Electronic Colloquium on Computational Complexity, Report No. 74 (2026)

Improved analysis of list-decodability of random linear codes: It's all about counting constraints

Rohan Goyal* Venkatesan Guruswami†

Abstract

List-decoding and list recovery ask how much corruption or uncertainty a code can tolerate while still keeping the number of plausible codewords small. For large alphabet codes, the ultimate benchmark for list-decoding is the (ε-relaxed) generalized Singleton bound, which targets list-of-L decoding radius with rate R up to radius $\frac{L}{L+1}(1-R-\varepsilon)$. We prove improved alphabet-size bounds for random linear and additive (folded) codes in this regime. Specifically, we show that random s-folded codes over any finite field $\mathbb{F}_q$ with $s = \Omega(1/\varepsilon)$ meet the ε-relaxed generalized Singleton bound for all list sizes L, matching the optimal $\exp(\Theta(1/\varepsilon))$ dependence on the alphabet size. For random linear codes, we show that alphabet size $\exp(O(\log L/\varepsilon))$ suffices, improving the previous $\exp(O(L/\varepsilon))$ bound. In the important regime of $L = \Theta(1/\varepsilon)$, where one list-decodes up to radius $(1-R-\varepsilon)$, this improves the alphabet size from $\exp(O(1/\varepsilon^2))$ to $\exp(\widetilde{O}(1/\varepsilon))$ for random linear codes.

For list recovery, we close the gap between the two best previous tradeoffs: prior work achieved either polynomial alphabet size in ℓ or near-optimal output list size, but not both simultaneously. We show that random linear codes achieve near-optimal output list size $(\ell/(R+\varepsilon))^{O(R/\varepsilon+1)}$ over alphabet size $(\ell/(R+\varepsilon))^{O((R+\varepsilon)/\varepsilon^2)}$, which is polynomial in ℓ.

Our gains stem from isolating the right combinatorial tools to count constraints, and identifying canonical configurations avoiding which suffice for list-decoding or list-recovery. For list-decoding, we combine tools from weakly-partition-connected agreement hypergraphs with the partition structure implicit in recent subspace-design arguments to count only partition-induced local profiles, capturing the genuinely new linear constraints in a bad witness. For list recovery, we pair a reworked local coordinate-wise linear framework with discrete Brascamp–Lieb inequalities to quotient arbitrary bad configurations to minimal profiles. Together, our methods yield modular techniques and a general framework for improving the analysis of random linear codes across a broad range of settings, instantiated concretely here for list-decoding and list-recovery.

Additionally, our presentation is self-contained and fully develops and proves all necessary ingredients.

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

ISSN 1433-8092

Contents

1 Introduction

The central trade-offs in list decoding and list recovery concern how much corruption or uncertainty a code of certain rate can tolerate while still keeping the number of plausible codewords small. For list-decoding, a simple information-theoretic bound says that a rate R code over an alphabet size q cannot correct a fraction of errors exceeding $h_q^{-1}(1-R)$. This limit can be approached arbitrarily closely with sufficiently large list-sizes. Let us say a code C is (ρ, L)-list-decodable if every Hamming ball of relative radius ρ contains at most L codewords of $\mathcal{C}$. Then, a standard random coding argument (see e.g., [ZP82, Eli91]) shows that a random code of rate R over an alphabet size q is, with high probability, $(h_q^{-1}(1-R-1/L), L)$-list-decodable.[1] Over sufficiently large alphabet (specifically $q = \exp(\Theta(1/\varepsilon))$), this implies that random codes of rate R are $(1-R-\varepsilon, O(1/\varepsilon))$-list-decodable.

However, fully random codes have little structure and do not admit a succinct description or encoding. The goal then becomes to study structured codes and minimize the random bits required to sample the code. In particular, we aim to understand list-decodability of *linear* codes, which do have a succinct description via a basis of the code (generator matrix). Despite a rich body of work that spans a couple of decades [Eli91, GHSZ02, GHK10, CGV13, Woo13, RW14, LW18] including a significant recent revival of interest [MRRZ+20, GLM+22, GM22, PP24, BGM23, AGG+25, LMS25, BDGZ25, BCDZ25b], our understanding of linear codes still has significant gaps. In this work, we focus on the large alphabet regime, with the goal being list-decodability up to radius $1-R-\varepsilon$.

