** *Let $S = \{v_1, \dots, v_m\}$ have affine dimension d. 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 $\dim \Lambda = m - 1 - d$. 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 $\delta = \dim(E \cap \Lambda)$,*

$$b_2(S/K) - 2 \leq \dim K + \delta. \tag{3}$$

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 2.2 (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 $K \leq \operatorname{dir}(S)$,*

$$b_2(S/K) \leq b_2(T/(K \cap U)) + \dim K - \dim(K \cap U) + \mathbf{1}_{U \subseteq K}. \tag{4}$$

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 s 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 $s - (2 - b)$. 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

$$s - (2 - b) \leq \dim K - \dim(K \cap U).$$

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 (4). 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 2.3 (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 $L_1 \le U$ with*

$$b_2(T/H) + \mathbf{1}_{H=U} \le 2 + a \dim H + w \dim(H \cap L_1), \qquad 2a + w \le m.$$

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

Proof. For a direction line L, set $m_L = b_2(T/L) - 2$. 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 L_1 maximize m_L 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 $H = L_1$ 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 2.2. □

Lemma 2.4 (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 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 $L + M$, 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. □

3 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 2.3, discarding its nonnegative indicator. Dimension seven will follow from affine independence in Section 4.

Lemma 3.1 (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 L with capture $c_L \ge 6$. It is at most seven: two parallel lines have affine span at most two. For any 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. Hence

$$b_2(S/P) \le 12 - c_L. \tag{5}$$

If $c_L = 7$ and another direction M captured at least five, the selected subsets would meet in at least four points. There are at most four cross-intersections, so Lemma 2.4 would make all eight points coplanar, a contradiction. 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 get nine, and transverse planes get six, enough by (5). Cost is nine.

If $c_L = 6$, 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 2.3 at 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 get six, again covering (5). Zero and full kernels satisfy every displayed certificate directly. □

Lemma 3.2 (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 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. 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 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 2.3 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 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 3.3 (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 2.3 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 3.2 and 2.2 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 L captures five, $y_V = 2$, $y_L = 1$ 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 2.4 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. □

4 Dependency supports in larger affine dimension

Use the notation of Lemma 2.1 with $m = 8$. Distinctness excludes a nonzero affine dependency supported on fewer than three points. We will repeatedly use the following observation. 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 4.1 (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 $t = |C|$ and $U = \mathrm{dir}(C)$. All dependencies are supported on C, so $u = \dim U = t - 3$. Distinctness implies $t \ge 4$. 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 $t - b - 2$. Thus

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

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 2.1 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 of dimension $k \ge 2$, we have $\delta \le k/2$. 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 $k \ge 4$. Therefore

$$b_2(S/K) \le 2 + \tfrac{3}{2} \dim K \qquad (k \ge 2). \tag{6}$$

For a line kernel, $\delta = 2$ is impossible. If $\delta = 1$, Lemma 2.1 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 (6) 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

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

as required by Lemma 2.1. In all three full-core cases, zero and full kernels satisfy the displayed certificates directly. □

Lemma 4.2 (Dimensions six and seven)**.** *In affine dimension six the sufficient cost is at most eight; in dimension seven it is seven.*

Proof. In dimension six the dependency space has dimension one. Let its nonzero support C have size $t \geq 3$, so $U = \mathrm{dir}(C)$ has dimension $t-2$. If $\delta = 1$ for a proper kernel, the observation at the start of the section gives

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

Thus $y_V = 1$, $y_U = 1/a$ works and has cost $6 + (t-2)/a \leq 8$. 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 2.1 gives $b_2(S/K) \leq 2 + \dim K$ for proper K. Weight one on V also covers the full kernel and has cost seven. □

Proof of Theorem 1.2. The upper bounds follow from the planar and low-dimensional arguments and Lemmas 4.1–4.2. 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

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

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

5 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 [3, 4].

