Electronic Colloquium on Computational Complexity, Report No. 317 (2026)

Explicit Subspace Evasive Sets via Subspace Designs

Joshua Brakensiek* Yeyuan Chen† Mahdi Cheraghchi‡ Rohan Goyal§
Venkatesan Guruswami¶ Aaron Putterman‖ Zihan Zhang **

October 2026

Abstract

Given a finite field $\mathbb{F}_q$, we say that a set $A \subseteq \mathbb{F}_q^n$ is an (r, c) subspace evasive set if and only if for any affine subspace $U \subseteq \mathbb{F}_q^n$ with bounded dimension $\dim(U) \leq r$, the intersection size $|A \cap U|$ is at most c. The probabilistic method shows the existence of (r, c) subspace evasive sets with $|A| = q^{(1-\epsilon)n}$ with $c = O(r/\epsilon)$. However, the best explicit constructions by Dvir–Lovett (STOC 2012) and Ben-Aroya–Shinkar (CJTCS 2013) have c growing as an exponential function of r.

Here, we give an explicit construction of such subspace evasive set that achieves the intersection bound $c = O(\min(r \log(r/\epsilon)/\epsilon, r^2/\epsilon))$ when both r and $1/\varepsilon$ are constants. Our approach is simple and the key idea is to compose subspace design codes (Guruswami-Xing, STOC 2013) with a suitably chosen "local" subspace evasive set. As a corollary, we give the first construction of an explicit (strongly) capacity-achieving list-recoverable code with nearly optimal list size, circumventing all previously-known barriers to construction.

*University of California, Berkeley, CA, USA. Email: josh.brakensiek@berkeley.edu. Research supported in part by Venkatesan Gurusawmi's Simons Investigator award and NSF grants CCF-2211972 and DMS-2503280.

†University of Michigan, Ann Arbor, MI, USA. Email: yeyuanch@umich.edu. Research partially supported by the National Science Foundation under Grant No. CCF-2236931.

‡University of Michigan, Ann Arbor, MI, USA. Email: mahdich@umich.edu. Research partially supported by the National Science Foundation under Grant No. CCF-2236931.

§Massachusetts Institute of Technology, Cambridge, MA, USA. Email: rohan_g@mit.edu. Research supported by Yael Tauman Kalai's NSF Award 6956054.

¶Department of Electrical Engineering and Computer Sciences, Department of Mathematics, and the Simons Institute for the Theory of Computing, UC Berkeley, Berkeley, CA 94709, USA. Email: venkatg@berkeley.edu. Research supported in part by a Simons Investigator Award, a UC Noyce initiative award, DOD Advanced Research Projects Agency grant HR0011262E031, and NSF grant 2211972.

‖Harvard University, Cambridge, MA, USA. Supported in part by a Jane Street Graduate Research Fellowship, the Simons Investigator Awards of Madhu Sudan and Salil Vadhan, and AFOSR award FA9550-25-1-0112. Email: aputterman@g.harvard.edu.

**Simons Institute for the Theory of Computing, University of California Berkeley, Berkeley, CA, USA. Email: zihanz@hku.hk.

ISSN 1433-8092

1 Introduction

In this work, we study *explicit* constructions of subspace evasive sets, a fundamental object with connections to pseudorandomness, coding theory, and Ramsey theory. Formally, given a finite field $\mathbb{F}_q$, we say that a set $A \subseteq \mathbb{F}_q^n$ is an (r, c) subspace evasive set if and only if for any affine subspace $U \subseteq \mathbb{F}_q^n$ with bounded dimension $\dim(U) \leq r$, the intersection size $|A \cap U|$ is at most c. Intuitively, the set A should have minimal overlap with any low-dimensional affine space. As a classical example, the case $r = 1$ corresponds to finding a collection of points in $\mathbb{F}_q^n$ such that no $c + 1$ points lie on the same line; the case $r = 2$ corresponds to no $c + 1$ points lying in the same plane, and so forth.

This notion was first introduced by Pudlák and Rödl [PR04], motivated by an application to bipartite Ramsey graphs. Specifically, they showed that an explicit construction of an $(n/2, c)$ subspace evasive set $A \subseteq \mathbb{F}_2^n$ can be used to construct explicit c-Ramsey bipartite graphs with $|A|$ vertices (where a c-Ramsey bipartite graph is a bipartite graph with no empty or complete c by c subgraph). Using this connection, they gave the first construction of $o(\sqrt{N})$-Ramsey bipartite graphs on N vertices.[1]

Inspired by this initial line of work, many subsequent works extended the study of subspace evasive sets and found concrete applications of subspace evasive sets to other areas in theoretical computer science. For instance, the work of Guruswami [Gur11] showed that explicit constructions of subspace evasive sets with good quality lead to explicit list decodable/recoverable codes. Subsequently, Dvir and Lovett [DL12] gave explicit subspace evasive sets which when plugged into [Gur11, GW13] gave capacity-achieving list-decodable codes with $O(1)$ list-size. These subspace evasive sets also played a crucial role in the design of better affine extractors [BR15] and even in combinatorics [ST24]. In this work, we *reverse* some of these established connections, and show that recent work in designing better list-recoverable codes actually leads to much-improved explicit subspace evasive sets.

To make our discussion more concrete, let us fix $0 < \varepsilon < 1$ and $r \geq 1$. Our goal in this paper is to design explicit (r, c) subspace evasive sets $A \subseteq \mathbb{F}_q^n$ with size at least $|A| \geq q^{(1-\varepsilon)n}$, while ensuring that c is as small as possible. As a simple baseline, one can consider what happens when we select A *uniformly at random*. By a simple probabilistic argument (see, for instance, Lemma 8 of [Gur11]), if one samples A of size $q^{(1-\varepsilon)n}$ in this way, one can show that it will be a $(r, O(r/\varepsilon))$ subspace evasive set with high probability. Complementing this, the work of Sudakov and Tomon [ST24, Theorem 1.1] shows that there is a matching lower bound. Indeed, any A with size $q^{(1-\varepsilon)n}$ *cannot* be an $(r, o(r/\varepsilon))$ subspace evasive set when $\varepsilon < 1/20$ and $r = (1 + \Omega(1)) \log_2(1/\varepsilon)$. Thus, for most regimes, the *optimal* (r, c)-subspace evasive sets have $c = O(r/\varepsilon)$.

The central question in the study of subspace evasive sets is the pursuit of *explicit* constructions, where one can algorithmically determine the elements of our subspace evasive set $A \subseteq \mathbb{F}_q^n$ efficiently. Motivated by the broad applications in [PR04, Gur11], and the hope that better explicit subspace evasive sets can lead to downstream explicit constructions of other combinatorial objects we pose the following challenge:

Question 1. *Can we provide explicit constructions of $(r, c(r, \varepsilon))$ subspace evasive set $A \subseteq \mathbb{F}_q^n$ with size at least $|A| \geq q^{(1-\varepsilon)n}$, ideally matching the probabilistic method bound of $c(r, \varepsilon) = O(r/\varepsilon)$?*

In the special case $r = 1$, Führer and Taranchuk [FT24] construct a $(1, O(\sqrt{1/\varepsilon}))$ subspace

[1] The problem has since seen major progress with other approaches and we now know explicit $(\log N)^{O(1)}$-Ramsey bipartite graphs; still a near-optimal explicit subspace-evasive set in $\mathbb{F}_2^n$ would be a very pleasing way to construct $\Theta(\log N)$-Ramsey bipartite graphs. [CZ16, Li23]

evasive set, which is actually better than what can be guaranteed by the probabilistic method. In the general case, the pioneering work of Dvir and Lovett [DL12] gives explicit constructions with $c(r,\varepsilon) = (\frac{r}{\varepsilon})^r$, and follow-up work due to Ben-Aroya and Shinkar [BS14] refines this bound to $c(r,\varepsilon) = (\frac{2}{\varepsilon})^r$ when r and ε are both constants.

For general r, there has been little progress on Question 1 in the last decade; however, we invite the reader to Section 1.2 for discussion of many related works. As mentioned above, the main contribution of our work is to give explicit constructions of *near-optimal* $(r, c(r,\varepsilon))$ subspace evasive sets.

Theorem 2 (Main Theorem, informal, see Section 4)**.** *For any constants $r \geq 1$, $\varepsilon > 0$, for all large enough n, one can explicitly construct an $(r, c(r,\varepsilon))$ subspace evasive set $A \subseteq \mathbb{F}_q^n$ with size $|A| \geq q^{(1-\varepsilon)n}$ and intersection size $c(r,\varepsilon) = O(\min(r^2/\varepsilon, r\log(r/\varepsilon)/\varepsilon))$.*

Our bound on $c(r,\varepsilon)$ exponentially improves upon the previous work and is much closer to the probabilistic method bound of $c(r,\varepsilon) = O(r/\varepsilon)$. In turn, by using the reductions of [Gur11] and its follow-ups in conjunction with our new constructions, we resolve some open problems in coding theory. We elaborate upon these applications and more of our techniques in the following section.

1.1 Our Results and Techniques

For simplicity of presentation, we slightly modify the definition of a subspace evasive set. In particular, we replace the condition on affine sets (as stated in [DL12, FT24]) with subspaces.

Definition 3 (Subspace evasive set [PR04, DL12, GW13])**.** Let $\mathbb{F}$ be a field, a set $A \subseteq \mathbb{F}^n$ is (r,c) subspace evasive if for any subspace $U \subseteq \mathbb{F}^n$ with dimension $\dim(U) \leq r$, we have $|U \cap A| \leq c$.

Equivalently, A is (r,c) subspace evasive set if every subset of A of size more than c has rank more than r. This change of definition is overall mild, as any r-dimensional affine space is contained in an $r+1$-dimensional linear space, so an $(r+1,c)$ subspace evasive set Definition 3 captures the more traditional notion of an (r,c) subspace evasive set. In particular, our asymptotic bounds–such as Question 1–hold in either setting.

At the heart of our results is the notion of *list recovery*. In short, a code $C \subseteq \Sigma^n$ (not necessarily linear) is (ℓ, L) zero-error list-recoverable if for any sets $S_1, \ldots, S_n \subseteq \Sigma$ of size at most ℓ, the set $C \cap (S_1 \times \cdots \times S_n)$ has size at most L. Previously, Guruswami [Gur11] had shown that explicit subspace evasive sets can be used to construct explicit list-recoverable codes with bounded output list-size. Our primary technical contribution is a *constructive converse* that explicit list-recoverable codes in combination with a small "local" subspace evasive set can be used to explicitly construct a large "global" subspace evasive sets.

This relies on a modified notion of list-recoverability which we call *subspace list-recoverability*:

Definition 4 (Subspace list-recoverability)**.** For a local dimension s, and a global dimension n, we say that a code $C \subseteq (\mathbb{F}^s)^n$ is (r, ρ, ℓ, L) subspace list-recoverable if the following holds: for every $\mathbb{F}$-linear subspace $U \subseteq (\mathbb{F}^s)^n$ with $\dim(U) \leq r$, and every choice of $S_1, \ldots S_n \in \binom{\mathbb{F}^s}{\leq \ell}$, we have

$$|\{c \in C \cap U : \exists y \in (S_1 \times \cdots \times S_n), \mathrm{Ham}(c,y) \leq \rho n\}| \leq L.$$

Here $\mathrm{Ham}(c,y) = \sum_{i=1}^n [c_i \neq y_i]$ denotes the Hamming distance.

Intuitively, this is a *weaker* requirement than being a standard (ρ, ℓ, L) list-recoverable code, which requires that for any $S_1, \ldots S_n \in \binom{\mathbb{F}^s}{\leq \ell}$,

$$|\{c \in C : \exists y \in (S_1 \times \cdots \times S_n), \mathrm{Ham}(c,y) \leq \rho n\}| \leq L.$$

Our new definition of *subspace list-recoverability* only requires that after taking an *intersection* with a low-dimensional linear space (albeit an arbitrary one), the resulting code satisfies the ordinary list-recovery guarantee. In particular, any (ρ, ℓ, L) list-recoverable code is also (r, ρ, ℓ, L) list-recoverable for every r. As we shall see, this distinction is particularly useful when constructing subspace evasive sets, as we must only ever bound the number of points that lie in the intersection with a fixed-dimensional subspace.

Key Idea: Composition. The core conceptual insight of this paper is that the *composition* of a subspace list-recoverable code with a "local" subspace evasive set is sufficient to construct a "global" subspace evasive set with near-optimal parameters. This composition does need a (mild) structural requirement that the subspace evasive sets are graphs of functions. We encapsulate this observation as follows.

Theorem 5 (Informal version of Theorem 8)**.** *Let* $\mathrm{Enc} : \mathbb{F}^k \to (\mathbb{F}^s)^n$ *be the encoding map of an* $\mathbb{F}$*-additive*[2] *code* $C \subseteq (\mathbb{F}^s)^n$ *which is* $(r, 0, c, L)$ *list-recoverable. Let* $f : \mathbb{F}^s \to \mathbb{F}^b$ *be a function such that* $A = \{(a, f(a)) \ : \ a \in \mathbb{F}^s\} \subseteq \mathbb{F}^{s+b}$ *is an* (r, c) *subspace evasive set. Then, their composition*

$$B = \{(x, f(\mathrm{Enc}(x)_1), \ldots, f(\mathrm{Enc}(x)_n)) \ : \ x \in \mathbb{F}^k\} \subseteq \mathbb{F}^{k+bn}$$

is an (r, L) *subspace evasive set of size* q^k*.*

If we think of the subspace evasive set itself as a code, this construction has close parallels to *code concatenation* in coding theory. Intuitively, Theorem 5 shows that one can use subspace list-recovery to effect a local-to-global principle that *amplifies* a small subspace evasive set into a larger one.