Building on the breakthrough of [BGM23], [AGG+25] showed the existence of $(1-R-\varepsilon, O(1/\varepsilon))$-list-decodable linear codes over a field of size $\exp(O(1/\varepsilon^2))$. This was the first result that showed linear codes over any constant field size independent of n achieve near optimal list-size bounds. This result was later recovered in [LMS25] who achieved the same alphabet size, leaving a big gap with the optimal alphabet size of $\exp(\Theta(1/\varepsilon))$.

An alternate method of imposing linear structure is via the class of *additive*-codes, where the alphabet is taken to be $\mathbb{F}_q^s$ for a finite field $\mathbb{F}_q$ but the linearity is only imposed over the underlying field $\mathbb{F}_q$. This method of imposing structure via linearity only over a small field has proven to be extremely useful in explicit constructions. In particular, *all known* constructions of explicit capacity-achieving list-decodable codes (in fact, even codes decodable beyond the Johnson bound) such as [GR08, KSY14, Kop14, KRSW23, GRZ22, GX22, JMST25] are additive. We additionally note that the breakthrough of [CZ25] showing optimal list-size bounds of folded Reed-Solomon codes could be extended to show that random additive codes over alphabets of size $\exp(O(1/\varepsilon^2))$ are also $(1-R-\varepsilon, O(1/\varepsilon))$-list-decodable.

Thus, the question of whether there exist linear, additive, or other structured $(1-R-\varepsilon, O(1/\varepsilon))$ list-decodable codes with alphabet size only $\exp(O(1/\varepsilon))$ in contrast to $\exp(O(1/\varepsilon^2))$ has remained a fundamental gap in our understanding of error-correcting codes.

In this work, we close this gap for additive codes, and nearly close it for linear codes. Specifically, we show that random linear codes over a field size of $\exp(\widetilde{O}(1/\varepsilon))$ are $(1-R-\varepsilon, O(1/\varepsilon))$-list-decodable with high probability. Further, for the class of additive codes, we achieve the optimal alphabet size of $\exp(O(1/\varepsilon))$. In fact, our results are stronger in that they approach the so-called *generalized Singleton bound* for any fixed target list-size L. Our work is thereby also of broader interest to the exciting recent theory of higher order MDS codes and its connections to maximal recoverability [BGM23, Rot22, BDG24, BG25].

[1] Here $h_q(\cdot)$ is the q-ary entropy function, ad $h_q^{-1}(\cdot)$ its inverse on $[0, 1-1/q]$. It is also known this list-size trade-off is tight for random codes; see e.g. [GMR+22], though it is possible that the best codes can do better.

Generalized Singleton bound. In the large-alphabet setting, the precise benchmark for list-decoding is the generalized Singleton bound [ST20, Rot22]. A generalization of the classical Singleton bound for minimum distance to larger tuples of codewords, the generalized Singleton bound states that for any rate R and positive integer L, in any rate R code $\mathcal{C} \subseteq \Sigma^n$ of large enough block length n, there must be $L+1$ distinct codewords in $\mathcal{C}$ and a center $y \in \Sigma^n$ such that $\sum_{i=1}^{L+1} \Delta(c_i, y) \leqslant L(1 - R + o(1)))$, where by $\Delta(x, y)$ we denote the fractional Hamming distance between x, y. Accordingly, a code C is said to attain the order-L generalized Singleton bound (also called order $(L+1)$ MDS [Rot22, BGM23]) if for any $L+1$ distinct codewords $c_1, \ldots, c_{L+1} \in \mathcal{C}$ and every center $y \in \Sigma^n$,

$$\sum_{i=1}^{L+1} \Delta(c_i, y) > L(1 - R) \ . \tag{1}$$

Note that such a code is $(\frac{L}{L+1}(1-R), L)$-list-decodable, and also satisfy an "average-radius" version of list-decodability. For $L = 1$, there are MDS codes that achieve the above guarantee for $L = 1$ over an alphabet of size $O(n)$. For $L \geqslant 2$, the breakthrough work [BGM23] showed that random linear and Reed-Solomon codes over an exponentially sized alphabet achieve the generalized Singleton bound w.h.p. This exponential alphabet size is in fact inherent when $L > 2$, as shown in [BDG24].

