Electronic Colloquium on Computational Complexity, Report No. 57 (2026)

Explicit Constant-Alphabet Subspace Design Codes

Rohan Goyal* Venkatesan Guruswami† Jun-Ting Hsieh ‡

April 16, 2026

Abstract

The subspace design property for additive codes is a higher-dimensional generalization of the minimum distance property. As shown recently [BCDZ25b], it implies that the code has similar performance as random linear codes with respect to all "local properties". Explicit algebraic codes, such as folded Reed-Solomon and multiplicity codes, are known to have the subspace design property, but they need alphabet sizes that grow as a large polynomial in the block length. Constructing explicit constant-alphabet subspace design codes was subsequently posed as an open question in [BCDZ25b].

In this work, we answer their question and give explicit constructions of subspace design codes over constant-sized alphabets, using the expander-based Alon-Edmonds-Luby (AEL) framework. This generalizes the recent work of [JS25], which showed that such codes share local properties of random linear codes. Our work obtains this consequence in a unified manner via the subspace design property. In addition, our approach yields some improvements in parameters for list-recovery.

*Massachusetts Institute of Technology, Cambridge rohan_g@mit.edu.
†University of California, Berkeley venkatg@berkeley.edu.
‡Massachusetts Institute of Technology, Cambridge juntingh@mit.edu.

ISSN 1433-8092

Contents

1 Introduction

In coding theory, a fundamental goal is to understand the trade-offs between different parameters of a code, such as its rate, distance, alphabet size, as well as error-tolerance properties like list-decodability and list-recoverability. In most parameter regimes, the best known trade-offs are obtained via probabilistic arguments showing that some random ensemble of codes meet the desired bounds. These existential results provide a benchmark for what is information-theoretically possible.

For many applications, however, one often seeks explicit deterministic constructions that approach the guarantees of random codes. Algebraic constructions provide a natural rich family of codes with strong parameters. These include Reed-Solomon codes, folded Reed-Solomon codes [GR08], and multiplicity codes [GW13, KSY14, Kop14]. Recently, there has been significant progress on the list size for list-decoding these codes [KRSW23, Tam24, Sri25, CZ25, AHS25, BCDZ25b]. In particular, it is now known [CZ25] that these codes achieve an optimal trade-off of list-decodability up to an error fraction $1 - R - \varepsilon$ with list size $O(1/\varepsilon)$, where R is the rate. However, a major limitation is that these well-studied algebraic codes typically require the alphabet size to be growing with the block length of the code.[1]

This leads to an important question: can one construct explicit codes over a *constant-sized alphabet* (independent of the block length) with similar guarantees as random ones? Recently, there has been significant progress in this direction, particularly through combinatorial constructions based on expander graphs. A remarkable work [JMST25] showed how expander-based constructions via the "AEL framework" (which is also the focus in this work and will be described in Section 1.1) can yield constant-alphabet codes matching the list-decoding performance of algebraic codes such as folded Reed-Solomon codes (including the optimal list size). A subsequent work [ST25] even gave near-linear-time list-decoding algorithms with such guarantees. Following this paradigm, a recent work of Jeronimo and Shagrithaya [JS25] showed that the AEL framework can transform (small) random linear codes into explicit codes while preserving a broad class of "local" properties.

Local properties. We first give a brief overview of *local coordinate-wise linear (LCL) properties* introduced in [LMS25], which generalize various previous notions of local properties [ST20, MRR+21, GM22, GMR+22, GZ23, GM24]. We will restrict to $\mathbb{F}$-additive codes (i.e., $\mathbb{F}$-linear codes with alphabet $\mathbb{F}^s$ for some $s \in \mathbb{N}$). Informally, a property of a code is LCL if it is witnessed by a small set of distinct codewords $x^{(1)}, \ldots, x^{(L)} \in C$ such that, for each $i \in [n]$, the entries $(x_i^{(j)})_{j \in [L]}$ satisfy certain linear constraints. Typically, we are interested in the *complement* of LCL properties; that is, we would like a code that does not contain distinct codewords $x^{(1)}, \ldots, x^{(L)}$ satisfying any property in some family of LCL properties. For example, a code is list-decodable if it does *not* contain L codewords close to any arbitrary vector, and this can be precisely captured by such local linear constraints.

The LCL framework captures several fundamental properties including list-decodability, list-recoverability, average pairwise distance [CGV13], list-decodability from burst errors [RV09], and

[1] An exception is the family of Algebraic-Geometry (AG) codes. There are explicit constructions of optimal-rate list-decodable AG codes over constant-sized alphabets [GR22, GX22], but analogous results for list-recovery are still unknown.

proximity gaps [GG25a]. With this unified lens, Levi, Mosheiff and Shagrithaya [LMS25] showed precise threshold theorems with respect to LCL properties for random linear codes in $\mathbb{F}_q$ as well as random Reed-Solomon codes, hence recovering several known results [BGM24, AGG+25].

Motivated by this, in an exciting work, Jeronimo and Shagrithaya [JS25] showed explicit constructions that achieve the same guarantees as random linear codes for *any* LCL property. Their construction is based on the Alon-Edmonds-Luby (AEL) construction [AEL95], which is a generalization of the graph-based distance amplification technique of [ABN+92]. This framework has since been used in several explicit code constructions [KMRS17, HW18, KRSW23, JMST25, ST25, JS25].

An underlying theme of the AEL framework is a "local-to-global" phenomenon,[2] where one uses a "pseudorandom" object, such as an expanding graph, to lift properties of a small constant-sized object to an infinite family of large objects. Jeronimo and Shagrithaya showed that this paradigm extends to LCL properties. Starting from a constant-sized code with LCL properties matching random linear codes (which can be obtained by brute force), the AEL construction gives an infinite family of codes that inherit these properties. We define the AEL construction and provide a more detailed discussion of [JS25] in Sections 1.1 and 1.3.

Subspace design captures all local properties. In another novel recent work, Brakensiek, Chen, Dhar, and Zhang [BCDZ25b] showed that a property known as *subspace design* simultaneously captures *all* LCL properties. A subspace design, first introduced by Guruswami and Xing [GX13], is a collection $\{H_1, \dots, H_n\}$ of linear subspaces in $\mathbb{F}^m$ such that for any low-dimensional subspace $A \subseteq \mathbb{F}^m$, the average intersection $\mathbb{E}_i \dim(H_i \cap A)$ is much smaller than $\dim(A)$. For an $\mathbb{F}_q$-additive code $C \subseteq (\mathbb{F}_q^s)^n$, we say that it is a subspace design code if the collection $\{C_i\}_{i\in[n]}$, where $C_i = \{x \in C \mid x_i = 0\}$, forms a subspace design; see Definition 2.3 for the formal definition. Note that this property necessarily requires the code to be *folded*, i.e., over an alphabet $\mathbb{F}_q^s$ for some sufficiently large s. Indeed, if C is $\mathbb{F}$-linear over $\mathbb{F}$ and $A \subseteq C$ is any subspace, then the restriction $x_i = 0$ imposes only a single linear constraint, and thus $\dim(C_i \cap A) \geqslant \dim(A) - 1$.

Guruswami and Kopparty [GK16] showed that folded Reed–Solomon codes and univariate multiplicity codes satisfy the subspace design property. The aforementioned work of Chen and Zhang [CZ25] on optimal list-decodability of folded Reed-Solomon codes in fact showed that the subspace design property with optimal parameters implies optimal list-decodability. Specifically, this implies that folded Reed-Solomon codes and univariate multiplicity codes achieve optimal list-decoding bounds.

Recently, Brakensiek et. al. [BCDZ25b] showed that being a subspace design code is the unifying property for the LCL framework of [LMS25]. At a high level, they showed that if random codes with rate R avoids a local property $\mathcal{V}$ with high probability, then any near-optimal subspace design code with rate close to R also does not contain $\mathcal{V}$. By [GK16], their result implies explicit codes that simultaneously simulate all local properties of random linear codes.

However, such codes require the alphabet size to be at least polynomial in the block length. For constant-alphabet subspace design codes, [BCDZ25b] proved existence by showing that a (folded) random linear code satisfies the subspace design property with high probability (see

[2] The local-to-global principle has been highly successful across theoretical computer science, from the classical Tanner codes [Tan81, SS96], the PCP theorem [AS98, ALM+98, Din07], to recent developments such as locally testable codes [DEL+22, PK22] and vertex expanders [HMMP24, HLM+25a, HLM+25b].

Theorem 2.6). They further posed the explicit construction of near-optimal subspace design codes over constant-sized fields as an open question.

Our work: explicit subspace design codes. We give explicit constructions of *subspace design codes* over constant-sized alphabets, This resolves the above-mentioned open question of [BCDZ25b], and also abstracts and generalizes the framework of [JMST25, JS25]. As mentioned earlier, the subspace design property alone implies (the avoidance of) *all* LCL properties shown for random linear codes and the construction of [JS25].

Theorem 1.1. *For any finite field $\mathbb{F}_q$, positive integer r, and reals $R, \varepsilon \in (0,1)$, there exists an explicit $\mathbb{F}_q$-additive code $C \subseteq \Sigma^n$ of rate R and alphabet $\Sigma = \mathbb{F}_q^{\mathrm{poly}(r,1/\varepsilon)\cdot q^{r^2}}$ such that for any subspace $A \subseteq C$ of dimension at most r, we have that*

$$\frac{1}{n}\sum_{i=1}^{n} \dim(A_i) \leqslant (R+\varepsilon)\cdot \dim(A)\,, \tag{1}$$

where $A_i = \{x \in A \mid x_i = 0\}$.

The guarantee in Theorem 1.1 is precisely the definition of a subspace design code. In words, for any low-dimensional subspace $A \subseteq C$, restricting a coordinate to 0 reduces the dimension to roughly $R \cdot \dim(A)$ on average. Our alphabet size is $\exp(\exp(r^2))$ when q is a constant, and it is an interesting question whether a better analysis could yield a smaller alphabet. We note that because of the q^{r^2} term, we can even choose $\varepsilon \leqslant q^{-o(r^2)}$.

Remark 1.2 (Distance and the subspace design parameter)**.** Suppose $A = \mathrm{span}\{x^*\}$ is a 1-dimensional subspace, where $x^* \in C$ is a minimum-weight codeword of relative weight δ. Then, $\frac{1}{n}\sum_{i=1}^{n} \dim(A_i) = 1-\delta$, since $A_i = \{0\}$ whenever $x^*_i \neq 0$. Thus, Equation (1) implies that the distance of our code $\delta \geqslant 1 - R - \varepsilon$, which approaches the Singleton bound $\delta \leqslant 1 - R + o(1)$.

On the other hand, the Singleton bound also implies that $\frac{1}{n}\sum_{i=1}^{n} \dim(A_i) \geqslant R - o(1)$. In particular, Equation (1) in Theorem 1.1 is almost optimal.

Focusing on the single subspace design property allows us to obtain an arguably simpler analysis and better parameters for downstream applications. To compare with prior work, we consider list-recovery, which was in fact one of the original motivations of studying LCL properties and subspace design. Using the reduction from subspace design to list-recovery established in [BCDZ25b], our construction achieves a list size bound that matches the best known bound for any linear code. Moreover, among explicit constructions with near-optimal list sizes, our construction has the smallest alphabet size. In Section 1.4, we give a more detailed discussion, including a comparison with prior work in Table 1.

For concreteness, we also include list-decoding, list-recovery, and curve-decoding parameters for our construction in Section 5. These results follow directly from the results of [CZ25, BCDZ25b, GG25a].