To explain concretely why this is the case, consider any r-dimensional subspace $U \subseteq \mathbb{F}^{k+bn}$, and consider all messages $X \subseteq \mathbb{F}^k$ whose corresponding points $B_X := \{(x, f(\mathrm{Enc}(x)_1), \ldots, f(\mathrm{Enc}(x)_n)) : x \in X\}$ land in U. Since X is the projection of B_X onto its first k coordinates, we have that X is itself contained in an r-dimensional subspace. The challenge still remains to show that $|X|$ is not too large.

Proving this relies on the *local* subspace evasive set. For every $i \in [n]$, we consider the following projection of B_X:

$$A_{X,i} := \{(\mathrm{Enc}(x)_i, f(\mathrm{Enc}(x)_i)) : x \in X\} \subseteq A.$$

Since Enc() is $\mathbb{F}$-linear, $A_{X,i}$ is a linear image of B_X, and it is contained in an r-dimensional space. Furthermore, since $A_{X,i}$ is contained in an (r, c) subspace evasive set, we have that $A_{X,i}$ and thus $S_i := \mathrm{Enc}(X)_i$ has cardinality at most c. Therefore, $\mathrm{Enc}(X) \subseteq S_1 \times \cdots \times S_n$, where each S_i has cardinality at most c. On the other hand, X is contained in an r-dimensional subspace. Since Enc is the encoding map of an $(r, 0, c, L)$ subspace list-recoverable code, we can conclude $|X| \leq L$. Therefore, B is an (r, L) subspace evasive set.

Taking a step back, it should not be so surprising that this combination of subspace evasive sets and list-recoverable codes is fruitful. List-recoverable codes guarantee that in any set with enough codewords, there must be some coordinate where the codewords take many different values. Subspace-evasive sets guarantee that if any set contains enough points, then those points span a high dimensional space. The composition in Theorem 5 uses the first property to find a coordinate with many different values, and the second property to ensure those values have high rank. This property of list-recoverable codes has also found many other surprising uses, including recent oracle separations of quantum complexity classes (see [YZ24, BHV26]).

[2] $\mathbb{F}$-additivity means that for any $c, c' \in C$, and $\alpha, \beta \in \mathbb{F}$, $\alpha c + \beta c' \in C$ as well. In other words, C is an $\mathbb{F}$-linear space.

The Building Blocks. Thanks to Theorem 5, we have reduced the task of constructing an explicit subspace evasive set into two problems: (1) efficient construction of the "local" subspace evasive set and (2) construction of a good additive subspace list-recoverable code. For the former challenge, we can efficiently derandomize the probabilistic construction of subspace evasive sets using the method of conditional expectations. In short, for a "semi-random" set A where some elements are deterministic and some are randomly chosen, we efficiently estimate the expected number of violations to our subspace evasive set property and derandomize one-at-a-time the elements of A, while keeping the expected number of violations monotonically decreasing.

For the latter challenge of constructing good subspace list-recoverable codes, we can use many recent advances in this space off-the-shelf. For example, the recent work of Brakensiek, Chen, Dhar, and Zhang [BCDZ26a] (see also the work of Goyal and Guruswami [GG25]) showed that any *subspace design code* can be used to construct very good list-recoverable codes. Subspace designs, introduced by Guruswami and Xing [GX13], are a pseudorandom family of linear maps which have found many applications including list-decoding (their original motivation in [GX13] and recently in [Sri25, GG26b]), list recovery [BCDZ26a, GG25], rank condensers and dimension expanders [FG15, GRX21], and algorithmic derandomization [BCDZ26b, CGG$^+$26], and proximity gaps of codes [GG26b, GGSW26]. Many of these applications have been discovered quite recently and have thus motivated a detailed investigation of better constructions of subspace designable codes [GK16, GGH26, GRSZ26, CDG26, AGG26]. As such, by composing these subspace design constructions with [BCDZ26a, GG25], we get a number of explicit subspace evasive set constructions achieving Theorem 2, see Section 4 for exact statements.

Implications for List-recovery. As observed by Guruswami [Gur11], explicit subspace evasive sets can be used to construct explicit list-recoverable codes. In broad strokes, we prove a family of results of the following form.

Theorem 6 (Informal, see Sections 5 and 6.2)**.** *For any constants $\ell \geq 1, \varepsilon, R \in (0,1)$, there are explicit codes with rate at least R that are $(1-R-\varepsilon, \ell, \mathrm{poly}(\ell/\varepsilon))$ list-recoverable. Furthermore, for the construction stated in Theorem 43, both the encoding and the list-recovery of the code can be done in $O_{R,\ell,\varepsilon}(1)\,\mathrm{poly}(n)$ time.*

See Table 1 for a comparison of our results with prior work, the most notable contrast being that the list size of all previous constructions had exponential dependence in $1/\varepsilon$. (See Table 2 for a more comprehensive comparison.) Some of our constructions get a list size of $O(\frac{\ell}{\varepsilon^2}\log\frac{\ell}{\varepsilon})$, which is not too far off the probabilistic method guarantee of $O(\ell/\varepsilon)$.

At first glance, it may seem counterintuitive that our construction has novel implications for list-recoverable codes, as state-of-the-art constructions of list-recoverable codes are a key input to Theorem 5. However, note that Theorem 5 requires as input an $\mathbb{F}$-*additive* code, but a subspace evasive set by definition has no additive structure. Thus, any list-recoverable code constructed using our subspace evasive sets circumvents lower bounds on the list-recoverability of linear and additive codes [GLM$^+$22, CZ25, LMS25, LS25]. Furthermore, this technique for constructing list-recoverable codes falls outside of the recently-popularized "AEL framework" [AEL95] for constructing list-decodable and list-recoverable codes [ST25, JS26, GGH26], thus circumventing recently-established lower bounds in that space as well [BCPZ26].

All of our constructions work by taking an established code construction (such as Reed–Solomon codes) and judiciously using the subspace evasive set to select a subcode with good list-recovery guarantees. For example, the work of Guruswami and Xing [GX22] (see also [KRZ26, Section 5.3])

Codes	Alphabet size $\lvert\Sigma\rvert$	List size L	Explicit?
Random Linear Codes [ZP81, Gur01, RW18, LS25]	$\ell^{O(1/\varepsilon)}$	$(\ell/\varepsilon)^{O(\ell/\varepsilon)}$	No
Random Linear Codes [BCDZ26a, GG26a]	$(\frac{\ell}{R+\varepsilon})^{O((R+\varepsilon)/\varepsilon^2)}$	$\left(\frac{\ell}{R+\epsilon}\right)^{O(1+R/\varepsilon)}$	No
Random Codes	$\ell^{O(1/\varepsilon)}$	$O(\ell/\varepsilon)$	No
Folded RS/Univariate Multiplicity Codes [GR08, Kop15, GW13, KRSW23, BCDZ26a]	$\left(\frac{n\ell}{\varepsilon^2}\right)^{O(\ell/\varepsilon^2)}$	$\left(\frac{\ell}{R+\epsilon}\right)^{O(1+R/\varepsilon)}$	Yes
Folded RS Codes & Subspace Evasive Sets [DL12]	$\left(\frac{n}{\varepsilon^2}\right)^{O(\log(\ell)/\varepsilon^2)}$	$(\frac{1}{\varepsilon})^{O(1/\varepsilon^3)}$	Yes
Codes Based on the AEL Framework [ST25, JS26, GGH26]	$\exp(\exp(O(\ell^2/\varepsilon^2)))$	$\left(\frac{\ell}{R+\epsilon}\right)^{O(1+R/\varepsilon)}$	Yes
Folded RS plus AEL Codes [KRSW23]	$(\frac{\ell}{\varepsilon})^{O(\ell^2\log(\ell/\varepsilon)/\varepsilon^2)}$	$\ell^{O(1/\varepsilon^4)}$	Yes
Folded AG Codes [GX13, GK16]	$\exp\left(\frac{\ell\log(\ell/\varepsilon)}{\varepsilon^2}\right)$	$2^{2^{2^{O_{\varepsilon,\ell}(\log^*(n))}}}$	Yes
AG Codes + BTT evasive subspace [GRZ21]	$(\frac{\ell}{\varepsilon})^{O(\ell/\varepsilon^2)}$	$\exp(\mathrm{poly}(\ell/\varepsilon))$	Yes
RS codes + Subspace Evasive Sets **(Theorem 30)**	$n^{O(1/\varepsilon^2)}$	$O(\frac{\ell}{\varepsilon^3}\log\frac{\ell}{\varepsilon})$	Yes
AG codes + Subspace Evasive Sets **(Theorem 35)**	$(\frac{\ell}{\varepsilon})^{O(\ell/\varepsilon^2)}$	$\mathrm{poly}(\ell/\varepsilon)$	Yes
Folded RS codes + Subspace Evasive Sets **(Theorem 37)**	$(\frac{n\ell}{\varepsilon^2})^{O(\ell/\varepsilon^2)}$	$O(\frac{\ell}{\varepsilon^2}\log\frac{\ell}{\varepsilon})$	Yes
AEL codes + Subspace Evasive Sets **(Theorem 33)**	$\exp(\exp(\ell^2/\varepsilon^2))$	$O(\frac{\ell}{\varepsilon^2}\log\frac{\ell}{\varepsilon})$	Yes
Any Linear Code [GLM+22, CZ25, LMS25, LS25]	Any	$\ell^{\Omega(R/\varepsilon)}$	Lower Bound
Classical AEL Codes [BCPZ26]	Any	$\ell^{\Omega(R/\varepsilon)}$	Lower Bound

Table 1: This table gives a summary of many constructions of list-recoverable codes as well as some known limitations.

shows that[3] there are explicit additive subcodes of Reed-Solomon codes such that the lists of codewords obtained in the list-recovery problem lie in a low-dimensional $O(\ell/\varepsilon^2)$-dimensional subspace of the message space. By taking a further subcode of this Reed–Solomon subcode based on our subspace evasive set construction within its message space, we get that this $O(\ell/\varepsilon^2)$-dimensional subspace has a small intersection with our subcoding as a subspace evasive set, yielding the desired $\mathrm{poly}(\ell/\varepsilon)$ list-size bound. We obtain analogous constructions for algebraic-geometry codes (based on [GRZ21]), folded Reed–Solomon codes (based on [GW13]), and AEL codes (based on [GGH26]). Each of these constructions yield different tradeoffs between alphabet size, list size, and encoding/decoding time (some of which have linear-dependence in n). See Section 5 for detailed statements of all of these constructions.

1.2 Related Work

We now give some broader context to subspace evasive sets by briefly discussing generalizations and connections in the literature. See in particular the recent paper of Lim, Nie and Zeng [LNZ26] which surveys a number of these works.

[3]These works only discuss the list-decoding case where $\ell = 1$, but it is straight-forward to generalize the whole proof to general list-recovery for any $\ell \geq 1$. See [CGZ26] for details.

Variety-evasive Sets. A natural generalization of (r, c) subspace evasive sets is requiring intersection of size at most c for families of non-affine sets $V \subseteq \mathbb{F}_q^n$, such as solutions of polynomial equations of higher degree. In particular, we say that a set $A \subseteq \mathbb{F}_q^n$ is (d, r, c) variety evasive if for every variety $V \subseteq \mathbb{F}_q^n$ of degree at most d and dimension at most r, we have that $|V \cap A| \leq c$. The case $d = 1$ coincides with the notion of subspace evasiveness. Variety evasive sets were introduced by Dvir, Kollár and Lovett [DKL14] as a direct generalization of Dvir and Lovett's [DL12] investigation of subspace evasive sets. Variety evasive sets should not be confused with the variety evasive subspace families [Guo24, AG26] which also are motivated by applications to derandomization.

Subspace-evasive Subspaces. In the study of dimension expanders, Guruswami, Resch, and Xing [GRX21] define a notion of *subspace evasive subspaces*. Here, one constructs an $\mathbb{F}_q$-subspace $H \subseteq \mathbb{F}_q^n$ which has small intersection with every $\mathbb{F}_{q^d}$-subspace $W \subseteq \mathbb{F}_{q^d}^{n/d}$ which can also be viewed as an $\mathbb{F}_q$-subspace $W \subseteq \mathbb{F}_q^n$.

Twisted Varieties. Closely related to variety evasive sets are the concept of *twisted* varieties, where one imposes that $A \subseteq \mathbb{F}_q^n$ is an $n-r$-dimensional variety, where we impose that for any degree-d, r-dimensional variety $V \subseteq \mathbb{F}_q^n$, the intersection $V \cap A$ is 0-dimensional. This notion was introduced by works of Dvir–Kollár–Lovett [DL12, DKL14] and Blagojević–Bukh–Karasev [BBK13], the latter of whom called these "non-degenerated embeddings." See the work of Lim, Nie and Zeng [LNZ26] for new bounds on the existence of twisted varieties.

Connections to Extremal Combinatorics. Evading varieties has recently found much interest [IV22, SZ26, LNZ26] due to the concept being a natural generalization of "points in general position." In particular, studying variety-evasive sets (even existentially) has a number of applications to incidence geometry [ST24, MTS24] and hypergraph Turán problems [BBK13, CLNZ25]. As mentioned previously, in certain parameter regimes, subspace evasive sets can also be used to construct explicit Ramsey graphs [PR04].

Applications of List-Recoverable Codes List-recoverable codes themselves have found many important applications in the literature. For instance, list-recoverability plays an important role in the construction of unbalanced lossless expanders [GUV09] and in oracle separations of quantum complexity classes [YZ24, BHV26].

1.2.1 Paper Structure

In Section 2, we define subspace list-recoverable codes, and give the general framework to construct the "global" subspace evasive sets given explicit subspace list-recoverable codes (SLRCs) and "local" subspace evasive sets. In Section 3, we list explicit constructions of useful SLRCs as well as describe a construction of "local" subspace evasive sets using the method of conditional expectation. In Section 4, we plug these prior constructions into the framework and get explicit subspace evasive sets with required qualities. In Section 5, we use the constructed subspace evasive sets to construct good list-recoverable codes as shown in Table 1. In the end, we show in Section 6 how to speed up the list-recovery of such codes using known techniques from coding theory.