Now, suppose we slightly relax the requirement, and demand that the code attain the ε-relaxed order-L generalized Singleton bound, where we replace the r.h.s of (1) with $L(1 - R - \varepsilon)$ for some $\varepsilon > 0$. Under this relaxation, we can have such codes, which are also $(\frac{L}{L+1}(1 - R - \varepsilon), L)$-list-decodable, over an alphabet of size $\exp(O(L/\varepsilon))$, as shown in [AGG$^+$25]. It is also known that the alphabet size has to be at least $\exp(\Omega(1/\varepsilon))$ [AGL24]. This leaves a factor L gap in the exponent between the upper and lower bounds on the alphabet size. In particular, in the important regime when $L \approx 1/\varepsilon$ (so the decoding radius is $\approx 1 - R - \varepsilon$) we have the aforementioned $\exp(\Omega(1/\varepsilon))$ vs. $\exp(O(1/\varepsilon^2))$ gap.

List-recovery. We also show that the same viewpoint yields improved bounds for list recovery. Recall that a code $\mathcal{C} \subseteq \Sigma^n$ is (δ, ℓ, L) list-recoverable if for every choice of sets $S_1, \ldots, S_n \subseteq \Sigma$ with $|S_i| \leqslant \ell$, there are at most L codewords $c \in \mathcal{C}$ with

$$\Delta(c, S_1 \times \cdots \times S_n) \leqslant \delta.$$

The case $\ell = 1$ is exactly list decoding.

For list recovery, the behavior of random linear codes is qualitatively different from that of completely random codes. While random codes can achieve output list size $O(\ell/\varepsilon)$, recent lower bounds show that all linear and additive codes necessarily require much larger output lists, roughly $\ell^{\Omega(R/\varepsilon)}$ [CZ25, LMS25, LW18, Che26]. The best previous upper bounds traded off alphabet size against output list size: [BCDZ25a, BCDZ25b] obtained near-optimal list sizes over substantially larger alphabets, whereas [LW18] obtained near optimal alphabet size with significantly larger output lists. In particular, when ε is treated as a constant, previous works could only achieve either $\mathrm{poly}(\ell)$ alphabet size or $\mathrm{poly}(\ell)$ list-size with the other parameter growing exponentially in ℓ and ε. In this work, we give the best of both worlds, achieving near optimal list-sizes with alphabet only polynomial in ℓ.

Previous works on explicit constructions. Before stating our results for list-decoding and list-recovery formally, we want to mention related work making significant progress on *explicit constructions* in this regime. Chen and Zhang [CZ25] showed that near-optimal subspace-design

codes achieve the ε-relaxed generalized Singleton bound, implying in particular that folded Reed–Solomon codes do as well. Brakensiek, Chen, Dhar, and Zhang [BCDZ25b] showed that subspace-design codes, and hence folded Reed-Solomon codes, also achieve optimal list-sizes for list-recovery. More recently, Jeronimo, Mittal, Srivastava, and Tulsiani [JMST25] gave the first explicit codes over alphabets of constant size (depending only on L, ε) that achieve the ε-relaxed generalized Singleton bound. [JS25] later improved [JMST25]'s construction to get near optimal list-recovery list-size bounds also over alphabets of constant size (depending only on ℓ, ε).

Previously, constructions for list-decoding were based on algebraic-geometric codes, which were shown to be $(1 - R - \varepsilon, L(\varepsilon))$-list-decodable over $\exp(\widetilde{O}(1/\varepsilon^2))$ alphabet size for a much larger but constant list-size $L(\varepsilon)$ [GX22, GRZ22].

For broader background and information on recent progress in list-decoding of algebraic codes, see the recent survey by Kumar and Ron-Zewi [KRZ26]. For recent progress in list-recovery, see the survey by Resch and Venkitesh [RV25].

1.1 Our results

We begin by defining random linear and random additive codes in our language.

Random linear and additive codes. A random linear code of rate R and block length n over $\mathbb{F}_q$ is the image of a uniformly random linear map $\mathbb{F}_q^{Rn} \to \mathbb{F}_q^n$. More generally, a random s-additive code over (the vector) alphabet $\mathbb{F}_q^s$ is the image of a uniformly random $\mathbb{F}_q$-linear map $\mathbb{F}_q^{Rns} \to (\mathbb{F}_q^s)^n$.

1.1.1 Our results for list decoding

In this work, we show that random linear/additive codes come much closer to the completely random benchmark in the large-alphabet regime than previously known. For additive codes, we obtain the optimal alphabet-size dependence on ε. For linear codes, we improve the best previous bound from $\exp(O(L/\varepsilon))$ to $\exp(O(\log L/\varepsilon))$. All our list-decoding results hold in the stronger average-radius sense.

Our first result resolves the optimal alphabet-size question for random additive codes (as they approach the generalized Singleton bound).