Lemma 5.1 (Folded-Wronskian budget)**.** *Under the hypotheses of Theorem 1.3, let* $\mathcal{P}_k = \{f \in \mathbb{F}_q[X] : \deg f < k\}$ *and let* $K_j \leq \mathcal{P}_k$ *be the kernel of the* j*th folded evaluation block. For* $W \leq \mathcal{P}_k$ *with* $1 \leq u = \dim W \leq s$*,*

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

Proof. Choose a basis $g_1, \ldots, g_u$ of distinct degrees $d_i < k$ 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 distinct elements γ^{d_b}. They are distinct because γ has order $q - 1 \geq sn$ and $0 \leq d_b < k \leq sn$. Also $\deg D \leq u(k-1)$.

Put $h_j = \dim(W \cap K_j)$. Change basis so the first h_j polynomials vanish on block j. For every $0 \leq t \leq s-u$, all entries in those columns vanish at $X = \gamma^{js+t}$. Each such column is divisible by $X - \gamma^{js+t}$, so the determinant has root multiplicity at least h_j. A basis change multiplies D by a nonzero scalar. All these roots, across j, t, are distinct by the same order condition. Summing multiplicities gives $(s-u+1)\sum_j h_j \leq \deg D \leq u(k-1)$. □

Proof of Theorem 1.3. All sn evaluation points are distinct and $k \le sn$, so the encoding is injective. Suppose eight distinct messages formed a forbidden average-radius list. Their affine-direction space $V \le \mathcal{P}_k$ has dimension at most seven. At block j, the evaluation fibers are affine cosets of $K_j \cap V$, so the number of messages whose folded symbol is in the two-symbol table is at most $b_2(S/(K_j \cap V))$.

Apply Theorem 1.2. For each certificate support $W \le V$, its dimension is at most seven, and Lemma 5.1 gives

$$\frac{1}{n}\sum_j \dim(W \cap K_j) \le \frac{k-1}{n(s-6)} \dim W =: r \dim W.$$

The mean number of captured messages is therefore at most $2 + 9r$. Average agreement at least $1 - \rho$ would require it to be at least $8(1-\rho)$, giving $r \ge 2/3 - 8\rho/9$, contrary to (2). If each of eight messages individually has agreement at least $1 - \rho$, its average does too, proving ordinary list recovery. □

Corollary 5.2 (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 1.3, 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. The theorem does not include equality $r = B$. □

Remark 5.3. Sharpness concerns the stated nonnegative-certificate problem. The asymptotic target and its coding obstruction originate in [1]. Our proof establishes a sufficient inequality through a particular class of nonnegative certificates.

6 Three replacements and a noncube sharp family

The following proof treats the structured sixteen-point statements independently of any universal sixteen-point assertion.

Lemma 6.1 (Cube intersection bound)**.** *An affine h-flat meets an independent-edge Boolean a-cube in at most 2^h points.*

Proof. Inside the cube's affine span, choose coordinate functionals whose restrictions give an injective projection of the intersection flat into $\mathbb{F}^r$, where $r \le h$ is that flat's dimension. Each chosen coordinate of a cube vertex has at most two values, so there are at most $2^r \le 2^h$ such vertices. The argument uses neither an ordering nor a characteristic assumption. □

Proof of the first assertion of Theorem 1.4. Translate the cube's affine span to its direction space U, of dimension four. At least thirteen retained vertices span U, since a proper affine subspace contains at most eight cube vertices. For $K \le V = \mathrm{dir}(S)$ put $H = K \cap U$, $h = \dim H$, and $\delta = \dim K - h$. Core fibers are its H-fibers. Let j be the number of points of S outside U. We have $0 \le j \le 3$.

No external points: $j = 0$**.** Each two-line capture is at most $4 + 3 = 7$ and each two-plane capture at most $8 + 3 = 11$. There is at most one line direction of capture seven. To see this, two such selected covers each contain four cube vertices and all three noncube points. Their common three points force all four support lines into a plane by Lemma 2.4. There are at most four cross-intersections, so their cube subsets share at most one point. The plane would contain at least seven cube vertices, contradicting Lemma 6.1.