1.1 The Alon-Edmonds-Luby (AEL) construction

Our construction is based on the Alon-Edmonds-Luby (AEL) framework [AEL95], which we present in this section.

Definition 1.3 (The Alon-Edmonds-Luby (AEL) construction)**.** Given

(1) an outer code C_{out} with an encoder $\mathsf{Enc}_{\text{out}} : \Sigma_{\text{out}}^k \to (\Sigma^{k_{\text{in}}})^n$,

(2) an inner code C_{in} with an encoder $\mathsf{Enc}_{\text{in}} : \Sigma^{k_{\text{in}}} \to \Sigma^d$, and

(3) a d-regular bipartite graph $G = (V_{\text{left}}, V_{\text{right}}, E)$ with $V_{\text{left}} = V_{\text{right}} = [n]$, where for each vertex, there is a fixed ordering of its incident edges.

The AEL code $C_{\text{AEL}} = C_{\text{AEL}}(C_{\text{out}}, C_{\text{in}}, G) \subseteq (\Sigma^d)^n$ is defined as follows. For any message $x \in \Sigma_{\text{out}}^k$, we first encode it with the outer code and obtain $y = \mathsf{Enc}_{\text{out}}(x) \in (\Sigma^{k_{\text{in}}})^n$. Each entry y_i is an element in $\Sigma^{k_{\text{in}}}$, and we encode it using the inner code, which gives $\mathsf{Enc}_{\text{in}}(y_i) \in \Sigma^d$. Then, we place each entry of $\mathsf{Enc}_{\text{in}}(y_i)$ on the d incident edges of vertex i in V_{left}. The final codeword $z \in (\Sigma^d)^n$ is such that for each $j \in V_{\text{right}}$, $z_j \in \Sigma^d$ is the collection of elements on the incident edges of j.

In most settings, $|\Sigma|$, k_{in} and d are constants, and the inner code is viewed as a *random* code, since one can obtain a code with properties matching those of random codes by brute force. The graph G is chosen to be a spectral expander, for which explicit constructions are well known. For the outer code C_{out}, one may choose explicit codes tailored to the application. In [HW18], list-recoverable codes (for erasures) were used, and it was shown that C_{AEL} inherits this property. In [KMRS17], they used multiplicity codes of [KSY14] (in the sub-constant distance regime) and showed that C_{AEL} inherits the local correctability of the outer code. In [KRSW23], they instantiated the outer code using folded Reed-Solomon codes and showed that C_{AEL} inherits the list-recovery property.

In an exciting work, Jeronimo, Mittal, Srivastava, and Tulsiani [JMST25] showed that it suffices for the outer code to have constant distance in order for C_{AEL} to be list-decodable up to capacity. In particular, this removes any application-specific requirement on the outer code, yielding the first purely combinatorial codes approaching the generalized Singleton bound. Their construction relies solely on properties of the "random" inner code, and they interpreted this as another instance of a "local-to-global" phenomenon, where properties of a constant-sized object transfer to an infinite family of large objects.

1.2 Overview of our work

Our construction also follows the "local-to-global" paradigm of the AEL framework (Definition 1.3). It was proved in [BCDZ25b] that a folded random linear code satisfies near-optimal subspace design with high probability (Theorem 2.6), and thus we can use it as the inner code. In our main theorem (Theorem 4.2), we show that the AEL construction inherits the subspace design property of the inner code, as long as the outer code has constant distance and the graph is a sufficiently good expander.

In our analysis, we use an abstract interpretation of the LCL properties in [LMS25]. Previously, local properties are defined with respect to a locality parameter L (e.g., the list size in the context of list-decoding and list-recovery). In [LMS25], a *local profile* is defined to be a tuple of subspaces $(V_1, \ldots, V_n)$, where each V_i is a subspace in $\mathbb{F}_q^L$. For technical issues related to differing field sizes and block lengths, [JS25] defined it as a tuple of matrices $(M_1, \ldots, M_n)$ in

$\mathbb{F}_q^{L\times L}$, and a code C contains a local profile if there are L distinct codewords such that their i-th coordinates, viewed as a vector in $\mathbb{F}_q^L$, is in the kernel of M_i.

We define local profiles more abstractly as a tuple of subspaces $(V_1, \ldots, V_n)$ in an arbitrary vector space V over $\mathbb{F}_q$. A $\mathbb{F}_q$-additive code $C \subseteq (\mathbb{F}_q^s)^n$ contains $(V_1, \ldots, V_n)$ if there exist a subspace $A \subseteq \mathbb{F}_q^k$ (in the message space) and an isomorphism $\varphi : V \to A^*$, where A^* denotes the dual space of A (i.e., the set of linear functionals from $A \to \mathbb{F}_q$), that satisfy the following: for each $i \in [n]$, $\varphi(V_i)$ (a subspace of A^*) has kernel (a subspace of A) contained in $\ker(\mathsf{Enc}_i)$, where $\mathsf{Enc}_i : \mathbb{F}_q^k \to \mathbb{F}_q^s$ is the encoding map for coordinate i. See Definition 3.3 for the formal definition. Although more abstract, we find that this definition avoids technicalities encountered in prior work and also leads to a more streamlined proof.

With this definition, we show an equivalence statement for subspace design codes (Theorem 3.5): the τ-subspace design property is equivalent to the property that every local profile $(V_1, \ldots, V_n)$ contained in C satisfies $\Phi \geqslant 0$, where Φ is some potential function depending only on the parameter τ and the average of $\dim(V_i)$. We note that similar potential functions were also used in [LMS25] and [JS25].

With this equivalence in hand, our analysis roughly goes as follows. Suppose our code contains any local profile $(V_1, \ldots, V_n)$ with $\Phi < 0$, due to a subspace $A \subseteq \mathbb{F}_q^k$. Then, transferring this to the left side of the AEL construction, the expansion of the graph implies that most inner codes also have local profiles $(V_{N_1(j)}, \ldots, V_{N_d(j)})$ with negative potential; here $j \in V_{\text{left}}$ and $N_1(j), \ldots, N_d(j)$ are its d neighbors in V_{right}. However, by the subspace design property of the inner codes, this forces $\mathsf{Enc}_{\text{out},j}(A) = 0$ for most indices j, contradicting the distance of the outer code.

1.3 The work of [JS25]

In this section, we briefly discuss the work of [JS25]. Jeronimo and Shagrithaya [JS25] showed that any LCL property satisfied (or avoided) by the inner code can be transferred to the AEL code. Since the inner code is a "random" code, we know precise characterizations of what LCL properties it avoids (due to [LMS25]). Thus, if there are L distinct codewords that satisfy a local profile, which they define as a tuple of $L \times L$ matrices $(M_1, \ldots, M_n)$, then porting over to the left side, it follows that most inner codewords satisfy a close approximation of the local profiles, which would be a contradiction.

The above is a simplified overview of [JS25] that hides several details. A challenge that they need to overcome is that the inner codewords may not be pairwise distinct. To overcome this, they need to work with a *robust* version of *implied* local profiles (which also appear implicitly in [LMS25]), which we will not elaborate here. One advantage of working directly with subspace design in our work is that we avoid such technical subtleties.

Threshold rates may change over extension fields. A crucial detail we would like to point out is that the construction of [JS25], particularly the inner code, is $\mathbb{F}_q$-linear, while the LCL properties are over a subfield $\mathbb{F}_{q_0}$ (i.e., $M_i \in \mathbb{F}_{q_0}^{L\times L}$ where $q_0 < q$ are powers of the same prime).

The inner code they chose is a random $\mathbb{F}_q$-linear code.[3] This leads to their construction working only for local properties over $\mathbb{F}_{q_0}$ whose threshold rates are the same for random linear

[3] From personal communication, the authors of [JS25] suggest that their proof goes through if they chose the inner code to be $\mathbb{F}_{q_0}$-additive.

codes over extension fields. It is conceivable that for some properties of interest, the threshold over an extension field may be different. This is *not* a concern for list-decoding and list-recovery (the primary application of [JS25]), as we know that the thresholds for these properties are independent of the field extension.

On the other hand, one might consider some properties that $\mathbb{F}_{q_0}$-additive codes can have, but for which it is unclear whether $\mathbb{F}_q$-linear codes can have them. As a concrete example, we mention a local property that was shown by [GG25a] to hold for $\mathbb{F}_{q_0}$-additive subspace design codes, but is not known to hold for codes linear over an extension of $\mathbb{F}_{q_0}$.

An $\mathbb{F}_{q_0}$-additive code $C \subseteq \Sigma^n$ is said to be *low-dimension-recoverable* if, for any 1-dimensional $\mathbb{F}_{q_0}$-linear spaces $A_1, \ldots, A_n \subseteq \Sigma$, the space of all codewords $c \in A_1 \times A_2 \times \cdots \times A_n$ is $O(1)$-dimensional. This is naturally a property that linear codes over $\Sigma = \mathbb{F}_{q_0}$ can never have, as then we would have $A_1 \times \cdots \times A_n = \Sigma^n$. On the other hand, $\mathbb{F}_{q_0}$-additive subspace design codes of rate $1/2$ do have this property [GG25a], but we do not know if rate $1/2$ $\mathbb{F}_q$-linear codes for any proper extension $\mathbb{F}_q$ of $\mathbb{F}_{q_0}$ possess such low-dimensional recoverability.

Note that since we construct subspace design codes in this work, our codes naturally inherit *all* LCL properties that hold for subspace design codes, including low-dimensional recoverability.

1.4 Comparison to prior work on list-recovery

For comparison with prior work, we focus on list-recovery of our construction. A code $C \subseteq \Sigma^n$ is (ρ, ℓ, L)-list recoverable if for every collection of sets $S_1, S_2, \ldots, S_n \subseteq \Sigma$, each $|S_i| \leqslant \ell$, there are at most L codewords $c \in C$ that are distance $\leqslant \rho$ away from $S_1 \times S_2 \times \cdots \times S_n$, i.e.,

$$\left|\left\{c \in C \;\middle|\; |\{i \in [n] : c_i \notin S_i\}| \leqslant \rho n\right\}\right| \leqslant L\,.$$

Note that (ρ, L)-list-decodability is equivalent to $(\rho, 1, L)$-list-recoverability.

Brakensiek et. al. [BCDZ25a] showed a reduction from subspace design to list-recovery; see also [GG25b, Theorem 5.1]. Plugging in Theorem 1.1 to their reduction, we get the following as an immediate corollary.

Corollary 1.4 (Consequence of [BCDZ25a])**.** *Our code $C \subseteq \Sigma^n$ from Theorem 1.1 of rate R and alphabet $\Sigma = \mathbb{F}_q^{\mathrm{poly}(\ell/\varepsilon)\cdot q^{2\ell^2/\varepsilon^2}}$ is $(1 - R - \varepsilon, \ell, L)$-list-recoverable for*

$$L \leqslant \left\lceil \left(\frac{\ell}{R+\varepsilon}\right)^{\frac{R}{\varepsilon}+1} \right\rceil .$$

In Table 1, we compare our list-recovery parameters with prior constructions. Note that our list size upper bound $L \leqslant \left(\frac{\ell}{R+\varepsilon}\right)^{O(R/\varepsilon+1)}$ matches the best known list size bound for random linear codes (in fact, any additive code), which is expected since optimal subspace design codes simulate all local properties of random linear codes [BCDZ25b]. Moreover, this bound is almost tight as it was shown that all linear codes must have $L \geqslant \ell^{\Omega(R/\varepsilon)}$ [CZ25, LMS25, LS25]. Among explicit constructions with near-optimal list size, folded Reed-Solomon and multiplicity codes [BCDZ25b] naturally require an alphabet size polynomial in n, while the construction of [JS25] has a constant alphabet but is exponentially larger than ours.