Theorem 1.1 (Informal for additive codes)**.** *For every $R, \varepsilon \in (0, 1)$ and every finite field $\mathbb{F}_q$, a random s-additive code with*

$$s = \Omega(1/\varepsilon)$$

meets the ε-relaxed generalized Singleton bound for all integers L, with high probability.

In particular, when $q = 2$, random $\mathbb{F}_2$-additive codes over alphabet size $\exp(O(1/\varepsilon))$ achieve the ε-relaxed generalized Singleton bound for all L. This matches the best possible dependence on ε, up to constant factors in the exponent.

We believe that the additive viewpoint is also very natural in the large-alphabet setting. As mentioned earlier, additive codes have been very prominent in *explicit constructions* with strong properties, including folded variants of Reed-Solomon and algebraic-geometric codes [GR08, GX22], multiplicity codes [KSY14, GW13, Kop14], and expander-based constructions [ABN$^+$92, AEL95, GI01, GI05, GR08, KMRZS17, GRZ22, JMST25, JS25]. Our use of random additive codes as the vehicle for matching the optimal alphabet dependence appears to be new. One previous notable is

in [BCDZ25b] who show that sufficiently folded random additive codes form subspace-design codes with high probability.

Our second list-decoding result gives the best known alphabet-size bound for random linear codes.

Theorem 1.2 (Informal for linear codes)**.** *For every $R, \varepsilon \in (0,1)$ and positive integers n, L with $n = \Omega(L/\varepsilon)$, a random linear code over $\mathbb{F}_q$ meets the order-L ε-relaxed generalized Singleton bound with high probability whenever*

$$q \geqslant \exp\left(O\left(\frac{\log L}{\varepsilon}\right)\right).$$

In particular, in the regime $L = \Theta(1/\varepsilon)$ where the goal is to list-decode a fraction $(1 - R - \varepsilon)$ of errors, this improves the alphabet-size bound from $\exp(O(1/\varepsilon^2))$ to $\exp(\widetilde{O}(1/\varepsilon))$, coming within a polylogarithmic factor in the exponent of the information-theoretic optimum.

1.1.2 Our results for list recovery

In this work, we also show that random linear/additive codes with significantly smaller alphabet sizes come close to achieving optimal list-size possible for list-recovery of linear codes over arbitrary alphabet sizes than previously known. In particular, for list recovering at distance $1 - R - \varepsilon$, we know that list sizes need to be of size at least $\ell^{\Omega(R/\varepsilon)}$, and additionally the best possible alphabet size known for list sizes independent of n at distance $1 - R - \varepsilon$ is $\ell^{\Omega(1/\varepsilon)}$[LW18] but unfortunately here the list size is $(\ell/\varepsilon)^{\ell/\varepsilon}$ growing exponentially in ℓ.

The best previous result for near optimal list sizes due to [BCDZ25a, BCDZ25b] then trades off alphabet size getting alphabet size $\exp(\Omega(\ell^{R/\varepsilon}/\varepsilon))$. In particular, when ε is treated as a constant, previous works could only achieve either $\mathrm{poly}(\ell)$ alphabet size or $\mathrm{poly}(\ell)$ list-size, while letting the other parameter grow exponentially. Our next theorem gives the best of both worlds.

Theorem 1.3 (Informal)**.** *A random $\mathbb{F}_q$-linear code of rate $R - \varepsilon_0$ is $(1 - R - \varepsilon, \ell, L_{\ell,R,\varepsilon})$ list-recoverable with high probability whenever*

$$q > (2L_{\ell,R,\varepsilon})^{4/\varepsilon_0} \qquad \text{and} \qquad n > 4L_{\ell,R,\varepsilon}^2/\varepsilon_0, \quad \text{where} \quad L_{\ell,R,\varepsilon} \leqslant \left(\frac{\ell}{R+\varepsilon}\right)^{(R+\varepsilon)/\varepsilon}.$$

In particular, random linear codes achieve near-optimal output list size

$$L_{\ell,R,\varepsilon} = \left(\frac{\ell}{R+\varepsilon}\right)^{O(R/\varepsilon+1)} \quad \text{over alphabets of size} \quad \left(\frac{\ell}{R+\varepsilon}\right)^{O((R+\varepsilon)/\varepsilon^2)}.$$

This matches the near-optimal list-size guarantees of [BCDZ25a, BCDZ25b] while simultaneously achieving alphabet size polynomial in ℓ. We note that the above result also naturally holds for random additive codes over the same alphabet sizes.