Notation. For any set A and non-negative integer $t \geq 0$, $\binom{A}{t}$ denote the collection of subsets of A with size t, and $\binom{A}{\leq t}$ denote the collection of subsets of A with size at most t. For any vector $x \in \Sigma^n$, let $x_{\leq m} \in \Sigma^m$ denote the length-m prefix of x and $x_i \in \Sigma$ denote the i-th coordinate of x. For a set of vectors $X \subseteq \Sigma^n$, let $X_{\leq m}$ denote $X_{\leq m} = \{x_{\leq m} \colon x \in X\}$ and X_m denote $X_m = \{x_m \colon x \in X\}$. We also define $x_{\geq m}$ and $X_{\geq m}$ similarly.

Given an $\mathbb{F}$-additive code $C \subseteq (\mathbb{F}^s)^n$, an encoder of C is an $\mathbb{F}$-linear function $f\colon \mathbb{F}^k \to (\mathbb{F}^s)^n$ with $\mathsf{Im}(f) = C$. If some encoder f can be computed in time T, we say C is encodable in time T.

For any subset $A \subseteq \mathbb{F}^n$, we say that A is constructable in time[4] T if there is a bijection $f\colon \{1, 2, \ldots, |A|\} \to A$ which can be computed in time T, including any preprocessing time needed to determine the function f. In a similar vein, we say that A has a membership oracle in time T if the indicator function $g\colon \mathbb{F}^n \to \{0, 1\}$ defined by $g(x) = \mathbf{1}[x \in A]$ can be computed in time T.

2 Local to Global Amplification via Subspace List-recoverable Codes

In this section, we show how to use subspace list-recoverable codes (SLRCs) to amplify local subspace evasive sets to global subspace evasive sets. Recall from Definition 4 that a code $C \subseteq (\mathbb{F}^s)^n$ is (r, ρ, ℓ, L) subspace list-recoverable if for any product set $S_1 \times \cdots \times S_n \subseteq (\mathbb{F}^s)^n$, where each S_i has cardinality at most ℓ, any r-dimensional subcode of C has at most L codewords within relative Hamming distance ρ of this product set. In particular, subspace list-recovery is a weaker notion than traditional list-recovery, and an $\mathbb{F}$-additive code $C \subseteq (\mathbb{F}^s)^n$ that is (ρ, ℓ, L) list-recoverable is automatically (r, ρ, ℓ, L) subspace list-recoverable for any $r \geq 0$.

This local-to-global reduction actually requires the "local" subspace evasive set to have a *generator function*, which is defined below.

Definition 7 (Generator function)**.** Let $f\colon \mathbb{F}^a \to \mathbb{F}^b$ be a function, we define $G^f := \{(x, f(x))\colon x \in \mathbb{F}^a\} \subseteq \mathbb{F}^{a+b}$ to be the set generated by f (i.e., the *graph* of f), and we say f is the generator function of G^f.

We now prove our core theorem, which shows how to construct a "global" subspace evasive set from a "local" subspace evasive set and a subspace list-recoverable code.

Theorem 8. *Let $\mathbb{F}$ be a field, $f\colon \mathbb{F}^s \to \mathbb{F}^b$ be the generator function of an (r, c_f) subspace evasive set G^f, and $C \subseteq (\mathbb{F}^s)^n$ with $\dim_{\mathbb{F}}(C) = k$ be an $\mathbb{F}_q$-additive $(r, 0, c_f, L)$ subspace list-recoverable code. We can construct a function $g\colon \mathbb{F}^k \to \mathbb{F}^{bn}$ such that $B = G^g = \{(x, g(x))\colon x \in \mathbb{F}_q^k\} \subseteq \mathbb{F}^{k+bn}$ is an (r, L) subspace evasive set with size $|B| = q^k$.*

Moreover, let f can be computed in time T_f and C is encodable in time T_C, then g can be computed in time $O(T_C + nT_f)$, B is constructable in time $O(T_C + nT_f)$, and B has membership oracle in time $O(T_C + nT_f)$.

Proof. Let $\mathrm{Enc}\colon \mathbb{F}^k \to (\mathbb{F}^s)^n$ denote an $\mathbb{F}$-linear encoder of C so that $\mathsf{Im}(\mathrm{Enc}) = C$ and Enc can be computed in time T_C. We construct $g\colon \mathbb{F}^k \to \mathbb{F}^{bn}$ as follows:

$$g(x) := (f(\mathrm{Enc}(x)_1), \ldots, f(\mathrm{Enc}(x)_n)) \in \mathbb{F}^{bn}, \quad \forall x \in \mathbb{F}^k.$$

We first prove that $B = \{(x, g(x))\colon x \in \mathbb{F}_q^k\} \subseteq \mathbb{F}^{k+bn}$ is indeed an (r, L) subspace evasive set. Let $U \subseteq \mathbb{F}^{k+bn}$ denote any subspace with $\dim(U) \leq r$. Let $U' = U_{\leq k} \subseteq \mathbb{F}^k$ denote the projection of U on the first k coordinates. Let $A = U \cap B$ and $A' = A_{\leq k}$ similarly. Since $A \subseteq B$, by the construction of B we know distinct elements x, y in A have distinct length-k prefixes $x_{\leq k}, y_{\leq k}$. Therefore, $|A| = |A'|$. It suffices to prove $|A'| \leq L$.

Suppose for contradiction that $|A'| > L$. For each $i \in [n]$, let $\mathrm{Enc}_i\colon \mathbb{F}^k \to \mathbb{F}^s$ denote the linear map outputting the i'th coordinate of the encoding map Enc of C, i.e., $\mathrm{Enc}_i(x) = \mathrm{Enc}(x)_i$

[4]We assume all field operations take time $O(1)$.

for all $x \in \mathbb{F}^k$. Since $\mathrm{Enc}(A') \subseteq \mathrm{Enc}(U')$ with $\dim(\mathrm{Enc}(U')) \le r$, and C is $(r, 0, c_f, L)$ subspace list-recoverable, we know because $|A'| > L$ that there must be some $i \in [n]$ so that $|\mathrm{Enc}_i(A')| > c_f$.

Now define $H_i = \{(\mathrm{Enc}_i(x), f(\mathrm{Enc}_i(x))) : x \in A'\}$. Note that $|H_i| \ge |\mathrm{Enc}_i(A')| > c_f$. Since $G^f \supseteq H_i$ is an (r, c_f) subspace evasive set, we must have that $\mathrm{rank}(H_i) > r$. This implies that

$$\begin{aligned} r \ge \dim(U) &\ge \mathrm{rank}(A) = \mathrm{rank}\{(x, g(x)) : x \in A'\} \\ &\ge \mathrm{rank}\{(\mathrm{Enc}_i(x), f(\mathrm{Enc}_i(x))) : x \in A'\} = \mathrm{rank}(H_i) > r, \end{aligned}$$

a contradiction. Therefore, we must have that $|A| = |A'| \le L$. This proves that B is an (r, L) subspace evasive set.

Finally we justify the complexity aspects of our construction. Evaluating g requires an evaluation of Enc and n evaluations of f, and thus $O(T_C + nT_f)$ time. In terms of the construction, we can compute a bijection $f_B \colon |B| \to B$ as $f_B(x) = (x, g(x))$ by one evaluation of g, which requires $O(T_C + nT_f)$ time. To implement the membership oracle for the constructed subspace evasive set, for a given $(x \in \mathbb{F}^k, y \in \mathbb{F}^{bn})$, we need to compute $g(x)$ to see whether $g(x) = y$. This can be implemented in $O(T_C + nT_f)$ time. □

3 Building Blocks

In this section, we discuss methods for constructing "local" subspace evasive sets, and record existing constructions of subspace list-recoverable codes from the literature.

3.1 Local Subspace Evasive Sets via Random Sampling

We first present how to construct the "local" subspace evasive set via pre-conditioning methods, which is the function f that we use in Theorem 8. The following construction can be seen as an intelligent brute-force search. More concretely, it is a derandomization of the probabilistic method union bound, which can be seen as the toy case of the derandomization of the Lovász Local Lemma [CGH13].

Theorem 9. *Let $s, b, r, d > 0$ be integers and $\mathbb{F}_q$ be a finite field, if $(s + b + d)r < bd$, then we can construct, in time $O(q^{(s+b)(r+1)+rd}d)$, a function $f \colon \mathbb{F}_q^s \to \mathbb{F}_q^b$ so that $G^f \subseteq \mathbb{F}_q^{s+b}$ is an $(r, d-1)$ subspace evasive set.*

Proof. Let $\mathbb{F}_q^s = \{x_1, \ldots, x_{q^s}\}$ and $g \colon \mathbb{F}_q^s \to \mathbb{F}_q^b$ denote a random function. There are at most $q^{(s+b)r}$ many r-dimensional subspaces U of $\mathbb{F}_q^{s+b}$. For each of these subspaces U, it has at most q^{rd} subsets $S \subseteq T$ with $|S| = d$. Therefore, there are at most $q^{(s+b+d)r}$ possible pairs (S, T). For each of such $S \subseteq T$, consider the bad event $E_{S,T}$ when $S \subseteq G^g = \{(x, g(x)) \in \mathbb{F}_q^{s+b} \colon x \in \mathbb{F}_q^s\}$ happens. Our goal is to construct a function $f \colon \mathbb{F}_q^s \to \mathbb{F}_q^b$ such that no $E_{S,T}$ happens conditioned on $f = g$.

We assign values to $f(x_1), \ldots, f(x_{q^s})$ one by one. For each $i \in [q^s]$, let $I_i = \{x_1, \ldots, x_i\}$ and $f_i \colon I_i \to \mathbb{F}_q^b$ denote the assigned values on I_i. Let $p_i = \mathbb{E}[\sum_{S,T} E_{S,T} : f_i = g|_{I_i}]$. We start from $i = 0$ and $f_i = \emptyset$.

For each $i \in [q^s]$, in the i-th round, we have the following.

$$p_{i-1} = \mathbb{E}\left[\sum_{S,T} E_{S,T} : f_{i-1} = g|_{I_{i-1}}\right] = \frac{1}{q^b} \sum_{w \in \mathbb{F}_q^b} \mathbb{E}\left[\sum_{S,T} E_{S,T} : f_{i-1} = g|_{I_{i-1}} \wedge g(x_i) = w\right]$$

Computing these expectations requires $O(q^{b+(b+s+d)r}d)$ time. Therefore, one can choose some $w \in \mathbb{F}_q^b$ such that $\mathbb{E}[\sum_{S,T} E_{S,T} : f_{i-1} = g|_{I_{i-1}} \wedge g(x_i) = w] \leq p_{i-1}$ in deterministic $O(q^{b+(b+s+d)r}d)$ time. By assigning $f_i(x_i) = w$ and $f_i|_{I_{i-1}} = f_{i-1}$, we can guarantee that $p_i \leq p_{i-1}$ and proceed to round $i+1$.

This whole procedure requires $O(q^{(b+s)(r+1)+rd}d)$ time. We can guarantee that

$$p_{q^s} = \mathbb{E}[\sum_{S,T} E_{S,T} : f = g] \leq p_0 = \mathbb{E}[\sum_{S,T} E_{S,T}].$$

Since we succeed when $p_{q^s} < 1$, it suffices to show that $p_0 = \mathbb{E}[\sum_{S,T} E_{S,T}] < 1$.

Fix any valid $S \subseteq T$. Let $S = \{a_1, \ldots, a_{|S|}\}$. $E_{S,T}$ happens iff for all $i \in [|S|]$, there is $g(a_{i,\leq s}) = a_{i,\geq s+1}$. For a uniformly random function g, the probability that this happens is q^{-b}.

If $|S| > |S_{\leq s}|$, then since G^g is generated by g, it be the case that $E_{S,T} = 0$. Otherwise, we have that

$$\Pr[E_{S,T}] \leq q^{-b|S_{\leq s}|} \leq q^{-b|S|} \leq q^{-bd}.$$

Since $(s+b+d)r < bd$, we have that

$$p_0 = \mathbb{E}\left[\sum_{S,T} E_{S,T}\right] \leq \sum_{S,T} q^{-bd} \leq q^{(b+s+d)r-bd} < 1,$$

as desired. □

Remark 10. From [GW13, Lemma 23], there exists a polynomial $p \in \mathbb{F}_{q^s}[X]$ with degree at most d such that $\{(x, p(x)_{\leq b}) \in \mathbb{F}_q^{s+b} : x \in \mathbb{F}_{q^s}\}$ achieves the similar subspace evasiveness as Theorem 9. We can enumerate all such polynomials $p(x)$ and find one with the target property. This gives an alternative and more space-efficient construction of the local subspace evasive sets we need.

3.2 Explicit Subspace List-recoverable Constructions

We next list useful explicit constructions of subspace list-recoverable codes which follows from recent advances in pseudorandomness and coding theory.

We first define lossless rank-condenser and states its implications for SLRCs. We make use of this notion in Section 3.2.3.

Definition 11 ([For14])**.** An additive code $C \subseteq \left(\mathbb{F}_q^s\right)^n$ forms a lossless rank-condenser up to rank r if for any subspace $U \subseteq C$ with $\dim U \leq r$, we have that there is an $i \in [n]$ such that $\pi_i : \left(\mathbb{F}_q^s\right)^n \mapsto \mathbb{F}_q^s$, the projection map onto the ith coordinate, is injective on U.

Lemma 12. *If an additive code $C \subseteq \left(\mathbb{F}_q^s\right)^n$ is a lossless rank-condenser up to rank r, then it also forms a $(r, 0, \ell, \ell)$ subspace list-recoverable code for all $\ell \in \mathbb{N}$.*

Proof. Consider any $U \subseteq C \subseteq \left(\mathbb{F}_q^s\right)^n$ with $\dim U \leq r$ as well as $S_1, \ldots, S_n \in \binom{\mathbb{F}_q^s}{\leq \ell}$. Define $\mathcal{L} = \{c \in U \cap C : \forall i \in [n], \pi_i(c) \in S_i\}$. Then there exists an $i \in [n]$ such that $\pi_i|_U$ is injective. Now, $|\pi_i(\mathcal{L})| = |\mathcal{L}|$ but $\pi_i(\mathcal{L}) \subseteq S_i$. Hence, $|\mathcal{L}| \leq |S_i| \leq \ell$. □

Next, we define subspace design codes [GX13] and demonstrate their implications for SLRCs. We make use of such codes in Sections 3.2.1 and 3.2.2.