Constructions	List size L	Alphabet size $\lvert\Sigma\rvert$	Explicit?
Random linear codes [LS25]	$(\ell/\varepsilon)^{O(\ell/\varepsilon)}$	$\ell^{O(1/\varepsilon)}$	No
Random linear codes [BCDZ25a]	$\left(\frac{\ell}{R+\varepsilon}\right)^{O(R/\varepsilon+1)}$	$\ell^{(\frac{\ell}{R+\varepsilon})^{O(R/\varepsilon)}/\varepsilon}$	No
[KRSW23]	$(\ell/\varepsilon)^{(\ell/\varepsilon)^2\log(\ell/\varepsilon)}$	$\ell^{O(1/\varepsilon^4)}$	Yes
[ST25]	$\exp\left(\exp\left(\widetilde{O}(\ell/\varepsilon)\right)\right)$	$\exp\left(\exp\left(\widetilde{O}(\ell/\varepsilon)\right)\right)$	Yes
[BCDZ25b]	$\left(\frac{\ell}{R+\varepsilon}\right)^{O(R/\varepsilon+1)}$	$(n\ell/\varepsilon^2)^{O(\ell/\varepsilon^2)}$	Yes
[JS25]	$\left(\frac{\ell}{R+\varepsilon}\right)^{O(R/\varepsilon+1)}$	$\exp\left(\exp\left(\exp\left(\widetilde{O}(\ell/\varepsilon)\right)\right)\right)$	Yes
Our work	$\left(\frac{\ell}{R+\varepsilon}\right)^{O(R/\varepsilon+1)}$	$\exp\left(\exp\left(O(\ell^2/\varepsilon^2)\right)\right)$	Yes
Any linear code [LS25]	$\geqslant \ell^{\lfloor\max(R/\varepsilon,1)\rfloor}$	Any	-

Table 1: Adapted from [KRSW23, BCDZ25b, JS25]. Constructions of $(1-R-\varepsilon,\ell,L)$-list-recoverable codes of constant rate $R\in(0,1)$.

One concrete place where we get an improvement in the alphabet size is the following. To study list-recovery using the LCL framework, one needs to look at high locality properties, namely $L=\ell^{O(1/\varepsilon)}$-local LCL properties. In our case, we only need to consider $O(\ell/\varepsilon)$-dimensional subspaces, which saves an exponential factor.

1.5 Organization

We organize our paper as follows. In Section 2, we introduce some preliminaries. In Section 3, we define the potential function and local profiles, and we show equivalence statements for subspace design codes. Then, in Section 4, we prove our main theorem (Theorem 4.2), which implies Theorem 1.1. Finally, in Section 5, we present the list-decoding, list-recovery, and curve-decoding parameters for our construction.

2 Preliminaries

We begin by introducing the basic coding-theoretic definitions we will be using. For any two vectors x,y in Σ^n where Σ is some alphabet, we define the fractional Hamming distance $\Delta(x,y)=\frac{1}{n}|\{i\in[n]:x_i\neq y_i\}|$ to be the fraction of coordinates where they differ. For a set $S\subseteq\Sigma^n$, we define $\Delta(x,S)=\min_{y\in S}\Delta(x,y)$ to be the fractional distance of x to its closest vector in S. Throughout this paper, all distances are taken to be fractional unless stated otherwise.

The two fundamental quantities associated with a code are its rate and distance. For a code $C\subseteq\Sigma^n$, we define its (relative) distance as $\delta(C)=\min_{x,y\in C,x\neq y}\Delta(x,y)$. Moreover, its rate $R(C)$ is defined as $R(C)=\frac{1}{n}\log_{|\Sigma|}|C|$.

In this paper, we will focus on additive codes over a finite field, defined as follows:

Definition 2.1 (Additive codes)**.** Let $\mathbb{F}$ be a finite field and let $\Sigma = \mathbb{F}^s$ for some positive integer s. A code $C \subseteq \Sigma^n$ is said to be $\mathbb{F}$-additive (or just additive when the field $\mathbb{F}$ is clear from context) if C is an $\mathbb{F}$-linear subspace of Σ^n. When $s = 1$, the code is simply called a linear code.

2.1 Vector spaces and dual spaces

We will need the following linear-algebraic notations and definitions. Let V be a finite-dimensional vector space over a field $\mathbb{F}$. We define $\mathcal{L}(V)$ to be the set of all linear subspaces of V. For subspaces U, W, we write $U + W = \{u + w \mid u \in U,\ w \in W\}$. Suppose $W \subseteq U$, then the quotient space $U/W \coloneqq \{u + W : u \in U\}$ consists of the set of cosets.

Definition 2.2. Let V be a vector space over a field $\mathbb{F}$.

- The *dual space* V^* is the vector space of all linear maps $f : V \to \mathbb{F}$.
- If $A \subseteq V$ is a subspace, its *annihilator* is

$$A^\perp \coloneqq \{f \in V^* \mid f(a) = 0\ \forall a \in A\}\,.$$

- If $B \subseteq V^*$ is a subspace, its *joint kernel* is

$$B^\circ \coloneqq \{v \in V \mid f(v) = 0\ \forall f \in B\}\,.$$

We note that the annihilator and kernel are dual concepts, i.e., $(A^\perp)^\circ = A$. For a subspace $B \subseteq V^*$ and a vector $v \in V$, we will use $Bv = 0$ to mean that $f(v) = 0$ for all $f \in B$. Thus, we can write $B^\circ = \{v \in V \mid Bv = 0\}$.

2.2 Subspace design codes

We now review the concept of subspace design codes. Subspace designs have been the driving force in many recent advances in coding theory, including [Sri25, CZ25, AHS25, BCDZ25a, BCDZ25b, GG25a, GG25b]. In the following, we use the notation as established in [GG25a].

Definition 2.3 (Subspace-Design Property)**.** For any function $\tau : \mathbb{N} \to \mathbb{R}_{\leqslant 1}$, an $\mathbb{F}_q$-additive code $C \subseteq (\mathbb{F}_q^s)^n$ is said to be a *τ-subspace design* code if for every $r \in \mathbb{N}$, and every $\mathbb{F}_q$-linear subspace A of C of dimension at most r,

$$\frac{1}{n}\sum_{i=1}^{n} \dim(A_i) \leqslant \dim(A) \cdot \tau(r)\,,$$

where $A_i = \{x \in A \mid x_i = 0\}$.

We will often use Definition 2.3 where we define the subspaces in the *message space* $\mathbb{F}_q^k$. In particular, suppose the code $C = \{(\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x)) \mid x \in \mathbb{F}_q^k\}$. Let $A' \subseteq \mathbb{F}_q^k$ is a subspace of dimension $\leqslant r$ and $A = \mathsf{Enc}(A') \subseteq C$, then A_i is precisely the subspace $\mathsf{Enc}(A' \cap \ker(\mathsf{Enc}_i))$,

and we have the following,

$$\frac{1}{n}\sum_{i=1}^{n}\dim(A' \cap \ker(\mathsf{Enc}_i)) \leqslant \dim(A') \cdot \tau(r)\,.$$

Note that the subspace design property necessarily requires the code to be *folded*, otherwise if C is $\mathbb{F}_q$-linear over $\mathbb{F}_q$, then we have $\dim(A_i) \geqslant \dim(A) - 1$ because $x_i = 0$ imposes only a single linear constraint.

Remark 2.4 (Parameter τ)**.** We can assume that $\tau(r)$ is a non-decreasing function, and moreover, the statement trivially holds when $\tau(r) = 1$. For our construction as well as known subspace design codes, τ is a function such that $\tau(r)$ is small for all small r, and $\tau(r) = 1$ otherwise.

On the other hand, from the discussion in Remark 1.2, the Singleton bound implies that $\tau(r) \geqslant R - o(1)$, where R is the rate of the code. Thus, we would like *near-optimal* subspace design codes where $\tau(r) \leqslant R + \varepsilon$ for all small r (via a sufficiently large alphabet size depending on r).

Folded Reed-Solomon codes and folded random linear codes. An s-folded Reed-Solomon code [GR08] is an $\mathbb{F}_q$-additive code in $(\mathbb{F}_q^s)^n$ where $q > sn$. Given evaluation points $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ and a primitive element $\gamma \in \mathbb{F}_q$ where $\alpha_i\gamma^t \neq \alpha_j$ for all $i \neq j$ and $t < s$, the code is obtained by encoding a polynomial $f \in \mathbb{F}_q[x]$ of degree at most k such that the i-th entry consists of the tuple $(f(\alpha_i), f(\alpha_i\gamma), \ldots, f(\alpha_i\gamma^{s-1})) \in \mathbb{F}_q^s$.

Guruswami and Kopparty [GK16] proved that folded Reed-Solomon (as well as univariate multiplicity codes) are optimal subspace design codes. This subspace design property has been at the heart of the recent progress on list-decoding and list-recovery of these codes.

Theorem 2.5 ([GK16])**.** *The s-folded Reed-Solomon codes of rate R are τ-subspace-design codes for $\tau(r) = \frac{sR}{s-r+1}$ for all $1 \leqslant r \leqslant s$ and $\tau(r) = 1$ otherwise.*

It is also known that folded random linear codes form subspace design codes as well. This result was proved in [BCDZ25b].

Theorem 2.6 ([BCDZ25b])**.** *Let $\varepsilon > 0$. Let $\mathsf{Enc}_1, \ldots, \mathsf{Enc}_n : \mathbb{F}_q^k \to \mathbb{F}_q^s$ be uniformly random linear functions. Then, with probability at least $1 - o(1)$, $C = \{(\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x)) \mid x \in \mathbb{F}_q^k\}$ is a τ-subspace design code, where $\tau(r) \leqslant R + \varepsilon$ for all $r \leqslant \varepsilon s/4$, and $R = k/sn$ denotes the code rate.*

2.3 List-decoding, list-recovery and curve-decoding from subspace designs

It was shown that list-decoding, list-recovery and curve-decoding follow from the subspace design property [CZ25, BCDZ25a, GG25a]. In this section, we state these implications, following the language of [GG25a, GG25b].

Theorem 2.7 (Average radius list-decoding of subspace design codes [CZ25, BCDZ25a])**.** *Any τ-subspace design additive code $C \subseteq (\mathbb{F}_q^s)^n$ has that for any $y \in (\mathbb{F}_q^s)^n$, and any distinct $c_1, \ldots, c_r \in$*

C, we have that

$$\sum_{i=1}^{r} \Delta(y, c_i) \geqslant (r-1)(1-\tau(r-1)) \,.$$

In particular, there exists an $i \in [r]$ such that $\Delta(c_i, y) \geqslant \frac{r-1}{r}(1-\tau(r-1))$. Thus,

$$\left| \left\{ c \in C \mid \Delta(c_i, y) < \frac{r-1}{r}(1-\tau(r-1)) \right\} \right| \leqslant r-1 \,.$$

Theorem 2.8 (List-recovery of subspace design codes [BCDZ25a])**.** *Let $\ell \in \mathbb{N}$ and $\varepsilon > 0$. For any τ subspace design additive code $C \subseteq (\mathbb{F}_q^s)^n$, for any $L_1, \ldots, L_n \subseteq (\mathbb{F}_q^s)$ such that $|L_i| = \ell$ for all $i \in [n]$, we have that*

$$|\{c \in C \mid \Delta(c_i, L_1 \times L_2 \times \cdots \times L_n) < 1 - \tau(\lceil \ell/\varepsilon \rceil) - \varepsilon\}| \leqslant \left(\frac{\ell}{\tau(\lceil \ell/\varepsilon \rceil) + \varepsilon} \right)^{(\tau(\lceil \ell/\varepsilon \rceil)+\varepsilon)/\varepsilon} .$$

The above statement was originally proven in [BCDZ25a], and a proof for the list recovery in our language of τ-subspace design codes was also presented in the appendix of [GG25b].