Our list-recovery theorem can also be used to recover a slightly weaker version of our list-decoding bound for random linear codes.

Before moving on to an overview of our techniques, we would like to highlight that our presentation is entirely self-contained and proves all necessary ingredients.

1.2 Our techniques

Overview. At a high level, proving that a random linear codes has a target local property (such as list-decoding or list-recovery), is all about showing that any given bad configuration is unlikely, and then union bounding over all possible configurations. Thus, understanding local properties of random linear codes amounts to counting coordinate-wise linear constraints.

Our proofs isolate the right combinatorial tools to count constraints, and identify canonical configurations, avoiding which is sufficient to list-decode or list-recover. This methodology allows us to significantly reduce the number of configurations to union bound over, and since we use the tools and techniques established in a long line of works in this area in a whitebox manner, we are able to account for each probability error significantly more carefully.

Our list-decoding techniques brings together ideas from all of [AGG$^+$25, CZ25, LMS25, BCDZ25a, BCDZ25b], and presents a unified view for all of them.

List Decoding. For list-decoding, we combine tools from weakly-partition-connected agreement hypergraphs of Alrabiah, Guruswami, and Li, with the partition structure implicit in recent subspace-design arguments such as [CZ25]. First, we show that it suffices to avoid bad list-decoding configurations arising from weakly-partition-connected hypergraphs. Now, for such hypergraphs, to prove each such configuration is unlikely, we count such configurations in a way dependent on the rank of the arising configuration.

In particular, to establish list-decoding if we want to show that there are no $L+1$ codewords close to a received word y. We establish that this separately, for all ranks $r \in \mathbb{N}$, it is unlikely that there are $L+1$ codewords close to any received word span a rank r space. Splitting this off into rank dependent claims allows us to use better probability bounds and counts dependent on rank r.

To count constraints within spaces of low dimension, we use the partition structure implicit in [CZ25], to pass from equality constraints on $L+1$ codewords, to a canonical partition, and then replace the original agreement hypergraph by a *partition-induced sub-hypergraph* that retains only the first intersection with each part. This removes redundant equalities and isolates only the agreements that contribute genuinely new linear constraints.

List recovery. For list recovery, agreement hypergraphs alone are no longer useful for constraint counting. Here we instead use discrete Brascamp–Lieb inequalities following [BCDZ25a, BCDZ25b]. To go to canonical configurations (the analog of weakly partition connected hypergraphs for list-decoding), starting from a bad list-recovery configuration, we quotient by a maximal subspace so that there are too many constraints on the quotient space. This produces a *canonical* object to which the same counting philosophy applies. We can now account only for constraints that are genuinely new.

Since the Brascamp-Lieb inequality is a cruder combinatorial tool to work with than weakly-partitioned-hypergraphs, our alphabet size bounds for list-recovery are polynomially off from optimal. Regardless, we can also recover slightly weaker forms of our RLC results from the list-recovery ideas and [BCDZ25a]'s remainder Brascamp-Lieb inequality getting $\exp(\widetilde{O}(1/\varepsilon))$ alphabet sizes for random linear codes as well, but with worse constants and larger block length requirement. For completeness, we present this view in Appendix C.

Consequently, our paper is able to extract the key ideas and techniques in recent developments on both list-decoding and list-recovery, combine them, and use more conscious combinatorial counting methods and probability bounds, thereby giving a general template for analyzing local properties of random linear codes.

2 Preliminaries

We begin by introducing the basic coding-theoretic definitions we will be using.

Definition 1 (Fractional Hamming Distance)**.** For any two vectors x, y in Σ^n where Σ is some alphabet, we define $\Delta(x,y) = \frac{|\{i \in [n] : x_i \neq y_i\}|}{n}$ to be the fraction of coordinates where they differ.

For a set $S \subseteq \Sigma^n$, we define $\Delta(x,S) = \min_{y \in S} \frac{|\{i \in [n] : x_i \neq y_i\}|}{n}$ to be the minimum fractional Hamming distance of x to its closest vector in S.

The two fundamental quantities associated with a code are its rate and distance.

Definition 2 (Distance of a code)**.** For code $\mathcal{C} \subseteq \Sigma^n$, we define its (relative) distance as $\Delta(\mathcal{C}) = \min_{x,y \in \mathcal{C}, x \neq y} \Delta(x,y)$

Definition 3 (Rate of a code)**.** For a code $\mathcal{C} \subseteq \Sigma^n$, its rate $R(\mathcal{C})$ is defined as $R(\mathcal{C}) = \frac{\log_{|\Sigma|} |\mathcal{C}|}{n}$

We will focus on linear/additive codes in this paper, defined as follows.