Definition 13 (Subspace-Design Property [GX13, CZ25, GG26b])**.** For any function $\tau : \mathbb{N} \to \mathbb{R}_{\leq 1}$, an $\mathbb{F}_q$-additive code $\mathcal{C} \subseteq (\mathbb{F}_q^s)^n$ is said to be a *τ-subspace design* code if for every $r \in \mathbb{N}$, and every $\mathbb{F}_q$-linear subspace $\mathcal{A}$ of $\mathcal{C}$ of dimension at most r, the following holds:

$$\frac{1}{n}\sum_{i=1}^{n} \dim \mathcal{A}_i \leq \dim(\mathcal{A}) \cdot \tau(r)$$

where $\mathcal{A}_i = \{a \in \mathcal{A} : \ a_i = 0\}$.

Lemma 14. *If an additive code $C \subseteq \left(\mathbb{F}_q^s\right)^n$ is a τ-subspace design with $\tau(r) < 1/r$, then it also forms a $(r, 0, \ell, \ell)$ subspace list-recoverable code for all $\ell \in \mathbb{N}$.*

Proof. Consider any $U \subseteq C \subseteq \left(\mathbb{F}_q^s\right)^n$ with $\dim U \leq r$ as well as $S_1, \ldots, S_n \in \binom{\mathbb{F}_q^s}{\leq \ell}$. Define $\mathcal{L} = \{c \in U \cap C : \ \forall i \in [n], \pi_i(c) \in S_i\}$. Observe that now, $\frac{1}{n}\sum_{i=1}^{n} \dim U_i < 1$ where $U_i = \{u \in U : \ u_i = 0\}$. Thus, there exists an $i \in [n]$ with $\dim U_i = 0$. Hence π_i is injective on U. Therefore by Lemma 12, we have that C is $(r, 0, \ell, \ell)$ subspace list-recoverable. □

Theorem 15 (subspace list-recovery of subspace-designs [BCDZ26a, GG25])**.** *If $\mathcal{C} \subseteq \Sigma^n$ is a τ-subspace design code, then for any $\varepsilon > 0$, C is $\left(r, 1 - \tau(r) - \varepsilon, \ell, \left(\frac{\ell}{\tau(r)+\epsilon}\right)^{(\tau(r)+\epsilon)/\epsilon}\right)$ subspace list-recoverable.*

A proof of the above fact is found in [GG25, Appendix A, Theorem A.4].

Corollary 16. *If $\mathcal{C} \subseteq \Sigma^n$ is a τ-subspace design code, then C is $\left(r, 0, \ell, \ell^{1/(1-\tau(r))}\right)$ subspace list-recoverable. Additionally, when $\tau(r) \leq 1/(1+\log_2 \ell)$, then C is $(r, 0, \ell, 2\ell)$ subspace list-recoverable.*

Proof. Set $\varepsilon = 1 - \tau(r)$ in Theorem 15. Setting $\tau(r) = \frac{1}{1+\log \ell}$ gives that C is $(r, 0, \ell, \ell^{\frac{1+\log_2 \ell}{\log_2 \ell}}) = (r, 0, \ell, 2\ell)$ subspace list-recoverable. □

We now instantiate Lemma 14 and Corollary 16 with specific choices of subspace design codes.

3.2.1 Construction 1: [GGH26] subspace designs

We now present the first construction of subspace list-recoverable codes via the subspace designs of Goyal, Guruswami, and Hsieh [GGH26] based on AEL codes [AEL95].

Theorem 17 ([GGH26])**.** *For any finite field $\mathbb{F}_q$, $R, \varepsilon > 0$ with $R + \varepsilon \leq 1$, and dimension $r \in \mathbb{N}$, there exists an $s = O_{q,r,\varepsilon}(1) = \mathrm{poly}(r, 1/\varepsilon) \cdot q^{r^2}$ such that for all sufficiently large n, there exists an explicit code $C \subseteq (\mathbb{F}_q^s)^n$ of rate $\geq R$, that forms a τ-subspace design with $\tau(r) \leq R + \varepsilon$. In particular, C can be computed in time $O_{q,r,\varepsilon}(1) \cdot \mathrm{poly}(n)$.*

By combining Theorem 17 with Lemma 14, we get a family of SLRCs with the following parameters.

Corollary 18. *For any finite field $\mathbb{F}_q$ and $r \in \mathbb{N}$, for all large enough n, there exists an explicit τ subspace-design additive code $C \subseteq (\mathbb{F}_q^s)^n$ with rate $R \geq 1/2r$, $\tau(r) < 1/r$, $s = O_{q,r}(1) = \mathrm{poly}(r) \cdot q^{r^2}$ which can be computed in time $O_{q,r}(1) \cdot \mathrm{poly}(n)$. In particular, this code is an $(r, 0, \ell, \ell)$ subspace list-recoverable code for all $\ell \in \mathbb{N}$.*

Likewise, combining Theorem 17 with Corollary 16, obtains the following family of SLRCs.

Corollary 19. *For any finite field $\mathbb{F}_q$ and $r, \ell \in \mathbb{N}$, for all large enough n, there exists an explicit τ subspace-design additive code $C \subseteq (\mathbb{F}_q^s)^n$ with rate $R \geq \frac{1}{2+2\log_2 \ell}$, $\tau(r) \leq \frac{1}{1+\log_2 \ell}$, $s = O_{q,r}(1) = \mathrm{poly}(r, \log \ell) \cdot q^{r^2}$ which can be computed in time $O_{q,r}(1) \cdot \mathrm{poly}(n)$. In particular, this code is an $(r, 0, \ell, 2\ell)$ subspace list-recoverable code for all $\ell \in \mathbb{N}$.*

3.2.2 Construction 2: [GK16] subspace designs

We next present a construction of subspace list-recoverable codes via the subspace designs of Guruswami and Kopparty [GK16].

Theorem 20 ([GK16])**.** *For any $R \in (0, 1)$ and $s, n \in \mathbb{N}$ such that Rsn is an integer, and any finite field $\mathbb{F}_q$ with $q > sn$, there exists an explicit additive τ-subspace design code with $\tau(r) \leq \frac{sR}{s-r+1}$ for all $r \leq s$. Additionally, the code can be computed in time $n \cdot \mathrm{poly}(s, \log q)$.*[5]

Combining Theorem 20 with Lemma 14 yields the following SLRCs.

Corollary 21. *For any $r \in \mathbb{N}$, and integer $n \geq 2$, and finite field $\mathbb{F}_q$ with $q > 4nr$, there exists an explicit τ subspace-design additive code $C \subseteq (\mathbb{F}_q^s)^n$ with rate $R \geq 1/8r$, $\tau(r) < 1/4r$, $s = 2r$ which can be computed in time $n \cdot \mathrm{poly}(r, \log q)$. In particular, this code is an $(r, 0, \ell, \ell)$ subspace list-recoverable code for all $\ell \in \mathbb{N}$.*

Furthermore, combining Theorem 20 with Corollary 16 obtains the following SLRCs.

Corollary 22. *For any $r, \ell \in \mathbb{N}$ with $n > 4\log \ell$, and finite field $\mathbb{F}_q$ with $q > 4nr$, there exists an explicit τ subspace-design additive code $C \subseteq (\mathbb{F}_q^s)^n$ with rate $R \geq 1/(3 + 3\log_2 \ell)$, $\tau(r) < 1/(1 + \log_2 \ell)$, $s = 2r$ which can be computed in time $n \cdot \mathrm{poly}(r, \log q, \log \ell)$. In particular, this code is an $(r, 0, \ell, 2\ell)$ subspace list-recoverable code.*

3.2.3 Construction 3: [GRSZ26] lossless-rank-condensers

Our final construction of subspace list-recoverable codes uses the lossless-rank condensers of Guo, Raj, Shangguan, and Zhang [GRSZ26] (using Lemma 12):

Theorem 23 ([GRSZ26])**.** *For any $R \in (0, 1), r \in \mathbb{N}$, and any non-prime field $\mathbb{F}_q$ with $q > \mathrm{poly}(r)$, there exists an infinite explicit family of $\mathbb{F}_q$-additive codes forming lossless rank condensers up to rank r with $s = O(r)$ and rate $\Omega(1/r)$. In particular, this family of codes forms an explicit infinite family of $(r, 0, \ell, \ell)$ subspace list-recoverable codes for all $\ell \in \mathbb{N}$. Additionally, the code can be computed in time $\mathrm{poly}(n, r, \log q)$.*

4 Explicit Subspace Evasive Sets

In this section we combine the local-to-global reduction (Theorem 8), the local optimal subspace evasive sets (Theorem 9), and various explicit subspace list-recoverable codes from Section 3.2 to explicitly construct subspace evasive sets.

Our first construction considers the case in which the field size q is constant with respect to n. In this case, we make use of Corollary 18 and Corollary 19 derived from [GGH26].

[5] This code is in fact the [GR08] folded Reed-Solomon code.

Theorem 24. *Fix a prime power q and constants $r \in \mathbb{Z}^+, \varepsilon \in (0,1)$. For all large enough n, we can construct $(r, L = O(\min(\frac{r^2}{\varepsilon}, \frac{r\log(r/\varepsilon)}{\varepsilon})))$ subspace evasive sets $A \subseteq \mathbb{F}_q^n$ with size $|A| \geq q^{(1-\varepsilon)n}$. We can construct a membership oracle for A with running time $O_{q,r,\varepsilon}(1)\operatorname{poly}(n)$.*

Proof. We split the proof into two cases.

- (Case A) $L = O(\frac{r^2}{\varepsilon})$, and
- (Case B) $L = O(\frac{r\log(r/\varepsilon)}{\varepsilon})$.

In these two different cases we will use Corollary 18 and Corollary 19 respectively. We let D denote the reciprocal of the target rate of the subspace list recoverable code, i.e., $R = \frac{\dim_{\mathbb{F}_q}(C)}{sM} \geq \frac{1}{D}$. We then set the different parameters as follows.

- (Case A) $\ell = \lceil \frac{16r^2}{\varepsilon} \rceil, D = 2r$, and
- (Case B) $\ell = \lceil \frac{256r(1+\log(r/\varepsilon))}{\varepsilon} \rceil, D = 2 + 2\log_2 \ell$. In this case $D \leq 20(1 + \log_2(r/\varepsilon))$.

Let $t = \lceil \frac{4D}{\varepsilon} \rceil, s = s_0 t, b = \lfloor \frac{\varepsilon s}{2D} \rfloor, d = \ell + 1$ where $s_0 = O_{q,r,\varepsilon}(1)$ is the constant s in the statement of Corollary 18 (Case A) or Corollary 19 (Case B). Then we check the parameter requirement of Theorem 9 and invoke it: Since $b \geq 4r$, we know $b - r \geq \frac{\varepsilon s}{4D}$. Therefore

$$\frac{r(s+b)}{b-r} \leq \frac{r(5s/4)}{\varepsilon s/4D} = \frac{5rD}{\varepsilon}.$$

Splitting by case, we then compute that

- (Case A) $\frac{r(s+b)}{b-r} \leq \frac{5rD}{\varepsilon} \leq \frac{10r^2}{\varepsilon} < \ell + 1 = d$, and
- (Case B) $\frac{r(s+b)}{b-r} \leq \frac{5rD}{\varepsilon} \leq \frac{100r(1+\log(r/\varepsilon))}{\varepsilon} < \ell + 1 = d$.

In both cases, Theorem 9 provides a function $f \colon \mathbb{F}_q^s \to \mathbb{F}_q^b$ so that G^f is a (r, ℓ) subspace evasive set with construction time $O_{q,r,\varepsilon}(1)$.

By invoking Corollary 18 (Case A) or Corollary 19 (Case B), we get an $(r, 0, \ell, 2\ell)$ subspace list-recoverable code $\hat{C} \subseteq (\mathbb{F}_q^{s_0})^{Mt}$ with rate at least $R \geq 1/D$ and encoding time $O_{q,r,\varepsilon}(1)\operatorname{poly}(M)$ for all large enough M. Let $C \subseteq (\mathbb{F}_q^s)^M$ be the $\mathbb{F}$-additive code where groups of t consecutive coordinates of $\hat{C}$ are bundled together. By inspection, such a code is also an $(r, 0, \ell, 2\ell)$ subspace list-recoverable code, has rate at least $R \geq 1/D$, and encoding time $O_{q,r,\varepsilon}(1)\operatorname{poly}(M)$ for all large enough M.

Let $M = \lfloor \frac{\varepsilon n}{b} \rfloor$, we know that $R = \frac{1}{D} \geq \frac{b}{\varepsilon s}$. Therefore, $\dim(C) \geq \frac{bM}{\varepsilon} \geq n - \frac{b}{\varepsilon} \geq (1-\varepsilon)n + 1$ for large enough n. Let $k = n - bM$ and use a subcode of $C \subseteq (\mathbb{F}_q^s)^M$ with dimension k. By Theorem 8 we can construct a function $g \colon \mathbb{F}_q^k \to \mathbb{F}_q^{bM}$ such that $G^g \subseteq \mathbb{F}_q^n$ is an $(r, L = 2\ell)$ subspace evasive set with construction and membership oracle time $O_{q,r,\varepsilon}(1)\operatorname{poly}(n)$. □

The second construction replaces the SLRCs based on Theorem 17 with SLRCs based on Theorem 20. This is a more general construction since it works for all polynomial field sizes $q \leq \operatorname{poly}(n)$. However, the running time becomes $n^{O(rL)}$, which can be less efficient compared to $O_{q,\varepsilon,\ell}(1)\operatorname{poly}(n)$ running time of the previous construction when q is a constant.