Additionally, we present results for curve decoding of our code constructions. Thus, we begin by defining curve-decodadibility as defined in [GG25a]. They showed that the subspace design property of codes implies curve decoding and consequentially the notions of correlated agreement and proximity gaps. For simplicity, we refrain from discussing the consequences and demonstrate the primary conclusion of curve decoding.

Definition 2.9 (Curve-decodability)**.** An $\mathbb{F}_q$-additive code $\mathcal{C} \subseteq \Sigma^n$ is (ℓ, δ, a, b) curve-decodable if for every $u_0, u_1, \ldots, u_\ell \in \Sigma^n$, all functions $f : \mathbb{F}_q \to C$, whenever the set

$$A = \left\{ \alpha \in \mathbb{F}_q \mid \Delta\big(\sum_{j=0}^{\ell} u_j \alpha^j, f(\alpha)\big) \leqslant \delta \right\}$$

has at least a elements, there exist $c_0, c_1, \ldots, c_\ell \in \mathcal{C}$ such that

$$\left| \left\{ \alpha \in A \mid f(\alpha) = \sum_{j=0}^{\ell} c_j \alpha^j \right\} \right| \geqslant b \,.$$

When $\ell = 1$, we use the phrase *line-decodable.*

Theorem 2.10 (Curve-decodability of subspace design codes [GG25a])**.** *For arbitrary positive integers r, ℓ, a and any $\varepsilon \geqslant \frac{\ell+1}{r}$, every τ-subspace design code $\mathcal{C} \subseteq \Sigma^n$ is $(\ell, 1-\tau(r)-\varepsilon, a, \frac{\varepsilon}{r+\varepsilon} \cdot a)$ curve-decodable.*

2.4 Expander graphs

We review the concept of spectral expander graphs.

Definition 2.11 (Spectral expander)**.** A d-regular bipartite graph $G = (V_{\text{left}}, V_{\text{right}}, E)$ with $|V_{\text{left}}| = |V_{\text{right}}| = n$ is called a λ-expander if its normalized biadjacency matrix A, i.e., $A_{i,j} = 1/d$

if $(i,j) \in E$ and 0 otherwise, has second singular value $\sigma_2(A) \leqslant \lambda$.

Normally, a spectral expander is defined as a non-bipartite d-regular graph whose normalized adjacency matrix satisfies $\max(\lambda_2(A), |\lambda_{\min}(A)|) \leqslant \lambda$. One can convert an n-vertex λ-expander into a bipartite λ-expander on $[n] \times [n]$ via its double cover.

It is known that the optimal value of λ is $\frac{2\sqrt{d-1}}{d}$ by the Alon-Boppana bound, and graphs achieving this bound are called Ramanujan graphs. Although we do not require such a strong bound on λ, there exist many explicit constructions of near-Ramanujan graphs [LPS88, Mar88, Mor94, MOP20, Alo21].

Theorem 2.12 ([Alo21])**.** *For every degree d, every ε, and all sufficiently large $n \geqslant n_0(d,\varepsilon)$ where nd is even, there is an explicit construction of n-vertex d-regular λ-expanders with $\lambda \leqslant \frac{2\sqrt{d-1}}{d} + \varepsilon$.*

3 Characterization of subspace designs

3.1 Potential function and local profiles

We first define a potential function given a tuple of subspaces. We note that this was also used in [LMS25, JS25].

Definition 3.1 (Potential function)**.** Let V be any finite-dimensional vector space over a field $\mathbb{F}$, and let $n \in \mathbb{N}$. Define $\Phi_V : \mathcal{L}(V) \times (\mathcal{L}(V))^n \times \mathbb{R} \to \mathbb{R}$ as follows:

$$\Phi_V(U, (V_1, \dots, V_n), \alpha) = \alpha \dim(U) - \frac{1}{n} \sum_{i=1}^{n} (\dim(U) - \dim(U \cap V_i)) \ .$$

We will drop the subscript V if it is clear from context.

We will need the following result on the potential function when we apply a surjective linear map $M : V \to V'$, which may have a kernel.

Lemma 3.2. *Let V, V' be vector spaces, let $U, V_1, \dots, V_n \in \mathcal{L}(V)$, let $M : V \to V'$ be a surjective linear map such that $\ker(M) = W \in \mathcal{L}(V)$, and let $\alpha \in \mathbb{R}$. Then,*

$$\Phi_V(U + W, (V_1, \dots, V_n), \alpha) - \Phi_V(W, (V_1, \dots, V_n), \alpha) = \Phi_{V'}(M(U), (M(V_1), \dots, M(V_n)), \alpha) \, .$$

Proof. By Definition 3.1, it suffices to prove that for each V_i,

$$\dim((U + W) \cap V_i) - \dim(W \cap V_i) = \dim(M(U) \cap M(V_i)) \, .$$

Let $X = (U + W) \cap V_i$, and consider the restriction $M|_X : X \to V'$. We have that the image $\operatorname{im}(M|_X) = M(X) = M(U + W) \cap M(V_i) = M(U) \cap M(V_i)$, since $M(W) = \{0\}$. The kernel $\ker(M|_X) = X \cap W$, which equals $W \cap V_i$ because $(U + W) \cap W = W$. Then, by the rank-nullity theorem, $\dim(X) = \dim \ker(M|_X) + \dim \operatorname{im}(M|_X) = \dim(W \cap V_i) + \dim(M(U) \cap M(V_i))$. □

Next, we define local profiles.

Definition 3.3 (Local profiles)**.** Let $\mathsf{Enc}_1, \ldots, \mathsf{Enc}_n : \mathbb{F}_q^k \to \mathbb{F}_q^s$ be linear maps for some $s \in \mathbb{N}$, and $C = \{(\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x)) \mid x \in \mathbb{F}_q^k\}$ be the associated $\mathbb{F}_q$-additive code. Throughout this paper, we will assume that C has positive distance, i.e., $\mathsf{Enc} : \mathbb{F}_q^k \to (\mathbb{F}_q^s)^n$ is injective.

Let V be any $\mathbb{F}_q$-linear space. A sequence $(V_1, \ldots, V_n) \in \mathcal{L}(V)^n$ is called a V-local profile, or simply local profile when V is clear from context.

We say that C contains a V-local profile $(V_1, \ldots, V_n)$ if there exists a subspace $A \subseteq \mathbb{F}_q^k$ and an isomorphism $\varphi : V \to A^*$ such that, for each $i \in [n]$, we have $\varphi(V_i)^\circ \subseteq \ker(\mathsf{Enc}_i)$; that is, any vector $a \in A$ with $\varphi(V_i)(a) = 0$ satisfies $\mathsf{Enc}_i(a) = 0$.

Before proceeding, we first provide some intuition for Definition 3.3 and its connection to subspace design codes and the potential function Φ (Definition 3.1). In Definition 3.3, $A \subseteq \mathbb{F}_q^k$ is in the message space. For each $i \in [n]$, $\varphi(V_i)$ is a subspace of A^*, so the kernel $\varphi(V_i)^\circ$ is a subspace of A. By the rank-nullity theorem, we have

$$\dim(\varphi(V_i)^\circ) = \dim(A) - \dim(\varphi(V_i)) = \dim(V) - \dim(V_i)\,.$$

Here, we use that φ is an isomorphism from V to A^*.

Since $\varphi(V_i)^\circ \subseteq A$, the inclusion $\varphi(V_i)^\circ \subseteq \ker(\mathsf{Enc}_i)$ implies $\dim(\varphi(V_i)^\circ) \leqslant \dim(A \cap \ker(\mathsf{Enc}_i))$. Suppose $\widetilde{A} = \mathsf{Enc}(A) \subseteq C$ and $\widetilde{A}_i = \{x \in \widetilde{A} \mid x_i = 0\}$ (tying back to the definition of subspace design codes in Definition 2.3), then $\widetilde{A}_i = \mathsf{Enc}(A \cap \ker(\mathsf{Enc}_i))$, and

$$\frac{1}{n}\sum_{i=1}^{n} \dim(\widetilde{A}_i) = \frac{1}{n}\sum_{i=1}^{n} \dim(A \cap \ker(\mathsf{Enc}_i)) \geqslant \frac{1}{n}\sum_{i=1}^{n} \dim(\varphi(V_i)^\circ) = \frac{1}{n}\sum_{i=1}^{n} (\dim(V) - \dim(V_i))\,.$$

The right-hand-side appears in the potential function $\Phi_V(V, (V_1, \ldots, V_n), \alpha)$. In Section 3.2, we will crucially rely on this connection to show a characterization of subspace design codes.

A key advantage of this definition of local profile is its versatility. In the following, we show that the property of containing a local profile is preserved under taking quotients.

Lemma 3.4. *Let V be a linear space and $(V_1, \ldots, V_n)$ be a V-local profile, and let $W \subseteq V$. If a code $C = \{(\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x)) \mid x \in \mathbb{F}_q^k\}$ contains $(V_1, \ldots, V_n)$, then it also contains $((V_1 + W)/W, \ldots, (V_n + W)/W) \in \mathcal{L}(V/W)^n$.*

Proof. By Definition 3.3, if C contains $(V_1, \ldots, V_n)$, then there exists a subspace $A \subseteq \mathbb{F}_q^k$ and an isomorphism $\varphi : V \to A^*$ such that $\varphi(V_i)^\circ \subseteq \ker(\mathsf{Enc}_i)$.

$\varphi(W)$ is a subspace in A^*, and let $A' = \varphi(W)^\circ$ be its kernel, which is a subspace in A of dimension $\dim(V) - \dim(W) = \dim(V/W)$. Define a linear map $M : A^* \to A'^*$ given by the restriction $M(f) \coloneqq f|_{A'}$, where M takes a functional on A and restricts it to A'. The kernel of M is the set of functionals $f \in A^*$ such that $f(a) = 0$ for all $a \in A'$, i.e., $\ker(M) = (A')^\perp$, the annihilator of A', which means that $\ker(M) = (\varphi(W)^\circ)^\perp = \varphi(W)$ (see Definition 2.2). Then, since φ is an isomorphism, $\ker(M \circ \varphi) = \varphi^{-1}(\ker(M)) = W$.

The map $M \circ \varphi : V \to A'^*$ is surjective. By the isomorphism theorem, $A'^* \cong V/\ker(M \circ \varphi) = V/W$, and there is an isomorphism $\varphi' : V/W \to A'^*$ that maps a coset $v + W$ to $M(\varphi(v))$.

Now, it suffices to prove that $\varphi'((V_i + W)/W)^\circ \subseteq \ker(\mathsf{Enc}_i)$. By definition, $\varphi'((V_i + W)/W) = M(\varphi(V_i))$. Since M only restricts to evaluating on A' without changing their values, for any

$a \in A'$ we have $M(\varphi(v))(a) = \varphi(v)(a)$. Thus, any $a \in A'$ with $M(\varphi(V_i))(a) = 0$ also implies $\varphi(V_i)(a) = 0$, and by the assumption $\varphi(V_i)^\circ \subseteq \ker(\mathsf{Enc}_i)$, we have $a \in \ker(\mathsf{Enc}_i)$ as desired. □

3.2 Equivalence statements for subspace design codes

With the definitions of local profiles and potential function in hand, we next show an equivalence statement for subspace design codes.

