Counterexamples to the fine-grained list-recovery conjecture for folded Reed–Solomon codes

Scott Schubr
Luminary Oddities

Abstract

We give counterexamples to the fine-grained list-recovery conjecture of Chen and Zhang for folded Reed–Solomon codes. For every fixed input-list size $\ell \geq 3$ and integer $a \geq 3$, and for input-list size two with $a \geq 4$, we construct ℓ^a distinct codewords that each meet a common error radius strictly below the conjectured threshold for output cap $\ell^a - 1$. For each fixed pair (ℓ, a) this happens at every rational rate in an explicit interval $(0, R_0)$, with arbitrarily large folding and arbitrarily large length; the evaluation points form the usual consecutive full-length sequence. The construction combines coordinate-square message sets with blocks on which every selected message has a distinct symbol. An elementary degree-scheduling argument assigns the remaining input tables to equalize all individual errors. Polynomial identities and Vandermonde determinants realize the required evaluation kernels. As a concrete instance, sixteen codewords each have error $55/64$ at exact rate $1/79$, violating the conjectured ordinary cap-fifteen tradeoff with fixed positive slack.

1 Introduction and statements

List recovery asks how many codewords can agree with a small list of allowed symbols at each coordinate. In its ordinary version each recovered codeword must meet the error threshold individually; that is the version considered throughout this paper.

Chen and Zhang [3, Conjecture 3.6] proposed a precise tradeoff for folded Reed–Solomon codes [4] when the output cap plus one is a power of the input-list size, and showed with a hypercube-like message configuration that the conjectured radius cannot be exceeded [3, Theorem 3.1]. Brakensiek, Chen, Dhar and Zhang [1] proved the zero-error case, restated the positive-error question as their Conjecture 1.3, and call it the fine-grained question [1, Remark 1.7]; the case of input-list size two and output cap three is proved in [3, Theorem 1.8] (see [1, Remark 1.7]). For every pair (ℓ, a) in the region of Theorem 1.2 we disprove that tradeoff at all rates in an explicit interval $(0, R_0)$. An earlier note [5] introduced the configuration of independent coordinate squares sharing an origin, realized it in standard full-length folded Reed–Solomon codes, and used it to rule out the average-radius extrapolation of the conjectured curve at output cap fifteen; it left the ordinary conjecture open. The new ingredient here is the injective padding and degree scheduling of Section 3, which equalizes every individual error and so yields ordinary counterexamples, together with the extension to every (ℓ, a) in (3).

The mechanism has two parts. Several coordinate squares sharing one origin give large local captures, but initially produce unequal individual agreements. We then add evaluation-block types on which the selected messages have distinct symbols. At those blocks any ℓ selected messages can be chosen by an input table. Prescribed degree sequences in uniform multihypergraphs distribute these choices so that every message reaches the same agreement count. Filling remaining coordinates

evenly is already used in the upper-bound construction of Chen–Zhang [3, Section 3.1]; what is new is a schedule over injective blocks that balances unequal deficits from a different message geometry. An exact polynomial construction supplies all the special and injective block types in the ordinary consecutive full-length code.

1.1 The code and the conjecture

Let q be a prime power, let γ generate $\mathbb{F}_q^\times$, and let s, n, k be positive integers with $q > sn > k$. The message space consists of the polynomials $f \in \mathbb{F}_q[X]$ of degree less than k. Its consecutive s-folded encoding is

$$E_r(f) = \big(f(\gamma^{sr}), \dots, f(\gamma^{sr+s-1})\big), \qquad 0 \le r < n. \tag{1}$$

The rate over the alphabet $\mathbb{F}_q^s$ is $R = k/(sn)$. Following [3, Definition 1.2], evaluation points $\alpha_1, \dots, \alpha_n$ are *appropriate* if the sn elements $\gamma^i \alpha_j$ $(0 \le i < s)$ are distinct. In all our examples $\alpha_{r+1} = \gamma^{sr}$ and $sn = q - 1$, so the unfolded points γ^{sr+i} run through the nonzero field elements exactly once and are appropriate.