Theorem 25. *For any constants $r \in \mathbb{Z}_{>0}$, $\varepsilon \in (0,1)$, and $C > 0$, for all sufficiently large n and every prime power $q \le n^C$, there exists an explicit (r, L) subspace evasive set $A \subseteq \mathbb{F}_q^n$ with*

$$L = O\left(\min\left\{\frac{r^2}{\varepsilon}, \frac{r\log(r/\varepsilon)}{\varepsilon}\right\}\right)$$

and size $|A| \ge q^{(1-\varepsilon)n}$. We can construct a membership oracle for A with running time $n^{O_C(rL)}$.

Proof sketch. This proof is similar to that of Theorem 24. We split the proof into two cases.

- (Case A) $d = O(\frac{r^2}{\varepsilon})$, and
- (Case B) $d = O(\frac{r\log(r/\varepsilon)}{\varepsilon})$.

In these two different cases we will use Corollary 21 and Corollary 22 respectively and set different parameters as follows.

- (Case A) $\ell = \lceil \frac{50r^2}{\varepsilon} \rceil, D = 8r$, and
- (Case B) $\ell = \lceil \frac{256r(1+\log(r/\varepsilon))}{\varepsilon} \rceil, D = 3 + 3\log_2 \ell$ so that $D \le 33(1 + \log_2(r/\varepsilon))$.

Let e denote the smallest positive integer such that $Q = q^e > 8Dn$. We know $Q = \mathrm{poly}(n)$. Since an (r, d) subspace evasive set $A \subseteq \mathbb{F}_Q^{n/e}$ with size at least $Q^{(1-\varepsilon)n/e}$ actually implies an (r, d) subspace evasive set $A \subseteq \mathbb{F}_q^n$ with size at least $q^{(1-\varepsilon)n}$ via a linear bijection between $\mathbb{F}_q^e$ and $\mathbb{F}_Q$, it suffices to construct a subspace evasive set with the same quality but over the field extension $\mathbb{F}_Q$. Therefore, we can assume $q > 8Dn$ without loss of generality.

Let $s_0 = 2r, t = \lceil \frac{4D}{\varepsilon} \rceil, s = s_0 t, b = \lfloor \frac{\varepsilon s}{2D} \rfloor, d = \ell + 1$. We follow analogous reasoning as in the proof of Theorem 24. We only need to clarify the running time and check the parameter requirement of Corollary 21 (Case A) or Corollary 22 (Case B). Since $b \ge 4r$ and $M \le \frac{\varepsilon n}{b}$, it follows that $q > 8Dn \ge 4rMt$, so we can indeed invoke Corollary 21 (Case A) or Corollary 22 (Case B).

The construction time from Theorem 9 is $q^{O((b+s+d)r)} = q^{O(rd)} = n^{O(rL)}$ since $L = 2(d-1), d = \Omega(s)$ and $s \ge b$. Since the encoding time guaranteed by Corollary 21 and Corollary 22 is $\mathrm{poly}(n)$, by Theorem 8 is final construction time and membership oracle time can be bounded within $n^{O(rL)}$. □

The third construction uses [GRSZ26] based SLRCs instead. It provides better construction time in many cases. However, it only achieves intersection size $O(r^2/\varepsilon)$.

Theorem 26. *Fix $r \in \mathbb{Z}^+, \varepsilon \in (0,1)$ and prime power q, for infinitely many n, we can construct $(r, O(r^2/\varepsilon))$ subspace evasive sets $A \subseteq \mathbb{F}_q^n$ with size $|A| \ge q^{(1-\varepsilon)n}$. We can construct a membership oracle for A with running time $\max(r,q)^{O(r^3/\varepsilon)} + \mathrm{poly}(n, r, \log q)$.*

Proof sketch. The proof is basically the same as the (Case A) of the above proof of Theorem 25. The only two differences are: (i) We replace Corollary 21 with Theorem 23, with an advantage that we only need to assume $q > \mathrm{poly}(r)$ rather than $q > 8Dn$; and (ii) Some parameter settings need to be scaled by constant multiplicative factors to match the statement of Theorem 23. □

5 Explicit List-recoverable Codes

In this section we present four explicit constructions of $(1-R-\varepsilon, \ell, L = \text{poly}(\ell/\varepsilon))$ list-recoverable codes. All of these results share are based on the paradigm introduced by Guruswami and Wang [GW13] of taking a subcode of an additive code using a subspace evasive set. We begin by defining a notion of *dimension* list recovery.

Definition 27. For integers $\ell, r \geq 1$ and $\rho \in [0,1]$, we say that an additive code $C \subseteq (\mathbb{F}_q^s)^n$ is (ρ, ℓ, r) *dimension* list-recoverable if for any sets $S_1, \ldots, S_n \in \binom{\mathbb{F}_q^s}{\leq \ell}$, the list

$$\mathcal{L} = \{c \in C : \exists y \in (S_1 \times \cdots \times S_n), \text{Ham}(c, y) \leq \rho n\}.$$

lies in an r-dimensional subspace of $(\mathbb{F}_q^s)^n$.

Unlike our earlier notion of subspace list recovery (Defintion 4) which intersects the recovered list $\mathcal{L}$ with a low-dimensional subspace, Definition 27 says that $\mathcal{L}$ *always* lies in a low-dimensional subspace. Despite being a rather strict notion, all the families of additive codes we consider in this paper, when invoked with suitable parameters, are $(1 - R - \varepsilon, \ell, \text{poly}(\ell/\varepsilon))$ dimension list-recoverable. If we assume our additive code has an encoding map $\text{Enc} : \mathbb{F}_q^k \to (\mathbb{F}_q^s)^n$, by plugging in a suitable subspace evasive set $A \subseteq \mathbb{F}_q^k$ into the encoder, the *subcode* $\text{Enc}(A) \subseteq C$ has the property that its recovered list $\mathcal{L}$ lies in a low-dimensional subspace *and* this subspace has few elements in $\text{Enc}(A)$. We formalize this observation as follows.

Theorem 28. *For prime power q, integers $s, n, k, r, c, \ell \geq 1$ and $R, \varepsilon, \rho > 0$. Let $A \subseteq \mathbb{F}_q^k$ be an (r, c) subspace evasive set of size at least $q^{(1-\varepsilon/2)k}$ that is constructable in time T_A. Let $\text{Enc} : \mathbb{F}_q^k \to (\mathbb{F}_q^s)^n$ be the encoding map of a code C of rate $\frac{k}{sn} \geq R+\varepsilon$ which is (ρ, ℓ, r) dimension list-recoverable. Then $\text{Enc}(A) \subseteq (\mathbb{F}_q^s)^n$ is an (ρ, ℓ, c) list-recoverable code of rate at least R with encoding time $T_A + T_{\text{Enc}}$, where T_{Enc} is the runtime of* Enc.

Proof. For lists $S_1, \ldots, S_n \subseteq \mathbb{F}_q^s$ of size at most ℓ, we construct

$$\mathcal{L} = \{c \in C : \exists y \in (S_1 \times \cdots \times S_n), \text{Ham}(c, y) \leq \rho n\}.$$

Since C is (ρ, ℓ, r) dimension list-recoverable, we have that $\text{rank}\, \mathcal{L} \leq r$. Since A is an (r, c) subspace evasive set, we have that $A \cap \text{Enc}^{-1}(\mathcal{L})$ has at most c elements. Thus,

$$\{c \in \text{Enc}(A) : \exists y \in (S_1 \times \cdots \times S_n), \text{Ham}(c, y) \leq \rho n\} \subseteq \text{Enc}(A) \cap \mathcal{L} = \text{Enc}(A \cap \text{Enc}^{-1}(\mathcal{L}))$$

has at most c elements. Thus, $\text{Enc}(A)$ is (ρ, ℓ, c) list-recoverable. Furthermore, the rate of $\text{Enc}(A)$ is at least $\frac{(1-\varepsilon/2)k}{sn} \geq (1 - \varepsilon/2)(R + \varepsilon) \geq R$. The encoding time of $T_A + T_{\text{Enc}}$ follows from the construction being a direct composition. □

By picking various additive codes (RS, AEL, AG, and FRS) and invoking Theorem 28, we achieve a rich family of constructions of near-optimal list-recoverable codes. We now formally describe each of these constructions.

5.1 Subcodes of Reed–Solomon Codes

We first construct explicit subcodes of Reed–Solomon Codes with good list-recoverability. It builds upon the following additive subcodes of RS codes

Theorem 29 ([CGZ26], list-recovery generalization of [GX22]—see also [KRZ26, Section 5.3])**.** *For any constants $\ell \geq 1, \varepsilon, R \in (0,1)$, prime power $q \geq n$ and distinct evaluation points $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$, there exists $s = O(1/\varepsilon^2)$ and explicit $\mathbb{F}_q$-additive Reed-Solomon subcode $C \subseteq (\mathbb{F}_{q^s})^n$ of rate R such that C is $(1 - R - \varepsilon, \ell, O(\ell/\varepsilon^2))$ dimension list-recoverable.*

Composing Theorem 25, Theorem 29 (with $\varepsilon = \varepsilon/2$), and Theorem 28, we get the following explicit list-recoverable code.

Theorem 30. *For any constants $\ell \geq 1$, $\varepsilon \in (0,1)$, $R \in (0, 1-\varepsilon)$, and $M \geq 1$, for all sufficiently large n, every prime power $n \leq q \leq n^M$, and distinct evaluation points $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$, there exists $s = O(1/\varepsilon^2)$ and an explicit subcode of a Reed–Solomon code over $\mathbb{F}_{q^s}$ with evaluation points $\alpha_1, \ldots, \alpha_n$ and rate at least R that is*

$$\left(1 - R - \varepsilon, \ell, O\left(\frac{\ell}{\varepsilon^3} \log \frac{\ell}{\varepsilon}\right)\right)$$

list-recoverable. The encoding time is $n^{\mathrm{poly}_M(\ell/\varepsilon)}$.

Remark 31. Very recently, Alrabiah, Goyal, and Guruswami [AGG26] constructed explicit Reed–Solomon codes which (among other properties) are $(1-R-\varepsilon, \ell, O(\ell/\varepsilon))$ dimension list-recoverable. By composing that result with Theorem 25 and Theorem 28 one can construct codes of rate at least R that are $\left(1 - R - \varepsilon, \ell, O\left(\frac{\ell}{\varepsilon^2} \log \frac{\ell}{\varepsilon}\right)\right)$ list-recoverable, approximately the same as our Theorem 37.

5.2 Subcodes of AEL Codes

Our next construction of an explicit list-recoverable codes takes advantage of identifying a subcode of AEL-based subspace design codes in [GGH26].

Theorem 32. *For any constants $\ell \geq 1, \varepsilon, R \in (0,1)$ and prime power q, for $s = \exp(O(\ell^2/\varepsilon^2) \log q)$, there exist explicit $\mathbb{F}_q$-additive codes over alphabet $\mathbb{F}_q^s$ with rate at least R which are $(1 - R - \varepsilon, \ell, O(\ell/\varepsilon))$ dimension list-recoverable.*

Proof. Let $\tau(r) = R + \varepsilon/2$ for all $r \leq \frac{2\ell}{\varepsilon}$ and $\tau(r) = 1$ for $r > \frac{2\ell}{\varepsilon}$. By [GGH26, Theorem 1.1], there exist explicit τ-subspace design codes with the prescribed rate, $\mathbb{F}_q$-additivity, and alphabet size. Then, by [GG25, Lemma 2.10], such codes satisfies the required property that all messages concerned in the statement lie within a certain $\frac{2\ell}{\varepsilon}$-dimensional subspace of $\mathbb{F}_q^k$. □

Composing Theorem 24, Theorem 32 (with $\varepsilon = \varepsilon/2$), and Theorem 28, we get our next explicit list-recoverable code.

Theorem 33. *For any constants $\ell \geq 1, \varepsilon, R \in (0,1)$, there are explicit codes with rate at least R, alphabet size $\exp(\exp(O(\ell^2/\varepsilon^2)))$ that are $(1 - R - \varepsilon, \ell, O(\frac{\ell}{\varepsilon^2} \log \frac{\ell}{\varepsilon}))$ list-recoverable. The encoding time is $O_{\ell,\varepsilon}(1)\,\mathrm{poly}(n)$.*

5.3 Subcodes of AG Codes

Similarly, we also have explicit linear subcodes of AG codes with good list-recoverability. This is due to a generalization of [GRZ21] from list-decoding to list-recovery.

Theorem 34 ([CGZ26], list-recovery generalization of [GRZ21])**.** *For any constants $\ell \geq 1, \varepsilon, R \in (0,1)$, there exists a prime power $q = O(\frac{1}{\varepsilon^2})$, an extension $\mathbb{F}_{q^m}$ with size $q^m = (\frac{\ell}{\varepsilon})^{O(\ell/\varepsilon^2)}$ and explicit $\mathbb{F}_q$-linear subcodes of AG codes over $\mathbb{F}_{q^m}$ with rate R which are $(1-R-\varepsilon, \ell, \mathrm{poly}(\ell/\varepsilon))$ dimension list-recoverable.*

We next compose Theorem 24, Theorem 34 (with $\varepsilon = \varepsilon/2$), and Theorem 28 to get the following construction.

Theorem 35. *For any constants $\ell \geq 1, 0 < \varepsilon < 1$ and $R \in (0, 1-\varepsilon)$, there are explicit subcodes of algebraic-geometry codes over $\mathbb{F}_q, q = (\frac{\ell}{\varepsilon})^{O(\ell/\varepsilon^2)}$ with rate at least R that are $(1-R-\varepsilon, \ell, \mathrm{poly}(\ell/\varepsilon))$ list recoverable. The encoding time is $O_{\ell,\varepsilon}(1)\,\mathrm{poly}(n)$.*

Although the list size here is worse than before (with a exponent that is not explicitly calculated), it has the smallest-known alphabet size $\exp(\mathrm{poly}(\ell/\varepsilon))$ of an explicit $(1-R-\varepsilon, \ell, \mathrm{poly}(\ell/\varepsilon))$ list-recoverable code. Even in the classical list-decoding literature where $\ell = 1$, all previous explicit $(1-R-\varepsilon, \mathrm{poly}(1/\varepsilon))$ list-decodable codes require an alphabet of size at least $\exp(\exp(\mathrm{poly}(1/\varepsilon)))$ (and which is achieved by [JMST25]).