Theorem 3.5. *An additive code $C = \{(\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x)) \mid x \in \mathbb{F}_q^k\} \subseteq \left(\mathbb{F}_q^s\right)^n$ is a τ-subspace design code if and only if for any $r \in \mathbb{N}$, vector space V of dimension at most r, and every V-local profile $(V_1, \ldots, V_n)$ that C contains, we have*

$$\Phi_V(V, (V_1, \ldots, V_n), \tau(r)) \geqslant 0\,.$$

Proof. We first show that if the conclusion does not hold, then C is not a τ-subspace design code. In particular, there exists a positive integer r, a vector space V of dimension $\leqslant r$, and a V-local profile $(V_1, \ldots, V_n)$ that C contains, such that $\Phi_V(V, (V_1, \ldots, V_n), \tau(r)) < 0$.

Recall from Definition 3.3 that C containing $(V_1, \ldots, V_n)$ means that there exists a subspace $A \subseteq \mathbb{F}_q^k$, and an isomorphism $\varphi : V \to A^*$, such that $\varphi(V_i)^\circ \subseteq \ker(\mathsf{Enc}_i)$. In fact, since $\varphi(V_i)^\circ$ is a subspace in A, we have $\varphi(V_i)^\circ \subseteq \ker(\mathsf{Enc}_i) \cap A$. By the rank-nullity theorem, we have $\dim(\varphi(V_i)^\circ) = \dim(A^*) - \dim(\varphi(V_i)) = \dim(V) - \dim(V_i)$. Thus,

$$\begin{aligned}\frac{1}{n}\sum_{i=1}^{n} \dim(\ker(\mathsf{Enc}_i) \cap A) &\geqslant \frac{1}{n}\sum_{i=1}^{n} \dim(\varphi(V_i)^\circ) = \frac{1}{n}\sum_{i=1}^{n}(\dim(V) - \dim(V_i)) \\ &> \tau(r) \cdot \dim(V)\,,\end{aligned}$$

where the last inequality follows from $\Phi_V(V, (V_1, \ldots, V_n), \tau(r)) < 0$.

Now, consider the subspace $\widetilde{A} = \mathsf{Enc}(A) \subseteq C$ of dimension $\dim(\widetilde{A}) = \dim(V) \leqslant r$, and let $\widetilde{A}_i = \{a \in \widetilde{A} \mid a_i = 0\}$ for $i \in [n]$. We have that $\dim(\widetilde{A}_i) = \dim(\ker(\mathsf{Enc}_i) \cap A)$, and $\frac{1}{n}\sum_{i=1}^{n} \dim(\widetilde{A}_i) > \tau(r) \cdot \dim(\widetilde{A})$, which shows that C is not a τ-subspace design code.

For the other direction, if C is not a τ-subspace design code, then there exists a subspace $A \subseteq \mathbb{F}_q^k$ (in the message space) of dimension at most r such that $\frac{1}{n}\sum_{i=1}^{n} \dim(A \cap \ker(\mathsf{Enc}_i)) > \tau(r)\dim(A)$.

Let $V = A^*$, and for $i \in [n]$, let $V_i = (A \cap \ker(\mathsf{Enc}_i))^\perp$ (the annihilator of $A \cap \ker(\mathsf{Enc}_i)$). By definition, we have $V_i^\circ \subseteq \ker(\mathsf{Enc}_i)$. Moreover, since $\dim(V_i) = \dim(V) - \dim(A \cap \ker(\mathsf{Enc}_i))$,

$$\begin{aligned}\Phi_V(V, (V_1, \ldots, V_n), \tau(r)) &= \tau(r)\dim(V) - \frac{1}{n}\sum_{i=1}^{n}(\dim(V) - \dim(V_i)) \\ &= \tau(r)\dim(A) - \frac{1}{n}\sum_{i=1}^{n}\dim(A \cap \ker(\mathsf{Enc}_i)) < 0\,.\end{aligned}$$

Therefore, $(V_1, \ldots, V_n)$ is a V-local profile contained in C with $\Phi_V(V, (V_1, \ldots, V_n), \tau(r)) < 0$. □

By the "if" direction of Theorem 3.5, we know that if C is *not* a τ-subspace design code, then C contains a local profile $(V_1, \ldots, V_n)$ with $\Phi(V, (V_1, \ldots, V_n), \tau(r)) < 0$. Using the fact

that containment of a local profile is preserved under taking quotients (Lemma 3.4), we can show a stronger statement: if C is *not* a τ-subspace design code, then C contains a local profile $(V_1, \ldots, V_n)$ with $\Phi(U, (V_1, \ldots, V_n), \tau(r)) < 0$ for *all* subspaces $\{0\} \neq U \subseteq V$. This makes it easier to obtain a contradiction in our analysis in Section 4.

Lemma 3.6. *Suppose an additive code $C = \{(\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x)) \mid x \in \mathbb{F}_q^k\} \subseteq \left(\mathbb{F}_q^s\right)^n$ is **not** a τ-subspace design. Then there exists a positive integer r, a linear space V' of dimension at most r, along with a V'-local profile $(V_1', \ldots, V_n') \subseteq \mathcal{L}(V')^n$ contained in C, such that for all $\{0\} \neq U \subseteq V'$, we have $\Phi_{V'}(U, (V_1', \ldots, V_n'), \tau(r)) < 0$.*

Proof. By Theorem 3.5, if the code C is not a subspace design, then there exists a positive integer r, a vector space V of dimension at most r and a V-local profile $(V_1, \ldots, V_n)$ contained in C such that

$$\Phi_V(V, (V_1, \ldots, V_n), \tau(r)) < 0\,.$$

Let $W \subseteq V$ be an element of $\arg\max \Phi_V(*, (V_1, \ldots, V_n), \tau(r))$ of maximal dimension. Note that $W \neq V$ since $\Phi_V(V, (V_1, \ldots, V_n), \tau(r)) < 0$, but we know that the maximum value must be non-negative since $\Phi_V(\{0\}, (V_1, \ldots, V_n), \tau(r)) = 0$.

Now, by Lemma 3.4, C also contains the V/W-local profile $((V_1 + W)/W, \ldots, (V_n + W)/W)$. Let $V' \coloneqq V/W$ and $V_i' \coloneqq (V_i + W)/W$ for each $i \in [n]$. Let $M : V \to V/W$ be the linear map that maps v to the coset $v + W$. Then, we have $\ker(M) = W$ and $M(V_i) = V_i'$.

For any non-trivial subspace $U \subseteq V$ such that $U \not\subseteq W$, let $U' = M(U) = (U + W)/W \neq \{0\}$. Invoking Lemma 3.2 with U, $W = \ker(M)$, $V_1', \ldots, V_n'$, and M, we get

$$\begin{aligned}&\Phi_{V'}\left(U', \left(V_i', \ldots, V_n'\right), \tau(r)\right)\\ &\quad = \Phi_V(U + W, (V_1, \ldots, V_n), \tau(r)) - \Phi_V(W, (V_1, \ldots, V_n), \tau(r)) < 0\,,\end{aligned}$$

where the strict inequality follows since $\dim(U + W) > \dim(W)$ and W is a maximal element of $\arg\max \Phi_V(*, (V_1, \ldots, V_n), \tau(r))$. The above inequality holds for all $\{0\} \neq U' \subseteq V'$, which completes the proof. □

In the following, we give another characterization of subspace design codes. Here, we have a code with message space $\mathbb{F}_q^k$, and we consider an auxiliary space $\mathbb{F}_q^{k'}$ together with a linear map $M : \mathbb{F}_q^{k'} \to \mathbb{F}_q^k$. We are interested in $M(A)$ for subspaces $A \subseteq \mathbb{F}_q^{k'}$. Looking ahead, in the AEL construction, this lemma will be applied to the inner code C_{in} with M being the encoding map of the outer code restricted to a coordinate (where $k' = k_{\text{out}}$ and $k = k_{\text{in}}$).

Lemma 3.7. *Let $C = \{(\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x)) \mid x \in \mathbb{F}_q^k\} \subseteq \left(\mathbb{F}_q^s\right)^n$ be an $\mathbb{F}_q$-additive code which is a τ-subspace design code. Let V be a vector space and $(V_1, \ldots, V_n)$ be a V-local profile. Let $A \subseteq \mathbb{F}_q^{k'}$ be a subspace, $M : \mathbb{F}_q^{k'} \to \mathbb{F}_q^k$ be a linear map, and $\varphi : V \to A^*$ be an isomorphism satisfying $\varphi(V_i)^\circ \subseteq \ker(\mathsf{Enc}_i \circ M)$ for each $i \in [n]$. Then, either $M(A) = \{0\}$, or for any positive integer $r \geqslant \dim(V)$, there exists a subspace $\{0\} \neq U \subseteq V$ such that*

$$\Phi_V(U, (V_1, \ldots, V_n), \tau(r)) \geqslant 0\,.$$

Proof. Let $B = M(A) \subseteq \mathbb{F}_q^k$, and assume that $B \neq \{0\}$. We will consider the restriction of M to A, which we denote as $M_A : A \to B$. Note that we have $\dim(A) = \dim(B) + \dim(\ker(M_A))$,

thus the annihilator $\ker(M_A)^\perp \subseteq A^*$ has $\dim(\ker(M_A)^\perp) = \dim(A) - \dim(\ker(M_A)) = \dim(B)$, which is nonzero.

Let $U \coloneqq \varphi^{-1}(\ker(M_A)^\perp) \subseteq V$. We claim that in fact C contains the U-local profile $(V_1 \cap U, \ldots, V_n \cap U)$. Assuming this, the lemma follows by invoking Theorem 3.5: since U is a vector space of dimension $0 < \dim(U) \leqslant \dim(A) \leqslant r$, and C contains $(V_1 \cap U, \ldots, V_n \cap U)$, Theorem 3.5 states that

$$\Phi_V(U, (V_1 \cap U, \ldots, V_n \cap U), \tau(r)) = \Phi_V(U, (V_1, \ldots, V_n), \tau(r)) \geqslant 0\,.$$

To prove the claim, we first need to define an isomorphism $\varphi' : U \to B^*$. For $u \in U$, we define $\varphi'(u) \in B^*$ as follows: for any $b \in B$,

$$\varphi'(u)(b) = \varphi(u)(a)$$

where $a \in A$ is any element satisfying $M_A a = b$. This is well-defined because if $a \neq a'$ have $M_A a = M_A a' = b$, then $a - a' \in \ker(M_A)$ and $\varphi(u)(a - a') = 0$ due to $\varphi(u) \in \ker(M_A)^\perp$. The fact that φ' is an isomorphism is straightforward given that $\dim(U) = \dim(B) = \dim(B^*)$ and that $\varphi'(u) = 0 \implies \varphi(u) = 0 \implies u = 0$.

Therefore, we have a vector space U, a subspace $B \subseteq \mathbb{F}_q^k$, and an isomorphism $\varphi' : U \to B^*$. To show that C contains the U-local profile $(V_1 \cap U, \ldots, V_n \cap U)$, it suffices to show that $\varphi'(V_i \cap U)^\circ \subseteq \ker(\mathsf{Enc}_i)$, that is, any $b \in B$ with $\varphi'(V_i \cap U)(b) = 0$ satisfies $\mathsf{Enc}_i(b) = 0$.