Definition 4 (Additive codes)**.** Let $\mathbb{F}$ be a finite field and let $\Sigma = \mathbb{F}^s$ for some positive integer s. A code $\mathcal{C} \subseteq \Sigma^n$ is said to be $\mathbb{F}$-additive (or just additive when the field $\mathbb{F}$ is clear from context or not relevant to the discussion) if $\mathcal{C}$ is an $\mathbb{F}$-linear subspace of Σ^n. When $s = 1$, the code is simply called a linear code.

2.1 List-Decoding and List-Recovery

Definition 5 (Average radius list-decoding)**.** A code $\mathcal{C} \subseteq \Sigma^n$ is (δ, L)-average-radius list-decodable if for all distinct $c_1, \ldots, c_L, c_{L+1} \in \mathcal{C}$, their average distance to any center is greater than δ, i.e.,

$$\frac{\sum_{i=1}^{L+1} \Delta(c_i, y)}{L+1} > \delta \quad \text{for every } y \in \Sigma^n \ .$$

Definition 6. A code $\mathcal{C} \subseteq \Sigma^n$ is said to meet order L ε-relaxed generalized singleton bound, if for all distinct $c_1, \cdots, c_{L+1} \in \mathcal{C}$, and $y \in \Sigma^n$, we have that

$$\sum_{i=1}^{L+1} \Delta(c_i, y) > L(1 - R - \varepsilon)$$

i.e. if the code is $\left(\frac{L(1-R-\varepsilon)}{L+1}, L\right)$ average-radius list-decodable.

For simplicity, we say that the code $\mathcal{C}$ is $(\varepsilon, L)-$GSB decodable.

Definition 7 (List-recovery)**.** A code $\mathcal{C} \subseteq \Sigma^n$ is (δ, ℓ, L)-list-recoveable if for all sets $S_1, \ldots, S_n \subseteq \Sigma$ with $|S_i| \leqslant \ell$ for each i, we have

$$|\{c \in \mathcal{C} \mid \Delta(c, S_1 \times S_2 \times \cdots \times S_n) \leqslant \delta\}| \leqslant L \ .$$

2.2 Agreement hypergraphs

The following connectivity property of hypergraphs has served as a powerful abstraction for analyzing list-decodability. Note that for graphs the condition says that every cut has at least t edges, i.e., the graph is t-edge-connected.

Definition 8. A hypergraph $\mathcal{H} = (X, E)$ is t-WPC (weakly partition connected) if for all partitions $P_0 \sqcup P_1 \sqcup \cdots \sqcup P_r$ of the vertices X, the following holds:

$$\sum_{e \in E} \max(|\{j \mid e \cap P_j \neq \emptyset\}| - 1, 0) \geqslant tr \ .$$

Lemma 2.1. *Let hypergraph $\mathcal{H} = (X, E)$ be t-WPC. Then, for any $j \in X$, we have that*

$$|\{e \in E \mid j \in e\}| \geqslant t$$

Proof. Observe that if we consider the partition $\mathcal{P}_0 = \{j\}$ and $\mathcal{P}_1 = X \setminus \{j\}$. Then, we have that

$$\sum_{e \in E} \max(|\{j \mid e \cap P_j \neq \emptyset\}| - 1, 0) \geqslant t \implies \sum_{e \in E} \mathbf{1}(|e \cap \mathcal{P}_0| \geqslant 1) \geqslant t$$

as desired. □

Lemma 2.2 ([AGG+25])**.** *If $\mathcal{H} = (X, E)$ is a hypergraph such that $\sum_{e \in E} \max(|e| - 1, 0) \geqslant t \cdot (|X| - 1)$ with $|X| \geqslant 2$, then there exists $X' \subseteq X$ such that $\mathcal{H}' = (X', \{e \cap X' \mid e \in E\})$[2] is t-WPC.*

For a proof, see Lemma B.1. In Appendix B, we also present Chen and Zhang's [CZ25] proof of the optimal list-decoding bounds of subspace design codes.

2.3 Brascamp-Lieb inequalities

Definition 9 (Linear subspaces)**.** For a vector space V, we define $\mathcal{L}(V)$ to be the set of all linear subspaces of V.