An input table is a sequence $\mathcal{T} = (\mathcal{T}_r)_{r=0}^{n-1}$ with $\mathcal{T}_r \subseteq \mathbb{F}_q^s$ and $|\mathcal{T}_r| \le \ell$. The relative error of a message is

$$\mathrm{err}_{\mathcal{T}}(f) = \frac{1}{n}\big|\{r : E_r(f) \notin \mathcal{T}_r\}\big|.$$

The code is (ρ, ℓ, L) list recoverable if, for every such table, at most L messages have error at most ρ. For $M = \ell^a$, define

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

Conjecture 1.1 (Chen–Zhang [3, Conjecture 3.6])**.** *Let $\ell \ge 2$ and $a \ge 2$ be integers, put $L+1 = \ell^a$, and fix $\varepsilon > 0$, a rate $R \le (a-1)/a$, and a generator γ. There is a constant C_0 such that, if $s \ge C_0$, $(k-1)/s \ge a$ and n is sufficiently large, then every rate-R folded Reed–Solomon code with appropriate evaluation points is $(\Phi_{\ell,a}(R) - \varepsilon, \ell, L)$ list recoverable.*

The conjecture quantifies over every code with appropriate evaluation points, and C_0 may depend on ε, ℓ, a, R and γ. It is therefore refuted by exhibiting, for one fixed (ℓ, a, R) with $R \le (a-1)/a$ and one fixed $\varepsilon > 0$, codes with arbitrarily large folding s and, for each such s, arbitrarily large length and $(k-1)/s \ge a$, for every choice of generator, that contain $L+1$ messages of error at most $\Phi_{\ell,a}(R) - \varepsilon$ against some table. The reformulation [1, Conjecture 1.3] puts the slack in the rate instead; since $\Phi_{\ell,a}$ is linear and strictly decreasing, a radius slack ε is the same as a rate slack $(a-1)M\varepsilon/(a(M-\ell))$, and all errors below are at most $1 - \ell/M$, so the strict violations below refute both forms.

1.2 Parameters and results

Fix integers ℓ, a with

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

and put

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

$$C = (\ell - 1)(2\ell t + c), \qquad B = \frac{a(M - \ell)}{a - 1}. \tag{4}$$

Section 3 shows that t is a positive integer and $C > B$.

Theorem 1.2. *Fix integers ℓ, a such that either $\ell \geq 3$, $a \geq 3$, or $\ell = 2$, $a \geq 4$, and put $M = \ell^a$. There is an explicit rational $R_0 = R_0(\ell, a) > 0$ such that the following holds for every rational rate $R \in (0, R_0)$. There are a rational $\varepsilon = \varepsilon(\ell, a, R) > 0$ and an integer $s_0 = s_0(\ell, a)$ such that, for every integer $s \geq s_0$, there are arbitrarily large prime powers q and consecutive full-length folded Reed–Solomon codes of rate exactly R, together with tables of exactly ℓ symbols per block and M distinct messages, each satisfying*

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

The codes satisfy $q = sn + 1$, $k < sn$, and $(k-1)/s \geq a$ for all sufficiently large members of each fixed-s family. One may take $R_0 = C/(BD_0)$ with $D_0 = \max\{\lceil (Md - C)/\ell \rceil, \lfloor B/(C - B) \rfloor + 1\}$ in the notation of Section 1.2; for example $R_0(2, 4) = 3/196$ and $R_0(3, 3) = 19/918$.

Thus every indicated fixed parameter instance of the conjecture fails at every sufficiently small fixed rate, each with its own fixed positive slack. The parameters ℓ, a are fixed before the folding and length quantifiers. Proposition 3.3 in Section 3 compares the resulting error with the optimal list-recovery radius.

Theorem 1.3 (A numerical cap-fifteen instance)**.** *For every integer $s \geq 10$ there are arbitrarily long consecutive full-length folded Reed–Solomon codes of exact rate $1/79$ and tables of exactly two symbols per block for which sixteen distinct messages each have relative error $55/64$. At this rate,*

$$\Phi_{2,4}(1/79) - \frac{55}{64} = \frac{13}{15168} > \frac{1}{10000},$$

so these codes are not $(55/64 + 1/10000,\ 2,\ 15)$ list recoverable.