For such b, by definition of φ', we have $\varphi(V_i \cap U)(a) = 0$ for all $a \in A$ such that $M_A a = b$. Denoting $M_A^{-1} b \coloneqq \{a \in A \mid M_A a = b\}$, we have

$$M_A^{-1} b \subseteq \varphi(V_i \cap U)^\circ = \varphi(V_i)^\circ + \varphi(U)^\circ = \varphi(V_i)^\circ + \ker(M_A) \subseteq \ker(\mathsf{Enc}_i \circ M) + \ker(M_A)\,,$$

where we use that $\varphi(U)^\circ = (\ker(M_A)^\perp)^\circ = \ker(M_A)$, and the assumption $\varphi(V_i)^\circ \subseteq \ker(\mathsf{Enc}_i \circ M)$. Therefore, we have $b \in M_A(\ker(\mathsf{Enc}_i \circ M) + \ker(M_A)) \subseteq \ker(\mathsf{Enc}_i)$, which implies that $\mathsf{Enc}_i(b) = 0$ as desired. □

4 Our construction

We first state a simple lemma about bipartite spectral expanders.

Lemma 4.1. *Let $G = ([n], [n], E)$ be a d-regular bipartite λ-expander. For any $x \in \mathbb{R}^n$, let $\mu = \frac{1}{n}\sum_{i=1}^n x_i$, and let $y \in \mathbb{R}^n$ be such that $y_j = \frac{1}{d}\sum_{i \in N(j)} x_i$ for each $j \in [n]$. Then,*

$$\frac{1}{n}\sum_{j=1}^n (y_j - \mu)^2 \leqslant \lambda^2 \cdot \|x\|_\infty^2\,.$$

Proof. We can write y as Ax, where $A \in \mathbb{R}^{n \times n}$ is the normalized adjacency matrix of G with $A_{i,j} = 1/d$ if $(i, j) \in E(G)$ and 0 otherwise. Then,

$$\frac{1}{n}\sum_{j=1}^n (y_j - \mu)^2 = \frac{1}{n}\|Ax - \mu \cdot \mathbf{1}\|_2^2 = \frac{1}{n}\|A(x - \mu \cdot \mathbf{1})\|_2^2\,.$$

Observe that $x - \mu \cdot \mathbf{1}$ is orthogonal to $\mathbf{1}$. Since G is a λ-expander, we have $\|Av\|_2^2 \leqslant \lambda^2 \|v\|_2^2$ for any vector $v \perp \mathbf{1}$. Thus, $\frac{1}{n}\|A(x - \mu \cdot \mathbf{1})\|_2^2 \leqslant \frac{1}{n}\lambda^2 \|x - \mu \cdot \mathbf{1}\|_2^2 \leqslant \lambda^2 \|x\|_\infty^2$, where we use that $\frac{1}{n}\|x - \mu\mathbf{1}\|_2^2 = \frac{1}{n}\|x\|_2^2 - \mu^2 \leqslant \|x\|_\infty^2$. □

Our main theorem. We show that the AEL construction (Definition 1.3) inherits the subspace design property of the inner codes, as long as the outer code has constant distance and the graph is a sufficiently good expander.

Theorem 4.2. *Let $\tau : \mathbb{N} \to \mathbb{R}_{\leqslant 1}$, $\varepsilon > 0$, and $r \in \mathbb{N}$. Suppose*

- *C_{out} is a code with $\mathsf{Enc}_{\text{out}} : \mathbb{F}_q^k \to (\mathbb{F}_q^{k_{\text{in}}})^n$ and has relative distance $\delta_{\text{out}} > 0$,*
- *C_{in} is a code with $\mathsf{Enc}_{\text{in}} : \mathbb{F}_q^{k_{\text{in}}} \to (\mathbb{F}_q^s)^d$ and is a τ-subspace design code,*
- *$G = (V_{\text{left}}, V_{\text{right}}, E)$ is a d-regular bipartite λ-expander with $|V_{\text{left}}| = |V_{\text{right}}| = n$ and suppose $\lambda < \varepsilon q^{-r^2/2}\sqrt{\delta_{\text{out}}}$.*

Then, $C = C_{\text{AEL}}(C_{\text{out}}, C_{\text{in}}, G) \subseteq ((\mathbb{F}_q^s)^d)^n$ a $\widetilde{\tau}$-subspace design code where $\widetilde{\tau}(r') = \tau(r') + \varepsilon$ for all $r' \leqslant r$, and $\widetilde{\tau}(r') = 1$ otherwise.

Proof. We first set a few notations. The vertices $i \in V_{\text{right}}$ and $j \in V_{\text{left}}$ are naturally associated with the set $[n]$. We write $\mathsf{Enc}_{\text{out},j} : \mathbb{F}_q^k \to \mathbb{F}_q^{k_{\text{in}}}$ to denote the outer encoder restricted to a coordinate $j \in V_{\text{left}}$. Similarly, $\mathsf{Enc}_{\text{in},\ell} : \mathbb{F}_q^{k_{\text{in}}} \to \mathbb{F}_q^s$ for the inner code restricted to $\ell \in [d]$, and $\mathsf{Enc}_{\text{AEL},i} : \mathbb{F}_q^k \to (\mathbb{F}_q^s)^d$ for the final encoder restricted to $i \in V_{\text{right}}$.

For contradiction, suppose C is *not* a $\widetilde{\tau}$-subspace design code. For simplicity, we denote $\tau' = \widetilde{\tau}(r) = \tau(r) + \varepsilon$. By Lemma 3.6, there exist a linear space V of dimension at most r and subspaces $V_1, \ldots, V_n \subseteq V$, such that C contains the V-local profile $(V_1, \ldots, V_n)$, and

$$\Phi_V(U, (V_1, \ldots, V_n), \tau') = \frac{1}{n}\sum_{i=1}^{n} \dim(U \cap V_i) - (1 - \tau')\dim(U) < 0\,, \tag{2}$$

for all subspaces $\{0\} \neq U \subseteq V$.

Recall that C containing $(V_1, \ldots, V_n)$ means that there is a subspace $A \subseteq \mathbb{F}_q^k$ (in the message space) and an isomorphism $\varphi : V \to A^*$ (where A^* is the dual space of A) such that $\varphi(V_i)^\circ \subseteq \ker(\mathsf{Enc}_{\text{AEL},i})$ for all $i \in [n]$. In other words, any vector $a \in A$ with $\varphi(V_i)(a) = 0$ satisfies $\mathsf{Enc}_{\text{AEL},i}(a) = 0$.

Recall that a codeword can be viewed as a regrouping of $\mathsf{Enc}_{\text{in}}(\mathsf{Enc}_{\text{out},j}(a)) \in (\mathbb{F}_q^s)^d$ for $j \in V_{\text{left}}$. For a vertex $j \in V_{\text{left}}$ and its d neighbors $N_1(j), \ldots, N_d(j) \in V_{\text{right}}$, we have that $\mathsf{Enc}_{\text{AEL},N_\ell(j)}(a) = 0$ implies that $\mathsf{Enc}_{\text{in},\ell}(\mathsf{Enc}_{\text{out},j}(a)) = 0$. Therefore, $\varphi(V_{N_\ell(j)})^\circ \subseteq \ker(\mathsf{Enc}_{\text{in},\ell} \circ \mathsf{Enc}_{\text{out},j})$ for each neighbor indexed by $\ell \in [d]$.

Next, we use the τ-subspace design property of C_{in}. Invoking Lemma 3.7 with $k' = k_{\text{out}}$, $k = k_{\text{in}}$, the linear map $M = \mathsf{Enc}_{\text{out},j} : \mathbb{F}_q^{k_{\text{out}}} \to \mathbb{F}_q^{k_{\text{in}}}$, and local profile $(V_{N_1(j)}, \ldots, V_{N_d(j)})$, it follows that either

(1) $\mathsf{Enc}_{\text{out},j}(A) = 0$, or

(2) for $r = \dim(V)$, there exists a non-trivial subspace $U \subseteq V$ such that

$$\Phi\left(U, (V_{N_1(j)}, \ldots, V_{N_d(j)}), \tau(r)\right) \geqslant 0\,.$$

The rest of the proof goes by showing that more than $1-\delta_{\text{out}}$ fraction of $j \in V_{\text{left}}$ has $\mathsf{Enc}_{\text{out},j}(A) = 0$, hence contradicting the distance δ_{out} of the outer code C_{out}. To do so, we will show that $\frac{1}{d}\sum_{\ell=1}^{d} \dim(U \cap V_{N_\ell(j)})$ is close to $\frac{1}{n}\sum_{i=1}^{n} \dim(U \cap V_i)$ for most j and most subspaces U.

Fix a non-trivial subspace $U \subseteq V$. Define vectors $x, y \in \mathbb{R}^n$ to be such that $x_i \coloneqq \dim(U \cap V_i)$ and $y_j \coloneqq \frac{1}{d}\sum_{\ell=1}^{d} \dim(U \cap V_{N_\ell(j)}) = \frac{1}{d}\sum_{\ell=1}^{d} x_{N_\ell(j)}$. Moreover, let $\mu \coloneqq \frac{1}{n}\sum_{i=1}^{n} x_i$, and note that $x_i \leqslant \dim(U)$. Then, by Lemma 4.1, we have

$$\frac{1}{n}\sum_{j=1}^{n}(y_j - \mu)^2 \leqslant \lambda^2 \cdot \dim(U)^2\,.$$

By Markov's inequality, we have that

$$\Pr_{j\sim[n]}\left[|y_j - \mu| \geqslant \varepsilon \cdot \dim(U)\right] \leqslant \frac{\lambda^2}{\varepsilon^2}\,.$$

On the other hand, we know from Equation (2) that $\mu < (1-\tau')\dim(U)$. Thus, if $|y_j - \mu| \leqslant \varepsilon \cdot \dim(U)$, then $y_j < (1 - \tau' + \varepsilon)\dim(U)$. Since $\tau' = \tau(r) + \varepsilon$, we have

$$\Phi\left(U, (V_{N_1(j)}, \ldots, V_{N_d(j)}), \tau(r)\right) = y_j - (1-\tau(r))\dim(U) < 0\,.$$

Taking a union bound over $\leqslant q^{r^2}$ many non-trivial subspaces $U \subseteq V$, we have that $1 - \frac{\lambda^2}{\varepsilon^2}q^{r^2}$ fraction of $j \in V_{\text{left}}$ satisfies $\Phi(U, (V_{N_1(j)}, \ldots, V_{N_d(j)}), \tau(r)) < 0$ for all non-trivial subspaces $U \subseteq V$. For such $j \in V_{\text{left}}$, we must have $\mathsf{Enc}_{\text{out},j}(A) = 0$.

Suppose $\lambda < \varepsilon q^{-r^2/2}\sqrt{\delta_{\text{out}}}$, then $> 1 - \delta_{\text{out}}$ fraction of $j \in V_{\text{left}}$ has $\mathsf{Enc}_{\text{out},j}(A) = 0$, which contradicts that C_{out} has distance δ_{out}. This completes the proof. □

From Theorem 4.2, Theorem 1.1 follows almost immediately.