5.4 Subcodes of Folded Reed–Solomon Codes

Finally we give explicit list-recoverable codes through a subspace evasive subcode of the folded Reed–Solomon codes in [GR08]. Such subcodes of folded RS codes were in fact the motivating use of subspace evasive sets in the list decoding context in [Gur11, GW13].

Theorem 36 ([GW13, Theorem 7])**.** *For any constants $\ell \geq 1, \varepsilon, R \in (0,1), s \geq 16\ell/\varepsilon^2$ and $q \geq sn$, there exist explicit $\mathbb{F}_q$-folded Reed–Solomon codes over $\mathbb{F}_q^s$ with rate at least R such that the code is $(1-R-\varepsilon, \ell, O(\ell/\varepsilon))$ dimension list-recoverable.*

To finish, we compose Theorem 25, Theorem 36 (with $\varepsilon = \varepsilon/2$), and Theorem 28 to get the following construction.

Theorem 37. *For any constants $\ell \geq 1, \varepsilon, R \in (0,1)$, there are explicit subcodes of folded Reed–Solomon codes with rate at least R, alphabet size $(\frac{n\ell}{\varepsilon^2})^{O(\ell/\varepsilon^2)}$ that are $(1-R-\varepsilon, \ell, O(\frac{\ell}{\varepsilon^2}\log\frac{\ell}{\varepsilon}))$ list-recoverable. The encoding time is $n^{\mathrm{poly}(\ell/\varepsilon)}$.*

Despite the large alphabet, this construction yields efficient list-recovery algorithms thanks to recent algorithmic advances [GG25, GHKS25]. This is explained in detail as in Section 6.2.

6 Algorithmic subspace evasion and list-recovery

We show that any of the above subspace evasive constructions can moreover be made algorithmic, i.e., given a low-dimensional input subspace, its intersection with the subspace evasive set can be computed efficiently. We then use this to make the list-recovery claim for the codes of Theorem 37 algorithmic.

6.1 Algorithmic version of subspace evasive set construction

The following result adds efficient intersection computation to the subspace evasive set construction of Theorem 8

Theorem 38. *Let $\mathrm{Enc}_1, \ldots, \mathrm{Enc}_n : \mathbb{F}_q^k \mapsto \mathbb{F}_q^s$ be linear maps constructible in time T_C such that the resulting code $C = \{(\mathrm{Enc}_1(x), \ldots, \mathrm{Enc}_n(x)), x \in \mathbb{F}_q^k\} \subseteq (\mathbb{F}_q^s)^n$ is an r-lossless rank condenser, and let $f : \mathbb{F}_q^s \mapsto \mathbb{F}_q^b$ be so that G^f is an (r, c_f) subspace-evasive set. Assume that given any linear space $A \subseteq \mathbb{F}_q^{s+b}$ of dimension $\leq r$, $G^f \cap A$ can be computed in time Dec_f.*

Then, we can construct a function $g : \mathbb{F}_q^k \mapsto \mathbb{F}_q^{bn}$ such that G^g is an (r, c_f) subspace-evasive set of size q^k, and G^g is constructable, and moreover given any subspace $U \subseteq \mathbb{F}_q^{k+bn}$ of dimension $\leq r$, $U \cap G^g$ can be computed in time $\mathsf{Dec}_f + (c_f + T_C) \cdot \mathrm{poly}(n, s, \log q)$

Proof. We let $g(x) = (f(\mathrm{Enc}_1(x)), \ldots, f(\mathrm{Enc}_n(x)))$ as in the proof of Theorem 8. Observe that by Lemma 12, the condenser is an $(r, 0, c_f, c_f)$ subspace list-recoverable code. Thus, by Theorem 8, the resulting construction is subspace-evasive. We now simply need to show that it is also "decodable" efficiently.

Let the given linear space be $U \subseteq \mathbb{F}_q^{k+bn}$ of dimension $\leq r$. Now, let U' be the projection of U onto the first k coordinates. Let $\dim U' = r' \leq r$. Now, by Definition 11, there is a coordinate $i \in [n]$ such that $\dim(\mathrm{Enc}_i(U')) = r'$. Observe that such an i can be computed in time $T_C \,\mathrm{poly}(n, s, r, \log q)$ by simply computing $\dim(\mathrm{Enc}_i(U'))$ for all $i \in [n]$.

Now, for all $u \in U$, let u' be the projection of it onto the first k coordinates and u'_i be the projection onto the following ith block of b coordinates. Observe that if $u \in U \cap G^g$, we must have that $u_i = f(\mathrm{Enc}_i(u'))$. That is, $(\mathrm{Enc}_i(u'), u_i) \in G^f$. Thus, we can now simply compute $\{(\mathrm{Enc}_i(u'), u_i) : u' \in U'\} \cap G^f$ in $\mathsf{Dec}_f + T_C \cdot \mathrm{poly}(n, \log q, s)$ time.

Since Enc_i is injective on U', we get that we can thus recover u' for all $u' \in U'$ such that there is an $u \in U \cap G^g$ with $u_{\leq k} = u'$. Additionally, there are at most c_f such choices of u'.

Now, it simply suffices to check which of them are in $G^g \cap U$ which takes $c_f \cdot T_C \cdot \mathrm{poly}(n, s, \log q)$ time. □

Corollary 39. *For any $\varepsilon \in (0, 1)$, for large enough k and for any (r, c_A) subspace-evasive set $A \subseteq (\mathbb{F}_q^k)$ that is constructable and has membership oracle in time T_A, there is an $A' \subseteq \mathbb{F}_q^{k+\lfloor \varepsilon k \rfloor}$ which is also (r, c_A) subspace-evasive with $|A'| = |A|$, constructible in time $O_{q,r,\varepsilon}(1) \cdot \mathrm{poly}(k) + c_A T_A$, and for any $U \subseteq \mathbb{F}_q^{k+\lfloor \varepsilon k \rfloor}$ of dimension $\leq r$, $A' \cap U$ and can be computed in time $O_{q,r,\varepsilon}(1)\,\mathrm{poly}(k) + c_A T_A$ time.*

Proof. Observe that in Theorem 38, we can pick the lossless rank-condenser to be of $s = O_{q,r,\varepsilon}(1)$ dimension and f from using Theorem 9 to be such that $bn \leq \varepsilon k$ such that the resulting set G^g is $(r, \mathrm{poly}(r, 1/\varepsilon))$ subspace-evasive using Section 4.

Now, let $A' = \{(a, g(a)) : a \in A\}$. Observe that $|A'| = |A|$ and $A' \cap U \subseteq G^g \cap U$ which can be computed in time $O_{q,r,\varepsilon}(1)\,\mathrm{poly}(k)$. But, now restricting to the first k coordinates, A is already (r, c_A) subspace-evasive. Thus, we can now check membership in A for all elements of $(G^g \cap U)_{\leq k}$ with an additional $c_A T_A$ time. □

6.2 Consequences for list-recovery

One key drawback of the above algorithmic results has been that the runtime scales as $n^{\mathrm{poly}(\ell/\varepsilon)}$ when $q \geq n$. To see this, we observe that all of Theorems 24 to 26 require $\mathsf{Dec}_f = q^{\mathrm{poly}(\ell/\varepsilon)}$. Moreover, in almost all algorithmically list-recoverable codes with constant dimension, the corresponding alphabet size q is larger than n, and thus the existence of an $O_{\ell,\varepsilon}(1)n^{O(1)}$ complexity list-decoder is unclear. We provide a method to sidestep this obstruction by constructing subcodes

of folded Reed–Solomon codes that are $(1-R-\varepsilon, \ell, \mathrm{poly}(\ell/\varepsilon))$ list-recoverable with a randomized list-recovery algorithm running in $O_{R,\ell,\varepsilon}(1)n^{O(1)}$ time.

Remark 40. We note that there are algorithmically $(1-R-\varepsilon, \ell, O_{\ell,\varepsilon}(1))$ list-recoverable constructions of rate R in the literature with alphabet $O_{\ell,\varepsilon,R}(1)$ as well, but as far as we know there is no stated result showing that these constructions have their list contained in a $\mathrm{poly}(\ell/\varepsilon)$-dimensional space. The construction in [GGH26] does have the second feature, however no list recovery algorithm was presented. We suspect that this should be possible by employing the techniques of [JMST25, ST25], but as far as we know, this has not been established in the literature. Here, we present an alternative method, of possible independent interest, that circumvents this gap.

We remind ourselves of a result from [GG25] about the list-recovery of the folded Reed-Solomon codes of [GR08]. To state their result, we require the definition of a *sum set*.

Definition 41 (Sum Sets)**.** $P \subseteq \mathcal{C}$ is an (u, v) *sum-set* in $\mathcal{C}$ if it is described by sets $A_1, A_2, \cdots, A_{u'}$ with $A_i \subseteq \mathcal{C}$, $|A_i| \leq v$, and $u' \leq u$ such that $P = A_1 + \cdots + A_{u'} = \{a_1 + a_2 + \ldots + a_{u'} : a_i \in A_i\}$.

Theorem 42. *For every choice of $\ell \in \mathbb{N}, \varepsilon > 0, R > 0$, any rate R s-folded Reed–Solomon code $\mathcal{C}$ for $s > s_0 := \frac{16(R+\varepsilon)\ell}{\varepsilon^2}$ has the following property.*[6]

There exists an algorithm that takes in input lists $L_1, \cdots, L_n \subseteq \mathbb{F}_q^s$ of size ℓ each, runs in time $\mathrm{poly}(n, s, \log q)$, and outputs the descriptions of $t = \widetilde{O}(\ell^2/\varepsilon^3)$ many

$$\left(\left\lceil \frac{2(R+\varepsilon)\log(2e\ell/(R+\varepsilon))}{\varepsilon} \right\rceil, \ell\right) \text{ sum-sets } P_1, \cdots, P_t$$

such that $\{c \in \mathcal{C} : \Delta(c, L_1 \times \cdots \times L_n) < 1 - R - \varepsilon\} \subseteq \bigcup_{i=1}^{t} P_i$ with probability $\geq \frac{1}{2}$.

Finally, we make use of the above results to achieve a $O_{R,\ell,\varepsilon}(1)n^{O(1)}$ time list-recovery algorithm. Broadly speaking, since we can efficiently find several sum-sets in a folded RS code and all concerned codewords are in their union, it suffices to compute intersections of the linear spans of these sum-sets with a subspace evasive set. Each sum-set is contained in an $\mathbb{F}_2$-linear subspace of dimension at most $u\ell$, so it is already enough to have subspace evasive sets over $\mathbb{F}_2$ rather than $\mathbb{F}_q$ when q has characteristic 2, and subspace evasive sets over $\mathbb{F}_2$ yield efficient intersection-solving algorithms.

Theorem 43. *For any $\varepsilon \in (0,1)$, $\ell \in \mathbb{N}$, and rate $R \in (0, 1-\varepsilon)$, there is a constant $s = O(\ell/\varepsilon^2)$, and an explicit family of codes $C \subseteq (\mathbb{F}_q^s)^n$ of rate $\geq R$, for all sufficiently large n and a choice of $q = 2^d$ with $sn \leq q < 2sn$, constructible in time $O_{R,\ell,\varepsilon}(1)\,\mathrm{poly}(n)$ and $(1-R-\varepsilon, \ell, \mathrm{poly}(\ell, 1/\varepsilon))$ list-recoverable.*

Moreover, there is a randomized algorithm given any $S_1, \cdots, S_n \subseteq \mathbb{F}_q^s$ with $|S_i| \leq \ell$ for all $i \in [n]$, such that $\{c \in C : \Delta(c, S_1 \times \cdots \times S_n) \leq 1 - R - \varepsilon\}$ can be output in time $O_{\varepsilon,\ell}(1)\,\mathrm{poly}(n)$ with probability at least $1/2$.

Proof. Pick $s = \lceil 64\ell/\varepsilon^2 \rceil$ and $q_0 = 2$, and let d be the smallest positive integer such that $2^d \geq sn$. Let $\mathbb{F}_q$ be the field of size $q = 2^d$ and let $k = \lceil (R + \varepsilon/2)sn \rceil - 1$ and $k_0 = dk$.

We let $r = \lceil 10\ell \log(2e\ell/\varepsilon)/\varepsilon \rceil$ and $\eta = \varepsilon/8$, and set $m = \lfloor k_0/(1+\eta) \rfloor$. By Theorem 24, we choose $A_0 \subseteq \mathbb{F}_{q_0}^m$ to be an $(r, \mathrm{poly}(\ell, 1/\varepsilon))$ subspace-evasive set with $|A_0| \geq 2^{(1-\eta)m}$. By Corollary 39, this gives a subspace-evasive set in $\mathbb{F}_{q_0}^{m+\lfloor \eta m \rfloor}$ with the same size and intersection bound, whose intersection with any subspace of dimension at most r can be computed in time $O_{\varepsilon,\ell}(1)\,\mathrm{poly}(m)$.

[6] Folded Reed–Solomon codes can be constructed for any $q \geq sn$ and do not require characteristic assumptions.

Padding with zero coordinates, we let $A \subseteq \mathbb{F}_{q_0}^{k_0}$ be the resulting subspace-evasive set. We have $|A| \geq 2^{(1-\varepsilon/2)k_0}$ for all sufficiently large n, and given any $U \subseteq \mathbb{F}_{q_0}^{k_0}$ of dimension at most r, $A \cap U$ can be output in time $O_{\varepsilon,\ell}(1)\operatorname{poly}(k_0) = O_{\varepsilon,\ell}(1)\operatorname{poly}(n)$. Going forward, for clarity in the argument, we let $L : \mathbb{F}_{q_0}^{k_0} \to \mathbb{F}_q^k$ be an $\mathbb{F}_{q_0}$-linear isomorphism.