The rate $1/79$ lies in $(0, R_0(2, 4))$, so Theorem 1.2 also covers it; Theorem 1.3 records the instance with a direct pair schedule and explicit constants. We first realize prescribed axis kernels and injective blocks by polynomials (Section 2), then prove Theorem 1.2 (Section 3) and Theorem 1.3 (Section 4).

2 A full-length realization with injective padding blocks

The following elementary polynomial construction supplies both axis-kernel blocks and blocks injective on the entire message configuration.

Lemma 2.1 (Polynomial realization)**.** *Fix integers $D > d \geq 1$ and $s \geq d$. Suppose $q - 1 = Dsm$, where m is a positive integer, and let γ generate $\mathbb{F}_q^\times$. Set $n = Dm$, $\delta = \gamma^m$, and, for $0 \leq i < D$, define*

$$\theta_i = \delta^{si}, \tag{5}$$

$$P_i(Y) = \prod_{u=0}^{s-1} (Y - \delta^{si+u}), \qquad p_i(X) = P_i(X^m). \tag{6}$$

Use the consecutive folded evaluations (1). The polynomials $p_0, \ldots, p_{d-1}$ are independent, and, on $V = \mathrm{span}_{\mathbb{F}_q}\{p_0, \ldots, p_{d-1}\}$,

$$\ker(E_{i+Dj}|_V) = \begin{cases} \mathbb{F}_q p_i, & 0 \leq i < d, \\ \{0\}, & d \leq i < D, \end{cases} \qquad 0 \leq j < m. \tag{7}$$

Every p_i has degree sm.

Proof. The element δ has order Ds. To establish independence without any characteristic restriction beyond the existence of this root of unity, write

$$P_0(Y) = \sum_{r=0}^{s} (-1)^r e_{s,r} Y^{s-r}.$$

The finite geometric-product identity gives

$$e_{s,r} = \delta^{r(r-1)/2} \prod_{u=0}^{r-1} \frac{1-\delta^{s-u}}{1-\delta^{r-u}}, \qquad 0 \le r \le s, \tag{8}$$

where the empty product is one. For completeness, the coefficients in $\prod_{u=0}^{s-1}(1+\delta^u T)$ obey $e_{s,r} = e_{s-1,r} + \delta^{s-1} e_{s-1,r-1}$, with zero terms outside the coefficient range. The displayed products satisfy this recurrence: after removing $\delta^{r(r-1)/2}$, it is the identity

$$\begin{bmatrix} s \\ r \end{bmatrix}_\delta = \begin{bmatrix} s-1 \\ r \end{bmatrix}_\delta + \delta^{s-r} \begin{bmatrix} s-1 \\ r-1 \end{bmatrix}_\delta,$$

whose product verification reduces to $1-\delta^s = (1-\delta^{s-r}) + \delta^{s-r}(1-\delta^r)$. Here the bracket denotes the product in the preceding coefficient formula without its power of δ. The boundary values and induction prove (8). All numerator and denominator factors are nonzero, since their positive exponents are at most $s < Ds$. In particular every coefficient of P_0 is nonzero in $\mathbb{F}_q$.

The scaling relation $P_i(Y) = \theta_i^s P_0(Y/\theta_i)$ shows that its coefficient of Y^{s-r} is $(-1)^r e_{s,r}\theta_i^r$. The D parameters θ_i are distinct, since δ^s has order D. On any $d+1$ selected columns, the coefficient rows $r = 0, \dots, d$ form an invertible diagonal matrix times a Vandermonde matrix. Thus any $d+1$ of the P_i are independent. Substitution $Y = X^m$ preserves linear independence.