Proof of Theorem 1.1. Given $r \in \mathbb{N}$ and $R, \varepsilon \in (0,1)$, we instantiate the ingredients in Theorem 4.2 as follows:

- Outer code C_{out}: We choose an explicit additive code with rate $R_{\text{out}} = 1 - \varepsilon/4$ and relative distance $\delta_{\text{out}} = \varepsilon/8$.
- Inner code C_{in}: We set $s = \Theta(r/\varepsilon)$. By Theorem 2.6, there exists a τ_{in}-subspace design code in $(\mathbb{F}_q^s)^d$ of rate R_{in} with $\tau_{\text{in}}(r') \leqslant R_{\text{in}} + \varepsilon/4$ for all $r' \leqslant \varepsilon s/16 \leqslant r$. Since s, d are constants, we can find such a code by brute force.
- Graph G: We use the explicit construction from Theorem 2.12, where $\lambda \leqslant 2/\sqrt{d}$ (as long as $n \geqslant n_0(d)$ is sufficiently large). We choose $d = \frac{\Theta(1)}{\varepsilon^2\delta_{\text{out}}}q^{r^2} = \text{poly}(1/\varepsilon)\cdot q^{r^2}$.

By choosing R_{in} to be $R + \varepsilon/2$, we get that the rate of C_{AEL} is $R_{\text{out}}R_{\text{in}} \geqslant R$. The alphabet is $\mathbb{F}_q^{sd} = \mathbb{F}_q^{\text{poly}(r,1/\varepsilon)q^{r^2}}$. By Theorem 4.2 (with τ_{in} and $\varepsilon/4$), our code is a τ-subspace design code

with $\tau(r') = \tau_{\text{in}}(r') + \varepsilon/4 \leqslant R_{\text{in}} + \varepsilon/2 \leqslant R + \varepsilon$ for all $r' \leqslant r$. This completes the proof of Theorem 4.2. □

5 Consequences for list-decoding, recovery and curve-decoding

In this section, we state the list-decoding, list-recovery, and curve-decoding parameters of our construction.

Definition 5.1. Let $C_{q,R,r,\varepsilon,n}$ be our explicit $\mathbb{F}_q$-additive code of rate R over alphabet $\Sigma = \mathbb{F}_q^{\text{poly}(r,1/\varepsilon)\cdot q^{r^2}}$ which is a τ-subspace design with $\tau(r') \leqslant R + \varepsilon$ for all $r' \leqslant r$.

We note that our constructions exist for each choice of parameters by Theorem 1.1. Our construction has not been explicitly defined for any of the below properties, but it naturally captures them due to the strength of subspace designs.

Theorem 5.2 (Average radius list-decoding)**.** *For any finite field $\mathbb{F}_q$, $R, \varepsilon \in (0,1)$ and positive integer L, the $\mathbb{F}_q$-additive code $C_{q,R,L,\varepsilon,n} \subseteq \Sigma^n$, of rate R and alphabet $\Sigma = \mathbb{F}_q^{\text{poly}(L/\varepsilon)\cdot q^{L^2}}$, has the property that for any distinct $c_0, \ldots, c_L \in C_{q,R,L,\varepsilon,n}$ and $y \in \Sigma^n$, we have*

$$\sum_{i=0}^{L} \Delta(y, c_i) \geqslant L(1 - R - \varepsilon) \ .$$

Proof. $C_{q,R,L,\varepsilon,n} \subseteq \Sigma^n$ is a τ-subspace design code with $\tau(L) \leqslant R + \varepsilon$. Now, we can apply Theorem 2.7. □

Theorem 5.3 (List-recovery)**.** *For any finite field $\mathbb{F}_q$, $R, \varepsilon_0, \varepsilon_1 \in (0,1)$ and positive integer ℓ, the $\mathbb{F}_q$-additive code $C_{q,R,\lceil \ell/\varepsilon_1 \rceil,\varepsilon_0,n} \subseteq \Sigma^n$, of rate R and alphabet $\Sigma = \mathbb{F}_q^{\text{poly}(\ell,1/\varepsilon_1,1/\varepsilon_0)\cdot q^{\lceil \ell/\varepsilon_1 \rceil^2}}$, has the following list-recovery property: for any $L_1, \ldots, L_n \subseteq \Sigma$ with $|L_i| = \ell$ for each $i \in [n]$,*

$$|\{c \in C \mid \Delta(c_i, L_1 \times L_2 \times \cdots \times L_n) < 1 - R - \varepsilon_0 - \varepsilon_1\}| \leqslant \left(\frac{\ell}{R + \varepsilon_0 + \varepsilon_1}\right)^{(R+\varepsilon_0+\varepsilon_1)/\varepsilon_1} \ .$$

Proof. $C_{q,R,\lceil \ell/\varepsilon_1 \rceil,\varepsilon_0,n} \subseteq \Sigma^n$ is a τ-subspace design code with $\tau(\lceil \ell/\varepsilon_1 \rceil) \leqslant R + \varepsilon_0$. Now, we can apply Theorem 2.8. Note that this is possible since the code C we construct is thus also a τ'subspace design with $\tau'(r) = \max(R + \varepsilon_0, \tau(r))$ for all r. □

Corollary 5.4. *For any finite field $\mathbb{F}_q$, $R, \varepsilon \in (0,1)$ and positive integer $\ell \geqslant 2$, there exists a choice of ε_0 and $\varepsilon_1 \in (0,1)$ with $\varepsilon_0 + \varepsilon_1 = \varepsilon$, such that the $\mathbb{F}_q$-additive code $C_{q,R,\lceil \ell/\varepsilon_1 \rceil,\varepsilon_0,n} \subseteq \Sigma^n$ of rate R and alphabet $\Sigma = \mathbb{F}_q^{\text{poly}(\ell,1/\varepsilon)\cdot q^{4\ell^2/\varepsilon^2}}$ has the following list-recovery property: for any $L_1, \ldots, L_n \subseteq \Sigma$ with $|L_i| = \ell$ for each $i \in [n]$,*

$$|\{c \in C \mid \Delta(c_i, L_1 \times L_2 \times \cdots \times L_n) < 1 - R - \varepsilon\}| \leqslant \left\lceil \left(\frac{\ell}{R + \varepsilon}\right)^{(R+\varepsilon)/\varepsilon} \right\rceil \ .$$

Proof. Let $L = \left\lceil \left(\frac{\ell}{R+\varepsilon}\right)^{(R+\varepsilon)/\varepsilon} \right\rceil$. Consider $\varepsilon_0 = \frac{\varepsilon^2}{4L\log(\ell/\varepsilon)}$ and $\varepsilon_1 = \varepsilon - \varepsilon_0$.

Thus, $C_{q,R,\lceil \ell/\varepsilon_1 \rceil, \varepsilon_0, n} \subseteq \Sigma^n$, is an $\mathbb{F}_q$-additive code of rate R, alphabet $\Sigma = \mathbb{F}_q^{\mathrm{poly}(\ell, 1/\varepsilon_1, 1/\varepsilon_0)\cdot q^{\lceil \ell/\varepsilon \rceil^2}} = \mathbb{F}_q^{\mathrm{poly}(\ell,1/\varepsilon)\cdot \mathrm{poly}(1/\varepsilon_0)\cdot q^{\lceil \ell/\varepsilon \rceil^2}}$ and

$$|\{c \in C \mid \Delta(c_i, L_1 \times L_2 \times \cdots \times L_n) < 1 - R - \varepsilon\}| \leqslant \left\lfloor \left(\frac{\ell}{R+\varepsilon}\right)^{(R+\varepsilon)/\varepsilon_1} \right\rfloor.$$

Therefore, it suffices to prove that:

- $\mathrm{poly}(1/\varepsilon_0) \cdot q^{\lceil \ell/\varepsilon \rceil^2} \leqslant \mathrm{poly}(\ell/\varepsilon) \cdot q^{4\ell^2/\varepsilon^2}$; and
- $\left(\frac{\ell}{R+\varepsilon}\right)^{(R+\varepsilon)/\varepsilon_1} \leqslant \left(\frac{\ell}{R+\varepsilon}\right)^{(R+\varepsilon)/\varepsilon} + 1/2$.

For the first, observe that it suffices to prove that $\log L + \lceil \ell/\varepsilon \rceil^2 \leqslant 4\ell^2/\varepsilon^2$ but $\log L = \frac{R+\varepsilon}{\varepsilon} \cdot \log_q(\ell/(R+\varepsilon)) \leqslant \ell/\varepsilon \cdot \ell/\varepsilon \leqslant \ell^2\varepsilon^2$ and thus, this part follows.

Now, for the second part we have that:

$$\begin{aligned}
\left(\frac{\ell}{R+\varepsilon}\right)^{(R+\varepsilon)/\varepsilon_1} &= \left(\frac{\ell}{R+\varepsilon}\right)^{(R+\varepsilon)(1/\varepsilon+1/\varepsilon_1-1/\varepsilon)} \\
&= \left(\frac{\ell}{R+\varepsilon}\right)^{(R+\varepsilon)/\varepsilon} \cdot \left(\frac{\ell}{R+\varepsilon}\right)^{(R+\varepsilon)(\varepsilon_0/\varepsilon\cdot\varepsilon_1)} \qquad (\varepsilon_1 \geqslant \varepsilon/2) \\
&\leqslant \left(\frac{\ell}{R+\varepsilon}\right)^{(R+\varepsilon)/\varepsilon} \cdot (\ell/\varepsilon)^{1/2L\log(\ell/\varepsilon)} \\
&\leqslant \left(\frac{\ell}{R+\varepsilon}\right)^{(R+\varepsilon)/\varepsilon} \cdot 2^{1/2L} \\
&\leqslant \left(\frac{\ell}{R+\varepsilon}\right)^{(R+\varepsilon)/\varepsilon} (1 + 1/2L) \\
&\leqslant \left(\frac{\ell}{R+\varepsilon}\right)^{(R+\varepsilon)/\varepsilon} + 1/2
\end{aligned}$$

as desired. □

Theorem 5.5 (Curve-decoding)**.** *For any finite field $\mathbb{F}_q$, $R, \varepsilon_0, \varepsilon_1 \in (0,1)$ and positive integers $\ell \geqslant 2, a$, the $\mathbb{F}_q$-additive code $C_{q,R,\lceil(\ell+1)/\varepsilon_1\rceil,\varepsilon_0,n} \subseteq \Sigma^n$ of rate R, and alphabet $\Sigma = \mathbb{F}_q^{\mathrm{poly}(\ell,1/\varepsilon_0,1/\varepsilon_1)\cdot q^{\lceil(\ell+1)/\varepsilon_1\rceil^2}}$, is $(\ell, 1-R-\varepsilon_0-\varepsilon_1, a, a\cdot\frac{\varepsilon_1}{\lceil(\ell+1)/\varepsilon_1\rceil+\varepsilon_1})$ curve-decodable.*

Proof. $C_{q,R,\lceil(\ell+1)/\varepsilon_1\rceil,\varepsilon_0,n} \subseteq \Sigma^n$ is a τ-subspace design code with $\tau(\lceil(\ell+1)/\varepsilon_1\rceil) \leqslant R + \varepsilon_0$. Now, we can apply Theorem 2.10. □

By setting $\varepsilon_0 = \varepsilon_1 = \varepsilon/2$ in Theorem 5.5, we get the following corollary.

Corollary 5.6. *For any finite field $\mathbb{F}_q$, $R, \varepsilon \in (0,1)$ and positive integers $\ell \geqslant 2, a$, the $\mathbb{F}_q$-additive code $C_{q,R,2\lceil(\ell+1)/\varepsilon\rceil,\varepsilon/2,n} \subseteq \Sigma^n$ of rate R, and alphabet $\Sigma = \mathbb{F}_q^{\mathrm{poly}(\ell,1/\varepsilon)\cdot q^{4\lceil(\ell+1)/\varepsilon\rceil^2}}$, is $(\ell, 1-R-\varepsilon, a, \Omega(a\cdot\varepsilon^2/\ell))$ curve-decodable.*

6 Acknowledgments

Part of this done was done while R.G. was visiting V.G. at the Simons Institute for the Theory of Computing. We thank Josh Brakensiek, Yeyuan Chen and Zihan Zhang for various discussions related to the recent progress on local properties of RLCs, and Zihan in particular for a chat about AEL and subspace designs. We also thank Nikhil Shagrithaya for comments on the paper and discussions about [JS25].