Definition 10. Let V be a linear space. A function $f : \mathcal{L}(V) \to \mathbb{R}$ is called *submodular* if

- (Zeroness) $f(\{0\}) = 0$.
- (Monotonicity) For all $U \subseteq W$, we have that $f(U) \leqslant f(W)$.
- (Submodularity) For all U, W, we have that $f(U) + f(V) \geqslant f(U + V) + f(U \cap V)$.

A key insight of [BCDZ25a] was to note and exploit the connection between discrete Brascamp-Lieb inequalities[CC09, CDK+13, CDK+24] and subspace-design codes for tasks of list-decoding and list-recovery. In this work, we also show how to use these inequalities *directly* to analyze random linear codes.

First, we state a version of the discrete Brascamp-Lieb inequality.[3]

[2] Note that multiple edges don't need to be distinct. Thus, $|E'| = |E|$.

[3] We find it convenient to work with the "dual form" of the statement in [BCDZ25a]. To match the hypothesis of their Theorem 1.6, one can take $E = V^*$, $A = U^\perp \subseteq V^*$, and $E_i \subseteq V_i^*$ with $E_i \hookrightarrow E$ given by $g \longmapsto g \circ \pi_i$.

Theorem 2.3 (Submodular Brascamp-Lieb Inequality)**.** *Let E be a linear space and let $E_1, \dots, E_n \subseteq E$ be subspaces. Suppose that for some $s_1, \dots, s_n \geqslant 0$, the following inequality holds for every linear subspace $F \subseteq E$:*

$$\dim E - \dim F \leqslant \sum_{i=1}^{n} s_i[\dim E_i - \dim(F \cap E_i)] \ .$$

Then, for every submodular function $f : \mathcal{L}(E) \to \mathbb{R}$, we have

$$f(E) \leqslant \sum s_i f(E_i) \ .$$

We provide a complete proof of the above inequality in Appendix A as Theorem A.1.

Theorem 2.4 (Entropic BL)**.** *Let A be a finite-dimensional vector space over $\mathbb{F}_q$. Let E be the linear space of functionals from A to $\mathbb{F}_q$, and let $E_1, E_2, \dots, E_n \subseteq E$ be subspaces. Suppose that for some $s_1, \dots, s_n \geqslant 0$ the following inequality holds for all linear subspaces $F \subseteq E$:*

$$\dim E - \dim F \leqslant \sum_{i=1}^{n} s_i \cdot \big(\dim E_i - \dim(F \cap E_i)\big) \ .$$

Then, if Z is any distribution on A, we have

$$H(E(Z)) \leqslant \sum s_i H(E_i(Z))$$

where H is Shannon entropy and $U(Z)$ for a subspace $U \subseteq E$ is the random variable given by applying all functionals in U to Z.

Proof. Let $f(U) = H(U(Z))$. Now, by Theorem 2.3, it would be sufficient to prove that f is submodular.

Now, clearly $f(E) = H(Z)$ as applying all functionals of E is equivalent to just declaring the appropriate element of V. Clearly, $f(\{0\}) = 0$ and monotonicity follows since more functional valuations can only increase entropy.

Now, observe that for any subspaces $U, W \subseteq E$, we want

$$f(U)+f(W) \geqslant f(U+W)+f(U\cap W) \iff f(U)-f(U\cap W)+f(W)-f(U\cap W) \geqslant f(U+W)-f(U\cap W) \ .$$

Or equivalently we want $H(U(Z) \mid (U \cap W)(Z)) + H(W(Z) \mid (U \cap W)(Z)) \geqslant H((U + W)(Z) \mid (U\cap W)(Z)) = H(U(Z), W(Z) \mid (U\cap W)(Z))$. But this holds since it is equivalent to $I(U(Z); W(Z) \mid (U \cap W)(Z)) \geqslant 0$ which we know is true. □

2.4 Reworked LCL framework

Local properties were first introduced in [MRRZ+20] to capture list-decoding and related properties of random LDPC codes. This framework has since been utilized and further developed in a series of works [GM22, GMR+22, LMS25]. In particular, [LMS25] defined *local coordinate-wise linear* (LCL) properties and established threshold behaviors for all LCL properties, and proved that the thresholds for all LCL properties are equal for random linear codes and randomly punctured Reed-Solomon codes. It was shown in [BCDZ25b] that the framework of LCL properties can also be extended from linear codes to additive codes. In [GG25a], the problem of proximity gaps of codes

was also shown to be captured by a related LCL property, allowing them to establish proximity gaps for random Reed-Solomon codes.