Write $r = i + Dj$. For an unfolded point in that block,

$$(\gamma^{s(i+Dj)+u})^m = \delta^{si+u},$$

because δ has order Ds. Hence every polynomial $P(X^m)$ has the same evaluation on the m replicas of type i. A polynomial P of degree at most s vanishes on the s distinct points $\delta^{si}, \dots, \delta^{si+s-1}$ if and only if P is a scalar multiple of P_i: its monic root product has degree s and divides P. For $i < d$ this gives the asserted axis kernel on V. For $i \ge d$, the span of $P_0, \dots, P_{d-1}$ has zero intersection with $\mathbb{F}_q P_i$, by the $d+1$ independence. This proves (7). □

Since the $sn = q-1$ unfolded points are distinct, the encoding is injective for every $k \le q-1$, and the rate is $k/(sn)$. Whenever $sm < k \le sn$, all of V lies in the message space. For a finite set of distinct messages in V, every type $i \ge d$ is injective, so a table consisting of the evaluations of any chosen ℓ distinct messages captures exactly those ℓ messages from that set.

3 All higher power caps

Throughout this section (ℓ, a) satisfies (3) and M, N, c, t, d, C, B are as in Section 1.2. All parameters are fixed before taking field-size or length limits. The integer t is positive: reducing $N = 1 + \ell + \cdots + \ell^{a-1}$ modulo $\ell+1$ gives remainder c. In particular $1 + t(\ell^2-1) + c(\ell-1) = M$. Elementary expansion gives

$$C = \frac{2\ell(M-1) - c(\ell-1)^2}{\ell+1} < 2M, \tag{9}$$

$$(C-B)(\ell+1)(a-1) = \begin{cases} [a(\ell-1)-2\ell]M + \ell[a(\ell-1)+2], & a \text{ even}, \\ [a(\ell-1)-2\ell]M + a(\ell-1) + \ell^2 + 1, & a \text{ odd}. \end{cases} \tag{10}$$

In (3), the coefficient $a(\ell-1)-2\ell$ is nonnegative and the remaining term is positive. Thus $C > B$. For $a = 2$ and for $(\ell, a) = (2, 3)$ the two constants are equal.

Lemma 3.1 (Uniform subset scheduling)**.** *Let $G \geq 0$ and let nonnegative integers $(z_v)_{v\in S}$ satisfy $\sum_v z_v = \ell G$ and $\max_v z_v \leq G$. Then there is a multiset of G subsets of S, each of size exactly ℓ, in which vertex v occurs exactly z_v times.*

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

Proposition 3.2 (Ordinary padding at every higher power cap)**.** *Let $D \geq (Md - C)/\ell$ be an integer, let $s \geq d$, and let $q \geq \ell$ be a prime power with $DsM \mid q - 1$. Put $m = (q - 1)/(Ds)$ and $n = Dm$, and let k be any integer with $sm < k \leq sn$. The consecutive full-length s-folded code of dimension k contains M distinct messages and a table of exactly ℓ symbols at every block against which every message has exactly $m(\ell D + C)/M$ agreements, that is, agreement fraction*

$$\tau_D = \frac{\ell D + C}{MD}.$$

Proof. Apply Lemma 2.1. It supplies independent degree-sm polynomials $p_0, \ldots, p_{d-1}$ spanning V, with kernel $\mathbb{F}_q p_i$ on special type $i < d$ and zero kernel on every other type; each type has m blocks. Since $k > sm$, V lies in the message space.

Choose $A \subseteq \mathbb{F}_q$ of size ℓ, containing $0, 1$. No subfield assumption is made. In each of the t coordinate planes put an $A \times A$ square, sharing only the origin, and on the possible remaining axis put an A-line:

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

Independence makes all these messages distinct, so $|S| = M$.

At special type $2h$, use the ℓ symbols $E_{2h}(\beta p_{2h+1})$, $\beta \in A$; at type $2h + 1$, use $E_{2h+1}(\alpha p_{2h})$, $\alpha \in A$. The symbols are distinct because the kernel is the corresponding other coordinate axis. The selected fibers capture precisely the ℓ^2 square messages: its zero fiber is the A-axis, and its other fibers are the parallel A-lines. No message in another square or on the remaining axis line can enter one of these fibers, by coordinate independence.

If $c = 1$, at its special axis use symbol zero and the $\ell - 1$ symbols $E_i(\beta p_0)$, $\beta \in A \setminus \{0\}$. The zero fiber consists of the ℓ messages of the remaining axis line. Each other selected fiber contains the single message βp_0: there are no messages in S combining a square with the remaining axis. These symbols are distinct, again by the exact kernel. This table therefore captures exactly $2\ell - 1$ messages. Here $t \geq 1$ ensures the required square containing p_0.