Now, let C_0 be the s-folded Reed–Solomon code of dimension k over $\mathbb{F}_q$ and block-length n. Let it be given by $\{\mathrm{Enc}(x) : x \in \mathbb{F}_q^k\}$.

Let $C = \{\mathrm{Enc}(L(a)) : a \in A\}$. Observe that $|C| = |A|$. Thus, the resulting code has rate

$$\frac{\log_2 |A|}{dsn} \geq (1-\varepsilon/2)\frac{k}{sn} \geq (1-\varepsilon/2)\left(R + \frac{\varepsilon}{2} - \frac{1}{sn}\right) \geq R,$$

for all sufficiently large n, where the last inequality uses $R < 1 - \varepsilon$.

We now show the required list-recovery guarantee. Fix $S_1, \ldots, S_n \subseteq \mathbb{F}_q^s$ of size at most ℓ each, and let $R_0 = k/(sn)$. Observe that by Theorem 42, applied to C_0 with rate R_0 and error parameter $\varepsilon/2$, there is an algorithm that outputs $P_1, \ldots, P_t$ which are (u, ℓ) sum-sets in C_0 in time $O_{\varepsilon,\ell}(1)\operatorname{poly}(n)$ with $t = \widetilde{O}(\ell^2/\varepsilon^3)$, where

$$u = \left\lceil \frac{4(R_0 + \varepsilon/2)\log(2e\ell/(R_0+\varepsilon/2))}{\varepsilon} \right\rceil, \qquad u\ell \leq r,$$

such that

$$\{c \in C : \Delta(c, S_1 \times \cdots \times S_n) \leq 1 - R - \varepsilon\} \subseteq \bigcup_{i=1}^{t} P_i$$

with probability at least $1/2$. Here, we pad the input sets to size ℓ if necessary. The theorem applies since $s > 64(R_0 + \varepsilon/2)\ell/\varepsilon^2$ and $R_0 < R + \varepsilon/2$, so its guaranteed radius is larger than $1 - R - \varepsilon$.

Now, we can observe that, for each i, we can write $P_i = A_{i,1} + \cdots + A_{i,u_i}$ with $u_i \leq u$ and $|A_{i,j}| \leq \ell$, and let

$$V_i = \operatorname{span}_{\mathbb{F}_{q_0}}\left(\bigcup_{j=1}^{u_i} A_{i,j}\right) \subseteq C_0.$$

Since $P_i \subseteq V_i$ and $\dim_{\mathbb{F}_{q_0}}(V_i) \leq u\ell \leq r$, we can compute

$$A \cap L^{-1}(\mathrm{Enc}^{-1}(V_i))$$

in time $O_{\ell,\varepsilon}(1)\operatorname{poly}(n)$, and it has size $\operatorname{poly}(\ell, 1/\varepsilon)$ due to the subspace-evasive property of A. The preimage is an $\mathbb{F}_{q_0}$-linear subspace, and a basis for it can be computed efficiently from the sum-set description.

Finally, observe that since $C \subseteq C_0$, we can compute $C \cap \left(\bigcup_{i=1}^{t} V_i\right)$ by encoding the points in these intersections, and retain exactly those codewords satisfying $\Delta(c, S_1 \times \cdots \times S_n) \leq 1 - R - \varepsilon$. Since $P_i \subseteq V_i$, this outputs the required list in time $O_{\ell,\varepsilon}(1)\operatorname{poly}(n)$ with probability at least $1/2$. Moreover, the list size is at most $t \cdot \operatorname{poly}(\ell, 1/\varepsilon) = \operatorname{poly}(\ell, 1/\varepsilon)$. □

AI Methodology.

The results in this paper were mostly developed in May and June 2026 without the use of LLMs. We prompted GPT models 5.5/5.6 with our constructions, but they could not improve the stated bounds. Some LLM assistance was used to improve the overall writing quality.

Recently we fed a draft of the paper into GPT-6 and it was able to improve the bound c in a (r, c)-subspace evasive set construction to the optimal $O(r/\epsilon)$ bound. This is via an entirely different approach. We will report this separately after understanding and rewriting the construction and proof. We note that our $\tilde{O}(r/\varepsilon)$ bound is almost optimal and already an exponential improvement over the previous bound.

References

[AEL95] Noga Alon, Jeff Edmonds, and Michael Luby. Linear time erasure codes with nearly optimal recovery (extended abstract). In *36th Annual Symposium on Foundations of Computer Science, FOCS 1995, Milwaukee, Wisconsin, USA, 23-25 October 1995*, pages 512–519. IEEE Computer Society, 1995. doi:10.1109/SFCS.1995.492581.

[AG26] Robert Andrews and Abhibhav Garg. An improved construction of variety-evasive subspace families. *CoRR*, abs/2605.05621, 2026. URL: https://doi.org/10.48550/arXiv.2605.05621, arXiv:2605.05621, doi:10.48550/ARXIV.2605.05621.

[AGG26] Omar Alrabiah, Rohan Goyal, and Venkatesan Guruswami. Explicit reed-solomon subspace designs: Optimal list and line decoding. Technical Report TR26-262, Electronic Colloquium on Computational Complexity, 2026. URL: https://eccc.weizmann.ac.il/report/2026/262/.

[BBK13] Pavle V. M. Blagojević, Boris Bukh, and Roman Karasev. Turán numbers for $K_{s,t}$-free graphs: topological obstructions and algebraic constructions. *Israel J. Math.*, 197(1):199–214, 2013. doi:10.1007/s11856-012-0184-z.

[BCDZ26a] Joshua Brakensiek, Yeyuan Chen, Manik Dhar, and Zihan Zhang. Combinatorial bounds for list recovery via discrete brascamp-lieb inequalities. In Aditya Bhaskara and Artur Czumaj, editors, *Proceedings of the 58th Annual ACM Symposium on Theory of Computing, STOC 2026, Salt Lake City, UT, USA, June 22-26, 2026*, pages 365–376. ACM, 2026. doi:10.1145/3798129.3800756.

[BCDZ26b] Joshua Brakensiek, Yeyuan Chen, Manik Dhar, and Zihan Zhang. From random to explicit via subspace designs with applications to local properties and matroids. In Aditya Bhaskara and Artur Czumaj, editors, *Proceedings of the 58th Annual ACM Symposium on Theory of Computing, STOC 2026, Salt Lake City, UT, USA, June 22-26, 2026*, pages 619–630. ACM, 2026. doi:10.1145/3798129.3800778.

[BCPZ26] Joshua Brakensiek, Yeyuan Chen, Aaron Putterman, and Zihan Zhang. Bounds and limitations on codes achieving list recovery capacity. *CoRR*, abs/2607.19576, 2026. URL: https://doi.org/10.48550/arXiv.2607.19576, arXiv:2607.19576, doi:10.48550/ARXIV.2607.19576.

[BHV26] John Bostanci, Andrew Huang, and Vinod Vaikuntanathan. Separating quantum and classical advice with good codes. *arXiv preprint arXiv:2602.09385*, 2026.

[BR15] Eli Ben-Sasson and Noga Ron-Zewi. From affine to two-source extractors via approximate duality. *SIAM J. Comput.*, 44(6):1670–1697, 2015. doi:10.1137/12089003X.

[BS14] Avraham Ben-Aroya and Igor Shinkar. A note on subspace evasive sets. *Chic. J. Theor. Comput. Sci.*, 2014, 2014. URL: http://cjtcs.cs.uchicago.edu/articles/2014/9/contents.html.

[CDG26] Gil Cohen, Dean Doron, and Noam Goldgraber. Algebraic-geometric parvaresh-vardy subspace designs and rank condensers. *CoRR*, abs/2609.32834, 2026. URL: https://doi.org/10.48550/arXiv.2609.32834, arXiv:2609.32834, doi:10.48550/ARXIV.2609.32834.

[CGG+26] Abhranil Chatterjee, Sumanta Ghosh, Rohit Gurjar, Roshan Raj, and Thomas Thierauf. Bipartite matching is in NC. *Electron. Colloquium Comput. Complex.*, TR26, 2026. URL: https://eccc.weizmann.ac.il/report/2026/100, arXiv:TR26-100.

[CGH13] Karthekeyan Chandrasekaran, Navin Goyal, and Bernhard Haeupler. Deterministic algorithms for the lovász local lemma. *SIAM J. Comput.*, 42(6):2132–2155, 2013. doi:10.1137/100799642.

[CGZ26] Yeyuan Chen, Zeyu Guo, and Zihan Zhang. List-recoverable subcodes of rs/ag codes, 2026. URL: https://github.com/yeyuanch/List-recoverable-subcodes-of-AG-codes.

[CLNZ25] Yaobin Chen, Xizhi Liu, Jiaxi Nie, and Ji Zeng. Random Turán and counting results for general position sets over finite fields. *Sci. China Math.*, 68(12):3043–3062, 2025. doi:10.1007/s11425-024-2384-x.

[CZ16] Eshan Chattopadhyay and David Zuckerman. Explicit two-source extractors and resilient functions. In Daniel Wichs and Yishay Mansour, editors, *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 670–683. ACM, 2016. doi:10.1145/2897518.2897528.

[CZ25] Yeyuan Chen and Zihan Zhang. Explicit folded Reed-Solomon and multiplicity codes achieve relaxed generalized singleton bounds. In Michal Koucký and Nikhil Bansal, editors, *Proc. 57th ACM Symp. on Theory of Computing (STOC)*, pages 1–12, 2025. URL: https://doi.org/10.1145/3717823.3718114, arXiv:2408.15925.

[DKL14] Zeev Dvir, János Kollár, and Shachar Lovett. Variety evasive sets. *Comput. Complexity*, 23(4):509–529, 2014. doi:10.1007/s00037-013-0073-9.

[DL12] Zeev Dvir and Shachar Lovett. Subspace evasive sets. In Howard J. Karloff and Toniann Pitassi, editors, *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 351–358. ACM, 2012. doi:10.1145/2213977.2214010.

[FG15] Michael A. Forbes and Venkatesan Guruswami. Dimension expanders via rank condensers. In Naveen Garg, Klaus Jansen, Anup Rao, and José D. P. Rolim, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2015, Princeton, NJ, USA, August 24-26, 2015*, volume 40 of *LIPIcs*, pages 800–814. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2015. URL: https://doi.org/10.4230/LIPIcs.APPROX-RANDOM.2015.800, doi:10.4230/LIPICS.APPROX-RANDOM.2015.800.

[For14] Michael Andrew Forbes. *Polynomial Identity Testing of Read-Once Oblivious Algebraic Branching Programs*. PhD thesis, Massachusetts Institute of Technology, Cambridge, Massachusetts, June 2014. URL: https://hdl.handle.net/1721.1/89843.

[FT24] Jakob Führer and Vladislav Taranchuk. Large line-free sets and their applications. *arXiv preprint arXiv:2403.18611*, 2024.

[GG25] Rohan Goyal and Venkatesan Guruswami. Structure theorems (and fast algorithms) for list recovery of subspace-design codes, 2025. *arXiv preprint arXiv:2512.08017*. URL: https://arxiv.org/abs/2512.08017, arXiv:2512.08017.

[GG26a] Rohan Goyal and Venkatesan Guruswami. Improved analysis of list-decodability of random linear codes: It's all about counting constraints. Number TR26-074, May 2026. URL: https://eccc.weizmann.ac.il/report/2026/074.

[GG26b] Rohan Goyal and Venkatesan Guruswami. Optimal proximity gaps for subspace-design codes and (random) reed-solomon codes. In Aditya Bhaskara and Artur Czumaj, editors, *Proceedings of the 58th Annual ACM Symposium on Theory of Computing, STOC 2026, Salt Lake City, UT, USA, June 22-26, 2026*, pages 1558–1568. ACM, 2026. doi:10.1145/3798129.3800864.

[GGH26] Rohan Goyal, Venkatesan Guruswami, and Jun-Ting Hsieh. Explicit constant-alphabet subspace design codes, 2026. To appear in FOCS 2026. URL: https://arxiv.org/abs/2604.15218, arXiv:2604.15218.

[GGSW26] Rohan Goyal, Venkatesan Guruswami, Yihang Sun, and Mary Wootters. Locality of curve-decoding and improved proximity gaps. In Mohit Singh and Tom Gur, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX 2026, Boston University, Boston, Massachusetts, USA, and RANDOM 2026, Boston University, Boston, Massachusetts, USA, August 19-21, 2026, August 19-21, 2026*, volume 392 of *LIPIcs*, pages 61:1–61:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2026. URL: https://doi.org/10.4230/LIPIcs.APPROX/RANDOM.2026.61, doi:10.4230/LIPICS.APPROX/RANDOM.2026.61.

[GHKS25] Rohan Goyal, Prahladh Harsha, Mrinal Kumar, and Ashutosh Shankar. Fast list recovery of univariate multiplicity and folded reed-solomon codes. *CoRR*, abs/2512.00248, 2025. URL: https://doi.org/10.48550/arXiv.2512.00248, arXiv:2512.00248, doi:10.48550/ARXIV.2512.00248.

[GK16] Venkatesan Guruswami and Swastik Kopparty. Explicit subspace designs. *Combinatorica*, 36(2):161–185, 2016. doi:10.1007/s00493-014-3169-1.

[GLM+22] Venkatesan Guruswami, Ray Li, Jonathan Mosheiff, Nicolas Resch, Shashwat Silas, and Mary Wootters. Bounds for list-decoding and list-recovery of random linear codes. *IEEE Trans. Inf. Theory*, 68(2):923–939, 2022. doi:10.1109/TIT.2021.3127126.

[GR08] Venkatesan Guruswami and Atri Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Trans. Inform. Theory*, 54(1):135–150, 2008. (Preliminary version in *38th STOC*, 2006). URL: https://doi.org/10.1109/TIT.2007.911222, arXiv:cs/0511072.