V.G. is supported by a Simons Investigator award, NSF grant CCF-2211972, and ONR grant N00014-24-1-2491.

R.G. is supported by (Yael Tauman Kalai's) grant from Defense Advanced Research Projects Agency (DARPA) under Contract No. HR0011-25-C-0300. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Defense Advanced Research Projects Agency (DARPA).

References

[ABN+92] Noga Alon, Jehoshua Bruck, Joseph Naor, Moni Naor, and Ron M Roth. Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs. *IEEE Transactions on information theory*, 38(2):509–516, 1992. 4

[AEL95] Noga Alon, Jeff Edmonds, and Michael Luby. Linear Time Erasure Codes With Nearly Optimal Recovery. In *Proceedings of IEEE 36th Annual Foundations of Computer Science*, pages 512–519. IEEE, 1995. 4, 5

[AGG+25] Omar Alrabiah, Zeyu Guo, Venkatesan Guruswami, Ray Li, and Zihan Zhang. Random Reed-Solomon codes achieve list-decoding capacity with linear-sized alphabets. *Advances in Combinatorics*, October 2025. 4

[AHS25] Vikrant Ashvinkumar, Mursalin Habib, and Shashank Srivastava. Algorithmic improvements to list decoding of folded Reed-Solomon codes. *arXiv preprint arXiv:2508.12548*, 2025. To appear in SODA 2026. 3, 10

[ALM+98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM (JACM)*, 45(3):501–555, 1998. 4

[Alo21] Noga Alon. Explicit expanders of every degree and size. *Combinatorica*, 41(4):447–463, 2021. 13

[AS98] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: A new characterization of NP. *Journal of the ACM (JACM)*, 45(1):70–122, 1998. 4

[BCDZ25a] Joshua Brakensiek, Yeyuan Chen, Manik Dhar, and Zihan Zhang. Combinatorial bounds for list recovery via discrete Brascamp–Lieb inequalities. *arXiv preprint arXiv:2510.13775*, 2025. To appear in STOC 2026. 8, 9, 10, 11, 12

[BCDZ25b] Joshua Brakensiek, Yeyuan Chen, Manik Dhar, and Zihan Zhang. From Random to Explicit via Subspace Designs With Applications to Local Properties and Matroids. *arXiv preprint arXiv:2510.13777*, 2025. To appear in STOC 2026. 1, 3, 4, 5, 6, 8, 9, 10, 11

[BGM24] Joshua Brakensiek, Sivakanth Gopi, and Visu Makam. Generic Reed–Solomon Codes Achieve List-Decoding Capacity. *SIAM Journal on Computing*, pages STOC23–118, 2024. 4

[CGV13] Mahdi Cheraghchi, Venkatesan Guruswami, and Ameya Velingker. Restricted isometry of Fourier matrices and list decodability of random linear codes. *SIAM Journal on Computing*, 42(5):1888–1914, 2013. 3

[CZ25] Yeyuan Chen and Zihan Zhang. Explicit Folded Reed-Solomon and Multiplicity Codes Achieve Relaxed Generalized Singleton Bounds. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, pages 1–12, 2025. 3, 4, 5, 8, 10, 11

[DEL+22] Irit Dinur, Shai Evra, Ron Livne, Alexander Lubotzky, and Shahar Mozes. Locally Testable Codes with constant rate, distance, and locality. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 357–374, 2022. 4

[Din07] Irit Dinur. The pcp theorem by gap amplification. *J. ACM*, 54(3):12–es, June 2007. 4

[GG25a] Rohan Goyal and Venkatesan Guruswami. Optimal proximity gaps for subspace-design codes and (random) Reed-Solomon codes. Cryptology ePrint Archive, Paper 2025/2054, 2025. To appear in STOC 2026. 4, 5, 8, 10, 11, 12

[GG25b] Rohan Goyal and Venkatesan Guruswami. Structure Theorems (and Fast Algorithms) for List Recovery of Subspace-Design Codes. *arXiv preprint arXiv:2512.08017*, 2025. 8, 10, 11, 12

[GK16] Venkatesan Guruswami and Swastik Kopparty. Explicit subspace designs. *Combinatorica*, 36(2):161–185, 2016. 4, 11

[GM22] Venkatesan Guruswami and Jonathan Mosheiff. Punctured low-bias codes behave like random linear codes. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 36–45, 2022. 3

[GM24] Venkatesan Guruswami and Jonathan Mosheiff. Punctured low-bias codes behave like random linear codes. *Discrete Analysis*, June 2024. Preliminary version in FOCS'22. 3

[GMR+22] Venkatesan Guruswami, Jonathan Moshieff, Nicolas Resch, Shashwat Silas, and Mary Wootters. Threshold Rates for Properties of Random Codes. *IEEE Trans. Inf. Theory*, 68(2):905–922, 2022. 3

[GR08] Venkatesan Guruswami and Atri Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Transactions on Information Theory*, 54(1):135–150, 2008. 3, 11

[GR22] Zeyu Guo and Noga Ron-Zewi. Efficient List-Decoding with Constant Alphabet and List Sizes. *IEEE Transactions on Information Theory*, 68(3):1663–1682, 2022. 3

[GW13] Venkatesan Guruswami and Carol Wang. Linear-algebraic list decoding for variants of Reed-Solomon codes. *IEEE Transactions on Information Theory*, 59(6):3257–3268, 2013. 3

[GX13] Venkatesan Guruswami and Chaoping Xing. List decoding Reed-Solomon, Algebraic-Geometric, and Gabidulin subcodes up to the Singleton bound. In *Proceedings of the 45th ACM Symposium on Theory of Computing*, pages 843–852, June 2013. 4

[GX22] Venkatesan Guruswami and Chaoping Xing. Optimal Rate List Decoding over Bounded Alphabets Using Algebraic-geometric Codes. *Journal of the ACM*, 69(2):10:1–10:48, 2022. 3

[GZ23] Zeyu Guo and Zihan Zhang. Randomly Punctured Reed-Solomon Codes Achieve the List Decoding Capacity over Polynomial-Size Alphabets. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 164–176. IEEE, 2023. 3

[HLM+25a] Jun-Ting Hsieh, Ting-Chun Lin, Sidhanth Mohanty, Ryan O'Donnell, and Rachel Yun Zhang. Explicit Two-Sided Vertex Expanders Beyond the Spectral Barrier. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, pages 833–842, 2025. 4

[HLM+25b] Jun-Ting Hsieh, Alexander Lubotzky, Sidhanth Mohanty, Assaf Reiner, and Rachel Yun Zhang. Explicit Lossless Vertex Expanders. In *Proceedings of the 66th annual Symposium on Foundations of Computer Science (FOCS)*, pages 894–911, 2025. 4

[HMMP24] Jun-Ting Hsieh, Theo McKenzie, Sidhanth Mohanty, and Pedro Paredes. Explicit two-sided unique-neighbor expanders. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 788–799, 2024. 4

[HW18] Brett Hemenway and Mary Wootters. Linear-time list recovery of high-rate expander codes. *Information and Computation*, 261:202–218, 2018. 4, 6

[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. 3, 4, 5, 6

[JS25] Fernando Granha Jeronimo and Nikhil Shagrithaya. Probabilistic Guarantees to Explicit Constructions: Local Properties of Linear Codes. *arXiv preprint arXiv:2510.06185*, 2025. To appear in STOC 2026. 1, 2, 3, 4, 5, 6, 7, 8, 9, 13, 22

[KMRS17] Swastik Kopparty, Or Meir, Noga Ron-Zewi, and Shubhangi Saraf. High-Rate Locally Correctable and Locally Testable Codes with Sub-Polynomial Query Complexity. *Journal of the ACM (JACM)*, 64(2):1–42, 2017. 4, 6

[Kop14] Swastik Kopparty. Some remarks on multiplicity codes. In Alexander Barg and Oleg R. Musin, editors, *Discrete Geometry and Algebraic Combinatorics*, volume 625 of *Contemporary Mathematics*, pages 155–176. AMS, 2014. 3

[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. (Preliminary version in *59th FOCS*, 2018). 3, 4, 6, 9

[KSY14] Swastik Kopparty, Shubhangi Saraf, and Sergey Yekhanin. High-rate codes with sublinear-time decoding. *Journal of the ACM (JACM)*, 61(5):1–20, 2014. 3, 6

[LMS25] Matan Levi, Jonathan Mosheiff, and Nikhil Shagrithaya. Random Reed-Solomon codes and random linear codes are locally equivalent. *arXiv preprint arXiv:2406.02238*, 2025. To appear in FOCS 2025. 3, 4, 6, 7, 8, 13

[LPS88] Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. Ramanujan graphs. *Combinatorica*, 8:261–277, 1988. 13

[LS25] Ray Li and Nikhil Shagrithaya. Near-Optimal List-Recovery of Linear Code Families. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2025)*, volume 353, pages 53:1–53:14, Dagstuhl, Germany, 2025. 8, 9

[Mar88] Grigorii Aleksandrovich Margulis. Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators. *Problemy peredachi informatsii*, 24(1):51–60, 1988. 13

[MOP20] Sidhanth Mohanty, Ryan O'Donnell, and Pedro Paredes. Explicit near-Ramanujan graphs of every degree. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 510–523, 2020. 13

[Mor94] Moshe Morgenstern. Existence and explicit constructions of $q+1$ regular Ramanujan graphs for every prime power q. *J. Combin. Theory Ser. B*, 62(1):44–62, 1994. 13

[MRR+21] Jonathan Mosheiff, Nicolas Resch, Noga Ron-Zewi, Shashwat Silas, and Mary Wootters. Low-density parity-check codes achieve list-decoding capacity. *SIAM Journal on Computing*, 53(6):FOCS20–38–FOCS20–73, November 2021. 3

[PK22] Pavel Panteleev and Gleb Kalachev. Asymptotically good quantum and locally testable classical LDPC codes. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 375–388, 2022. 4

[RV09] Ron M Roth and Pascal O Vontobel. List Decoding of Burst Errors. *IEEE Transactions on Information Theory*, 55(9):4179–4190, 2009. 3

[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. 3, 10

[SS96] Michael Sipser and Daniel A Spielman. Expander Codes. *IEEE Transaction on Information Theory*, 42(6), 1996. 4

[ST20] Chong Shangguan and Itzhak Tamo. Combinatorial list-decoding of Reed-Solomon codes beyond the Johnson radius. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2020, page 538–551, New York, NY, USA, 2020. Association for Computing Machinery. 3

[ST25] Shashank Srivastava and Madhur Tulsiani. List decoding expander-based codes up to capacity in near-linear time. (manuscript), 2025. 3, 4, 9

[Tam24] Itzhak Tamo. Tighter list-size bounds for list-decoding and recovery of folded Reed-Solomon and multiplicity codes. *IEEE Trans. Inform. Theory*, 70(12):8659–8668, 2024. 3

[Tan81] R. Michael Tanner. A Recursive Approach to Low Complexity Codes. *IEEE Transactions on Information Theory*, 27(5):533–547, 1981. 4

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il