Let h_v count the special types capturing message v. Then

$$0 \leq h_v \leq d, \qquad \sum_{v\in S} h_v = 2t\ell^2 + c(2\ell - 1) = \ell d + C. \tag{11}$$

After their m replicas, message v has mh_v agreements. There are $G = (D - d)m$ generic blocks. Prescribe additional degrees

$$z_v = m\left(\frac{\ell D + C}{M} - h_v\right). \tag{12}$$

Since $M \mid m$, these are integers. They are nonnegative because $\ell D + C \geq Md$ gives $(\ell D + C)/M \geq d \geq h_v$; the origin has $h_v = d$. For the upper bound, every message has $h_v \geq 1$, so it suffices that $(\ell D + C)/M - 1 \leq D - d$, that is $(M - \ell)D \geq Md + C - M$. In the region (3) one has $d \geq 7$ and $M/\ell \geq 4$. Put $x = Md - C$; then $x \geq M(d-2) \geq 5M$ by (9), and $\ell D \geq x$ gives

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

Also $D > d$, since $x > \ell d$. Hence $z_v \leq G$. Equation (11) yields $\sum_v z_v = \ell G$. Lemma 3.1 supplies G subsets of ℓ distinct messages with those degrees. Assign them to the generic blocks. Each generic evaluation is injective on V, so its assigned subset provides exactly ℓ distinct table symbols and captures precisely those messages. Every message now has the same number of agreements,

$$mh_v + z_v = \frac{m(\ell D + C)}{M} = n\tau_D. \qquad \square$$

Proof of Theorem 1.2. Put $D_0 = \max\{\lceil (Md - C)/\ell \rceil, \lfloor B/(C - B) \rfloor + 1\}$ and $R_0 = C/(BD_0)$. For $D \geq D_0$ we have $D(C - B) > B$, that is $1/D < C/(B(D+1))$, so the windows $(1/D,\, C/(BD))$ with $D \geq D_0$ cover $(0, R_0)$. Let $R = \nu/\omega \in (0, R_0)$ in lowest terms, and choose $D \geq D_0$ with $1/D < R < C/(BD)$. Let $s \geq s_0 := d$. Pick a prime π not dividing $DsM\omega$ and put $q = \pi^{\varphi(DsM\omega)\lambda}$ for integers $\lambda \geq 1$; Euler's theorem gives $DsM\omega \mid q-1$, and $q \geq \ell$ for large λ. Then $m = (q-1)/(Ds)$ is divisible by M and by ω, so $k = Rsn = \nu s D m/\omega$ is an integer. Moreover $k > sm$ because $RD > 1$, and $k < sn$ because $R < 1$; the code has rate exactly R. By Proposition 3.2, its M messages all have error $1 - \tau_D$, while

$$\Phi_{\ell,a}(R) - (1 - \tau_D) = \frac{1}{M}\Big(\frac{C}{D} - BR\Big) > 0.$$

Taking ε to be one third of this quantity proves the displayed inequality. As $\lambda \to \infty$ with s fixed, $m \to \infty$ and $(k-1)/s > m - 1/s \to \infty$, which gives arbitrarily large length and the eventual condition $(k-1)/s \geq a$. Every such R satisfies $R < R_0 \leq C\ell/(Bx) < 2\ell/(5B) \leq 2/15 < (a-1)/a$, by (9), $\ell D_0 \geq x \geq 5M$ and $B \geq M - \ell \geq 3\ell$. Finally $C/(BD_0)$ is rational and $R_0(2,4) = 3/196$, $R_0(3,3) = 19/918$ follow from $(C, B, D_0) = (20, 56/3, 70)$ and $(38, 36, 51)$. $\square$

Proposition 3.3. *Fix (ℓ, a) as in Theorem 1.2. For every rational R with $0 < R \leq 1/(Md-1)$, the codes of Proposition 3.2 at rate exactly R, built with $D = \lfloor 1/R \rfloor + 1$ and the field choice in the proof of Theorem 1.2, contain M messages each of error exactly*

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

Compared with the optimal large-alphabet radius $(L + 1 - \ell - LR)/(L+1)$ of [2], with $L + 1 = M$, this error is smaller by at least $\big(C/(1+R) - (M-1)\big)R/M$, which is positive for these R.