If there is no direction of capture seven, use $y_V = 14/3$. Captures at ranks one and two are at most six and eleven, respectively, and rank three has right-hand side sixteen. If there is a unique heavy direction L, use $y_V = 9/2$, $y_L = 1/2$, of cost $37/2$. Lines and planes are covered. A rank-three kernel containing L gets sixteen. If it does not contain L, two of its affine cosets meet the selected two L-lines in at most four points and cannot cover all seven points there. Its capture is at most fifteen, below its right-hand side $31/2$. Zero and full kernels are immediate.

One external point: $j = 1$**.** The fifteen-point core contains at least thirteen cube vertices, so its captures at $h = 1, 2, 3$ are bounded by $6, 10, 15$. At $h = 4$ its modified capture is sixteen. Hence

$$b_2(T/H) + \mathbf{1}_{H=U} \leq 2 + \tfrac{13}{3}h.$$

The external point is an affine coloop. Lemma 2.2 gives $y_V = 1$, $y_U = 10/3$, of cost $55/3$.

Two external points: $j = 2$**.** The fourteen-point core contains at least thirteen cube vertices. Its single-fiber and two-fiber bounds are $\min(14, 2^h+1)$ and $\min(14, 2^{h+1}+1)$; at $h = 0$ the two-fiber capture is exactly two. If the external quotient vectors have rank two, they are independent affine coloops. The modified core coefficient four suffices, and Lemma 2.2 gives $y_V = 1$, $y_U = 3$, of cost eighteen.

If their rank is one, use $y_V = 2$, $y_U = 2$, also of cost eighteen. Its right-hand side is $2 + 4h + 2\delta$. For $\delta = 1$ the core two-fiber bound plus two gives, at $h = 0, \ldots, 4$, the bounds $4, 7, 11, 16, 16$, each at most $4 + 4h$. For $\delta = 0$, no outsider shares a fiber with a core point. At $h = 1, \ldots, 4$, the maximum of two core fibers, one core fiber plus two outsiders, or two outsiders is bounded by $6, 10, 14, 16$, respectively, all at most $2 + 4h$. At $h = 0$ distinctness gives two.

Three external points: $j = 3$**.** The core T consists of thirteen cube vertices. A single core fiber has size at most $\min(13, 2^h)$ and two have total at most $\min(13, 2^{h+1})$. Let $r \in \{1, 2, 3\}$ be the rank of the three nonzero quotient vectors in V/U.

If $r = 3$, the outsiders are independent affine coloops. The modified core coefficient $11/3$ suffices, and Lemma 2.2 gives $y_V = 1$, $y_U = 8/3$, of cost $53/3$.

For $r = 1$ use $y_V = 3$, $y_U = 2/3$; for $r = 2$ use $y_V = 2$, $y_U = 5/3$. In either case the coefficient of h is $11/3$. The following bounds cover all possible h and δ:

r	δ	$h=0$	$h=1$	$h=2$	$h=3$	$h=4$
1	0	2	5	8	13	16
1	1	5	7	11	16	16
2	0	2	4	8	13	15
2	1	4	6	10	15	16
2	2	5	7	11	16	16

Each entry is at most $2 + (11/3)h + 3\delta$ in the rank-one case, or $2 + (11/3)h + 2\delta$ in the rank-two case. For completeness, we justify the counts rather than relying on the table alone. When $\delta = 0$,

no outsider joins a core fiber. Bound the capture by the maximum of two core fibers, one core fiber plus outsiders, and outsiders alone. At rank two at most two outsiders can occupy one fiber, since three in one fiber would have equal quotient vectors, of rank one. These observations give the $\delta = 0$ rows, with $h = 0$ handled by distinctness. For rank one and $\delta = 1$, or rank two and $\delta = 2$, add three to the core two-fiber bound.

In the remaining case $r = 2$, $\delta = 1$, if both selected fibers meet the core, the selected outsider quotient vectors lie in the line $\pi(K) \leq V/U$. At most two of the three lie there, since their total rank is two. Thus use the two-core-fiber bound plus two. If only one selected fiber meets the core, use the single-core-fiber bound plus three. If neither does, use three. Their maxima give the middle rank-two row. This includes oblique kernels as well as coordinate kernels.