[GRSZ26] Zeyu Guo, Roshan Raj, Chong Shangguan, and Zihan Zhang. Explicit rank extractors and subspace designs via function fields, with applications to strong blocking sets, April 2026. URL: https://arxiv.org/abs/2604.13431, arXiv:2604.13431, doi:10.48550/arXiv.2604.13431.

[GRX21] Venkatesan Guruswami, Nicolas Resch, and Chaoping Xing. Lossless dimension expanders via linearized polynomials and subspace designs. *Comb.*, 41(4):545–579, 2021. URL: https://doi.org/10.1007/s00493-020-4360-1, doi:10.1007/S00493-020-4360-1.

[GRZ21] Zeyu Guo and Noga Ron-Zewi. Efficient list-decoding with constant alphabet and list sizes. STOC 2021, page 1502–1515, New York, NY, USA, 2021. Association for Computing Machinery. doi:10.1145/3406325.3451046.

[Guo24] Zeyu Guo. Variety evasive subspace families. *Comput. Complexity*, 33(2):Paper No. 10, 61, 2024. doi:10.1007/s00037-024-00256-1.

[Gur01] Venkatesan Guruswami. *List decoding of error correcting codes*. PhD thesis, Massachusetts Institute of Technology, 2001. URL: http://dspace.mit.edu/handle/1721.1/8700.

[Gur11] Venkatesan Guruswami. Linear-algebraic list decoding of folded reed-solomon codes. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity, CCC 2011, San Jose, California, USA, June 8-10, 2011*, pages 77–85. IEEE Computer Society, 2011. doi:10.1109/CCC.2011.22.

[GUV09] Venkatesan Guruswami, Christopher Umans, and Salil P. Vadhan. Unbalanced expanders and randomness extractors from Parvaresh-Vardy codes. *J. ACM*, 56(4):20:1–20:34, 2009. (Preliminary version in *22nd CCC*, 2007). URL: https://doi.org/10.1145/1538902.1538904.

[GW13] Venkatesan Guruswami and Carol Wang. Linear-algebraic list decoding for variants of Reed-Solomon codes. *IEEE Trans. Inform. Theory*, 59(6):3257–3268, 2013. (Preliminary version in *26th IEEE Conference on Computational Complexity*, 2011 and *15th RANDOM*, 2011). URL: https://doi.org/10.1109/TIT.2013.2246813.

[GX13] Venkatesan Guruswami and Chaoping Xing. List decoding reed-solomon, algebraic-geometric, and gabidulin subcodes up to the singleton bound. In *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing*, STOC '13, page 843–852, New York, NY, USA, 2013. Association for Computing Machinery. doi:10.1145/2488608.2488715.

[GX22] Venkatesan Guruswami and Chaoping Xing. Optimal rate list decoding over bounded alphabets using algebraic-geometric codes. *J. ACM*, 69(2), January 2022. doi:10.1145/3506668.

[IV22] Ferdinand Ihringer and Jacques Verstraëte. Large $(k; r, s; n, q)$-sets in projective spaces, 2022. URL: https://arxiv.org/abs/2211.04329, arXiv:2211.04329.

[JMST25] Fernando Granha Jeronimo, Tushant Mittal, Shashank Srivastava, and Madhur Tulsiani. Explicit codes approaching generalized Singleton bound using expanders. In

Michal Koucký and Nikhil Bansal, editors, *Proc. 57th ACM Symp. on Theory of Computing (STOC)*, pages 843–854, 2025. URL: https://doi.org/10.1145/3717823.3718302, arXiv:2502.07308.

[JS26] Fernando Granha Jeronimo and Nikhil Shagrithaya. Probabilistic guarantees to explicit constructions: Local properties of linear codes. In Aditya Bhaskara and Artur Czumaj, editors, *Proceedings of the 58th Annual ACM Symposium on Theory of Computing, STOC 2026, Salt Lake City, UT, USA, June 22-26, 2026*, pages 806–813. ACM, 2026. doi:10.1145/3798129.3800795.

[Kop15] Swastik Kopparty. List-decoding multiplicity codes. *Theory Comput.*, 11:149–182, 2015. URL: https://doi.org/10.4086/toc.2015.v011a005, doi:10.4086/TOC.2015.V011A005.

[KRSW23] Swastik Kopparty, Noga Ron-Zewi, Shubhangi Saraf, and Mary Wootters. Improved list decoding of folded reed-solomon and multiplicity codes. *SIAM J. Comput.*, 52(3):794–840, 2023. URL: https://doi.org/10.1137/20m1370215, doi:10.1137/20M1370215.

[KRZ26] Mrinal Kumar and Noga Ron-Zewi. Advances in list decoding of polynomial codes, 2026. URL: https://arxiv.org/abs/2603.03841, arXiv:2603.03841.

[Li23] Xin Li. Two source extractors for asymptotically optimal entropy, and (many) more. In *64th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2023, Santa Cruz, CA, USA, November 6-9, 2023*, pages 1271–1281. IEEE, 2023. doi:10.1109/FOCS57990.2023.00075.

[LMS25] Matan Levi, Jonathan Mosheiff, and Nikhil Shagrithaya. Random reed-solomon codes and random linear codes are locally equivalent. In *2025 IEEE 66th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 2097–2131, 2025. doi:10.1109/FOCS63196.2025.00112.

[LNZ26] Jeck Lim, Jiaxi Nie, and Ji Zeng. Evasive sets, twisted varieties, and container-clique trees. In Kasper Green Larsen and Barna Saha, editors, *Proceedings of the 2026 Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2026, Vancouver, BC, Canada, January 11-14, 2026*, pages 6199–6211. SIAM, 2026. doi:10.1137/1.9781611978971.221.

[LS25] Ray Li and Nikhil Shagrithaya. Near-optimal list-recovery of linear code families. In Alina Ene and Eshan Chattopadhyay, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2025, August 11-13, 2025, Berkeley, CA, USA*, volume 353 of *LIPIcs*, pages 53:1–53:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2025. URL: https://doi.org/10.4230/LIPIcs.APPROX/RANDOM.2025.53, doi:10.4230/LIPICS.APPROX/RANDOM.2025.53.

[MTS24] Aleksa Milojević, István Tomon, and Benny Sudakov. Incidence bounds via extremal graph theory, 2024. URL: https://arxiv.org/abs/2401.06670, arXiv:2401.06670.

[PR04] Pavel Pudlák and Vojtěch Rödl. Pseudorandom sets and explicit constructions of Ramsey graphs. In *Complexity of computations and proofs*, volume 13 of *Quad. Mat.*, pages 327–346. Dept. Math., Seconda Univ. Napoli, Caserta, 2004.

[RW18] Atri Rudra and Mary Wootters. Average-radius list-recoverability of random linear codes. In Artur Czumaj, editor, *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2018, New Orleans, LA, USA, January 7-10, 2018*, pages 644–662. SIAM, 2018. doi:10.1137/1.9781611975031.42.

[Sri25] Shashank Srivastava. Improved list size for folded Reed-Solomon codes. In Yossi Azar and Debmalya Panigrahi, editors, *Proc. 36th Annual ACM-SIAM Symp. on Discrete Algorithms (SODA)*, pages 2040–2050, 2025. URL: https://doi.org/10.1137/1.9781611978322.64, arXiv:2410.09031.

[ST24] Benny Sudakov and István Tomon. Evasive sets, covering by subspaces, and point-hyperplane incidences. *Discret. Comput. Geom.*, 72(3):1333–1347, 2024. doi:10.1007/s00454-023-00601-1.

[ST25] Shashank Srivastava and Madhur Tulsiani. List decoding expander-based codes up to capacity in near-linear time. 2025. doi:10.1109/FOCS63196.2025.00077.

[SZ26] Andrew Suk and Ji Zeng. On higher dimensional point sets in general position. *Combin. Probab. Comput.*, 35(1):134–148, 2026. doi:10.1017/s0963548325100254.

[Tam24] Itzhak Tamo. Tighter list-size bounds for list-decoding and recovery of folded reed-solomon and multiplicity codes. *IEEE Trans. Inf. Theory*, 70(12):8659–8668, 2024. doi:10.1109/TIT.2024.3402171.

[YZ24] Takashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure. *Journal of the ACM*, 71(3):1–50, June 2024. URL: http://dx.doi.org/10.1145/3658665, doi:10.1145/3658665.

[ZP81] Victor Vasilievich Zyablov and Mark Semenovich Pinsker. List concatenated decoding. *Problemy Peredachi Informatsii*, 17(4):29–33, 1981.

A Comprehensive Table of Prior Work

In Table 2, we present a comprehensive version of Table 1 which details essentially all prior works on list-recovery.

Codes	Alphabet size $\lvert\Sigma\rvert$	List size L	Explicit?
Random Linear Codes [ZP81, Gur01, RW18, LS25]	$\ell^{O(1/\varepsilon)}$	$(\ell/\varepsilon)^{O(\ell/\varepsilon)}$	No
Random Linear Codes [BCDZ26a]	$\ell^{(\ell/(R+\varepsilon))^{O(1+R/\varepsilon)}/\varepsilon}$	$\left(\frac{\ell}{R+\epsilon}\right)^{O(1+R/\varepsilon)}$	No
Random Linear Codes [GG26a]	$(\frac{\ell}{R+\varepsilon})^{O((R+\varepsilon)/\varepsilon^2)}$	$\left(\frac{\ell}{R+\epsilon}\right)^{O(1+R/\varepsilon)}$	No
Random Codes	$\ell^{O(1/\varepsilon)}$	$O(\ell/\varepsilon)$	No
Folded RS Codes [GR08]	$\left(\frac{n}{\varepsilon^2}\right)^{O(\log(\ell)/\varepsilon^2)}$	$\left(\frac{n}{\varepsilon^2}\right)^{O(\log(\ell)/\varepsilon^2)}$	Yes
Folded RS Codes & Subspace Evasive Sets [DL12]	$\left(\frac{n}{\varepsilon^2}\right)^{O(\log(\ell)/\varepsilon^2)}$	$(\frac{1}{\varepsilon})^{O(1/\varepsilon^3)}$	Yes
Univariate Multiplicity Codes [Kop15]	$\left(\frac{n}{\varepsilon^2}\right)^{O(\log(\ell)/\varepsilon^2)}$	$\left(\frac{n}{\varepsilon^2}\right)^{O(\log(\ell)/\varepsilon^2)}$	Yes
Folded RS/Univariate Multiplicity Codes [GW13]	$\left(\frac{n\ell}{\varepsilon^2}\right)^{O(\ell/\varepsilon^2)}$	$\left(\frac{n\ell}{\varepsilon}\right)^{O(\ell/\varepsilon)}$	Yes
Folded RS/Univariate Multiplicity Codes [KRSW23, Tam24]	$\left(\frac{n\ell}{\varepsilon^2}\right)^{O(\ell/\varepsilon^2)}$	$(\ell/\varepsilon)^{O((1+\log\ell)/\varepsilon)}$	Yes
Folded RS plus AEL Codes [KRSW23]	$(\frac{\ell}{\varepsilon})^{O(\ell^2\log(\ell/\varepsilon)/\varepsilon^2)}$	$\ell^{O(1/\varepsilon^4)}$	Yes
Folded AG Codes [GX13, GK16]	$\exp\left(\frac{\ell\log(\ell/\varepsilon)}{\varepsilon^2}\right)$	$2^{2^{2^{O_{\varepsilon,\ell}(\log^*(n))}}}$	Yes
AG Codes + BTT evasive subspace [GRZ21]	$(\frac{\ell}{\varepsilon})^{O(\ell/\varepsilon^2)}$	$\exp(\mathrm{poly}(\ell/\varepsilon))$	Yes
Codes Based on the AEL Framework [ST25]	$\exp(\exp(\ell/\varepsilon\log(\ell/\varepsilon)))$	$\exp(\exp(\ell/\varepsilon\log(\ell/\varepsilon)))$	Yes
Codes Based on the AEL Framework [JS26]	$\exp((\ell/\varepsilon)^{(\ell/\varepsilon)^{(\ell/\varepsilon)}})$	$(\ell/\varepsilon)^{O(\ell/\varepsilon)}$	Yes
Folded RS/Univariate Multiplicity Codes [BCDZ26a]	$\left(\frac{n\ell}{\varepsilon^2}\right)^{O(\ell/\varepsilon^2)}$	$\left(\frac{\ell}{R+\epsilon}\right)^{O(1+R/\varepsilon)}$	Yes
Codes Based on the AEL Framework [GGH26]	$\exp(\exp(O(\ell^2/\varepsilon^2)))$	$\left(\frac{\ell}{R+\epsilon}\right)^{O(1+R/\varepsilon)}$	Yes
RS codes + Subspace Evasive Sets **(Theorem 30)**	$n^{O(1/\varepsilon^2)}$	$O(\frac{\ell}{\varepsilon^3}\log\frac{\ell}{\varepsilon})$	Yes
AG codes + Subspace Evasive Sets **(Theorem 35)**	$(\frac{\ell}{\varepsilon})^{O(\ell/\varepsilon^2)}$	$\mathrm{poly}(\ell/\varepsilon)$	Yes
Folded RS codes + Subspace Evasive Sets **(Theorem 37)**	$(\frac{n\ell}{\varepsilon^2})^{O(\ell/\varepsilon^2)}$	$O(\frac{\ell}{\varepsilon^2}\log\frac{\ell}{\varepsilon})$	Yes
AEL codes + Subspace Evasive Sets **(Theorem 33)**	$\exp(\exp(\ell^2/\varepsilon^2))$	$O(\frac{\ell}{\varepsilon^2}\log\frac{\ell}{\varepsilon})$	Yes
Any Linear Code [GLM$^+$22, CZ25, LMS25, LS25]	Any	$\ell^{\Omega(R/\varepsilon)}$	Lower Bound
Classical AEL Codes [BCPZ26]	Any	$\ell^{\Omega(R/\varepsilon)}$	Lower Bound

Table 2: This table gives a summary of many constructions of list-recoverable codes as well as some known limitations.

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il