Proof. With $D = \lfloor 1/R \rfloor + 1$ we have $RD > 1$ and $D \geq Md$, so Proposition 3.2, with the field choice in the proof of Theorem 1.2, applies at rate exactly R. It gives agreement fraction $(\ell D + C)/(MD)$, and $1/D \geq R/(1+R)$. Positivity follows from $C/(M-1) > 1 + R$, which holds since $C/(M-1) \geq 4/3 - 1/(3(M-1)) \geq 4/3 - 1/45$ by (9) (for $\ell = 2$ this is the formula with $c \leq 1$; for $\ell \geq 3$ the main term is at least $3/2$ and the subtracted term is at most $(\ell-1)^2/((\ell+1)(\ell^3-1)) < 1/6$), while $Md \geq 160$ in the stated region gives $R \leq 1/159$. $\square$

Remark 3.4. For fixed (ℓ, a), as $R \to 0$, the conjectured curve, this construction and the optimal radius have slopes B/M, C/M and $(M-1)/M$ in R. The upper bound construction of Chen and

Zhang [3, Theorem 3.1] already shows that folded Reed–Solomon codes miss the optimal slope by the factor $B/(M-1)$, which tends to 1 as $a \to \infty$. The factor here is

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

which tends to $2\ell/(\ell+1)$. The range $R \le 1/(Md-1)$ on which Proposition 3.3 applies depends on a. List-size barriers for linear codes near capacity are treated in [2, Fact 1.4].

4 Proof of Theorem 1.3

Proposition 3.2 also applies with $D = 80$; here a direct pair schedule with explicit multiplicities replaces Lemma 3.1.

Proof of Theorem 1.3. Apply Lemma 2.1 with $D = 80$, $d = 10$ and m divisible by $84 \cdot 79$. Set $n = 80m$ and

$$k = \frac{80sm}{79}, \qquad V = \operatorname{span}\{p_0, \dots, p_9\}.$$

Then $k - sm = sm/79 \ge 1$, so these polynomials belong to the message space, and $k/(sn) = 1/79$. Use the sixteen messages

$$S = \{0\} \ \cup \bigcup_{h=0}^{4} \{p_{2h}, p_{2h+1}, p_{2h} + p_{2h+1}\}. \tag{13}$$

They are distinct because the ten axes are independent. Encoding is injective, so their codewords are distinct too.

At a block $r = i + 80j$ with $0 \le i < 10$, let i' be the other index in its pair $\{2h, 2h+1\}$ and choose the two-symbol table

$$\mathcal{T}_r = \{0, E_r(p_{i'})\}.$$

The second symbol is nonzero by the axis-kernel statement. Within S, its zero fiber consists exactly of $0, p_i$, and its other chosen fiber consists exactly of $p_{i'}, p_i + p_{i'}$. Indeed evaluation equality is equivalence modulo the line $\mathbb{F}_q p_i$, and independent coordinates exclude any other message. Thus the origin agrees at all $10m$ special blocks. Each of the fifteen other messages agrees at exactly the two types of its own square, contributing $2m$ agreements.

There remain $70m$ blocks, all injective on V. At each such block a table made from the evaluations of two distinct members of S captures exactly those two members. Assign unordered pairs of members to these blocks using the following multiplicities:

pair type	number of pairs	multiplicity per pair
origin and a nonzero message	15	$m/12$
two nonzero messages	105	$55m/84$.

All multiplicities are integral. Their sum is

$$\frac{15m}{12} + 105\frac{55m}{84} = 70m,$$

so assign the pair occurrences bijectively to the generic blocks and use their two evaluations as the tables. The origin gains $5m/4$ agreements. Each nonzero message gains

$$\frac{m}{12} + 14\frac{55m}{84} = \frac{37m}{4}.$$

Every message therefore has exactly

$$10m + \frac{5m}{4} = 2m + \frac{37m}{4} = \frac{45m}{4}$$

agreements, or agreement fraction $9/64$ out of $80m$ blocks. Every individual error is $55/64$.