The costs for $r = 1, 2$ are $3 \cdot 5 + (2/3) \cdot 4 = 53/3$ and $2 \cdot 6 + (5/3) \cdot 4 = 56/3$. All cases therefore satisfy the required bound. □

Proof of the sharp-family assertion of Theorem 1.4. Translate the cube to U. The thirteen vertices span U by Lemma 6.1. Independence of a, b modulo U makes the added points distinct and gives affine dimension six. The preceding theorem supplies $y_V = 2$, $y_U = 5/3$, of cost $56/3$.

For a matching lower bound, let $H_i \leq U$ be the four coordinate hyperplanes, and $A_1 = \operatorname{span}(a)$, $A_2 = \operatorname{span}(b)$. For every $X \leq V$ put $H = X \cap U$, $h = \dim H$. At least h of the four restricted coordinate functionals are nonzero, since they span H^*. Hence

$$\sum_i \dim(X \cap H_i) \leq 3h.$$

Also U, A_1, A_2 form a direct sum, so

$$\dim(X \cap A_1) + \dim(X \cap A_2) + \tfrac{1}{3} \sum_i \dim(X \cap H_i) \leq \dim X. \tag{7}$$

For each H_i, the core occupies two fibers of sizes between five and eight. The three new points have distinct nonzero quotient vectors modulo U and are singleton H_i-fibers. Thus $b_2(S/H_i) = 13$. In direction A_1, the square $t + \{0, a, b, a + b\}$ supplies two double fibers and all other core points are singleton fibers. Thus $b_2(S/A_1) = 4$, and similarly for A_2.

Multiply any valid certificate inequalities at A_1, A_2 by one and at the H_i by $1/3$. Their total left-hand excess over the intercept is

$$(4 - 2) + (4 - 2) + \frac{4(13 - 2)}{3} = \frac{56}{3}.$$

Applying (7) to each certificate support shows that this is at most its cost. This finite weak-duality argument is valid over infinite fields as well. The matching upper certificate proves the exact optimum. □

Sharpness and coding interpretation. The sharp family is assembled from a thirteen-vertex cube core and an attached square. It rules out a cube-only equality classification for this certificate problem. A coding lower bound requires simultaneous degree, evaluation and agreement constraints in addition to a certificate lower witness.

Proof method. The certificate bounds and coding consequences follow from the analytic arguments given above. Finite computations served as development diagnostics.

AI assistance. OpenAI assistants supported argument development, literature discovery, proof checking and drafting. The named author is responsible for the mathematical arguments and the manuscript.

References

[1] Y. Chen and Z. Zhang, *Explicit Folded Reed–Solomon and Multiplicity Codes Achieve Relaxed Generalized Singleton Bounds*, STOC 2025. arXiv:2408.15925v3, April 14, 2025; first version August 28, 2024.

[2] J. Brakensiek, Y. Chen, M. Dhar and Z. Zhang, *Combinatorial Bounds for List Recovery via Discrete Brascamp–Lieb Inequalities*, full version of STOC 2026 extended abstract. arXiv:2510.13775v2, October 11, 2026; first version October 15, 2025.

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

[4] J. Brakensiek, Y. Chen, M. Dhar and Z. Zhang, *From Random to Explicit via Subspace Designs With Applications to Local Properties and Matroids*, STOC 2026. arXiv:2510.13777v1, October 15, 2025.

[5] Y. Chen, M. Cheraghchi, K.-S. Si and Z. Zhang, *Evidence Toward a Conjecture in List Recoverability of Folded Reed–Solomon Codes*, manuscript, 2025. Bibliographic details and the reported binary zero-error result are given in [2].

[6] R. Goyal and V. Guruswami, *Structure Theorems (and Fast Algorithms) for List Recovery of Subspace-Design Codes*, arXiv:2512.08017v1, December 8, 2025.

[7] S. Schubr, *Independent Squares and Average-Radius Obstructions for Linear Codes*, Luminary Research Archive, author-published edition 1 (2026). `https://research.luminaryoddities.com/independent-squares-average-radius-obstructions-linear-codes/v/1`.