To obtain the field and length quantifiers, fix $s \geq 10$ and put $H = 80s \cdot 84 \cdot 79$. Choose a prime π not dividing H, and for integers $\lambda \geq 1$ take

$$q = \pi^{\varphi(H)\lambda}.$$

Euler's theorem gives $H \mid q-1$. Thus $m = (q-1)/(80s)$ is divisible by $84 \cdot 79$, and the construction applies. As $\lambda \to \infty$ its lengths tend to infinity, with s fixed. The argument works for any choice of generator. The unfolded points comprise all $q - 1 = sn$ nonzero field elements, so the evaluations are appropriate and $q > sn > k$. Also $(k-1)/s \geq 4$ for sufficiently large length.

At rate $1/79$,

$$\Phi_{2,4}(1/79) - \frac{55}{64} = \frac{7}{8} - \frac{7}{6 \cdot 79} - \frac{55}{64} = \frac{13}{15168} > \frac{2}{10000}.$$

Hence with $\rho_\circ = 55/64 + 1/10000$ all sixteen messages have error below $\rho_\circ < \Phi_{2,4}(1/79) - 1/10000$, and the codes are not $(\rho_\circ, 2, 15)$ list recoverable. Since s may first be chosen above any finite folding threshold and then λ taken arbitrarily large, this contradicts Conjecture 1.1 at fixed positive slack. □

For the rate-slack reformulation [1, Conjecture 1.3], the threshold at radius ρ is $R^*(\rho) = \frac{3}{4}(1 - 8\rho/7)$, and

$$R^*(\rho_\circ) - \frac{1}{79} = \frac{6}{7}\left(\frac{13}{15168} - \frac{1}{10000}\right) > \frac{1}{10000}.$$

Thus the example also lies strictly inside that formulation's conjectured region.

5 Scope of the results

The counterexamples hold at every rational rate in $(0, R_0)$, with $R_0(2,4) = 3/196$ and $R_0(3,3) = 19/918$, and the sixteen-message instance has slack $13/15168$. The rate range is set by the requirement $\ell D + C \geq Md$, which keeps the origin's deficit nonnegative. The region (3) consists exactly of the pairs (ℓ, a) with $C > B$; for $a = 2$ and for $(\ell, a) = (2, 3)$ the square configuration gives $C = B$, and the case $(\ell, a) = (2, 2)$ of the conjecture is proved in [3, Theorem 1.8] (see [1, Remark 1.7]).

Assistance and data availability

AI-assisted tools were used in mathematical exploration and manuscript preparation. The mathematical arguments are contained in this article. The construction uses no numerical experiment or external dataset.

References

[1] J. Brakensiek, Y. Chen, M. Dhar and Z. Zhang, *Combinatorial Bounds for List Recovery via Discrete Brascamp–Lieb Inequalities*, full version of the STOC 2026 extended abstract, arXiv:2510.13775v2, 11 October 2026. `https://arxiv.org/abs/2510.13775v2`.

[2] J. Brakensiek, Y. Chen, A. Putterman and Z. Zhang, *Bounds and Limitations on Codes Achieving List Recovery Capacity*, full version of the SODA 2027 extended abstract, arXiv:2607.19576v2, 9 October 2026. `https://arxiv.org/abs/2607.19576v2`.

[3] Y. Chen and Z. Zhang, *Explicit Folded Reed–Solomon and Multiplicity Codes Achieve Relaxed Generalized Singleton Bounds*, STOC 2025; arXiv:2408.15925v3, 14 April 2025. `https://arxiv.org/abs/2408.15925v3`.

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

[5] S. Schubr, *Independent Squares and Average-Radius Obstructions for Linear Codes*, Luminary Research Archive, edition 2, 27 October 2026. `https://research.luminaryoddities.org/independent-squares-average-radius-obstructions-linear-codes/v/2`.