In this work, we work with a more abstract view of LCL properties for additive codes inspired by [LMS25, BCDZ25b]. Our definitions deviate slightly from [LMS25] and previous works in order to be uniform for linear and additive codes. We begin by defining a [LMS25]-style potential function for local properties.

Definition 11. Let $\mathbb{F}_q$ be a field, let V be any finite dimensional vector space over $\mathbb{F}_q$, and $n \in \mathbb{N}$, define $\Phi_V : \mathcal{L}(V) \times (\mathcal{L}(V))^n \times \mathbb{R} \to \mathbb{R}$ as follows:

$$\Phi_V(U, (\mathcal{V}_1, \ldots, \mathcal{V}_n), \alpha) = \alpha \dim U - \frac{\sum_{i=1}^{n} (\dim U - \dim(U \cap \mathcal{V}_i))}{n}$$

Theorem 2.5. *Let V be a vector space and let $U, W, \mathcal{V}_1, \ldots, \mathcal{V}_n \in \mathcal{L}(V)$, let $M : V \to V'$ be a surjective linear map such that $\ker(M) = W$, and α be a real. Then*

$$\Phi_V(U + W, (\mathcal{V}_1, \ldots, \mathcal{V}_n), \alpha) - \Phi_V(W, (\mathcal{V}_1, \ldots, \mathcal{V}_n), \alpha) = \Phi_{V'}(MU, (M\mathcal{V}_1, \ldots, M\mathcal{V}_n), \alpha)$$

Proof. Note that it is sufficient to prove that for each $\mathcal{V}_i$, we have that

$$\dim((U + W) \cap \mathcal{V}_i) - \dim(W \cap \mathcal{V}_i) = \dim(M(U + W) \cap M\mathcal{V}_i) = \dim(MU \cap M\mathcal{V}_i)$$

but this follows from the definition of M as it does exactly the quotienting by W operation and the rank-nullity theorem. □

Definition 12 (Dual Space)**.** For any vector space V over a field $\mathbb{F}$, its dual V^* is the space of all linear functionals $M : V \to \mathbb{F}$.

Definition 13 (Annihilator)**.** Let V be a vector space and V^* be its dual space. For any subspace $A \subseteq V$, let $A^\perp$ be the subspace of V^* defined as $A^\perp = \{v \in V^* \mid v(a) = 0 \ \forall a \in A\}$.

Definition 14 (Joint Kernel)**.** Let V be a vector space and V^* be its dual space. For any subspace $B \subseteq V^*$, let B° be the subspace of V defined as $B^\circ = \{v \in V \mid b(v) = 0 \ \forall b \in B\}$

Note that the joint kernel of the subspace of functionals B is defined as the intersection of the kernels of all the functionals in B. Additionally, the annihilator and joint kernel are dual concepts i.e. $(A^\perp)^\circ = A$.

Definition 15 ((Containment of) Local profiles)**.** Let $\mathsf{Enc}_1, \ldots, \mathsf{Enc}_n : \mathbb{F}_q^k \to \mathbb{F}_q^s$ be linear maps for some positive integer s, and $\mathcal{C} = \{(\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x)) \mid x \in \mathbb{F}_q^k\}$ be the associated $\mathbb{F}_q$-additive code.

Let V be any $\mathbb{F}_q$-linear space. A sequence $(\mathcal{V}_1, \ldots, \mathcal{V}_n) \in \mathcal{L}(V)^n$ is called V-local profile, or simply local profile when V is clear from context.

We say that $\mathcal{C}$ contains a V-local profile $(\mathcal{V}_1, \ldots, \mathcal{V}_n)$ if there exists a subspace $A \subseteq \mathbb{F}_q^k$ and an isomorphism $\varphi_A : V \to A^*$ such that for each $i \in [n]$, we have $\varphi_A(\mathcal{V}_i)^\circ \subseteq \ker(\mathsf{Enc}_i)$.

Example. (Distance as a Local Property) To elaborate on our definition of local profiles and containment, we begin with the example of a code's distance. To capture the property of a code having distance δ, then if we consider V to be the one dimensional space $\mathbb{F}_q$, and for every $S \subseteq [n]$, with $|S| > (1-\delta)n$, we consider the local profile $\mathcal{V}_S = (\mathcal{V}_1, \cdots, \mathcal{V}_n)$, given by $\mathcal{V}_s = \{0\}$ for all $s \in S$, and equal to $\mathcal{V}_s = \mathbb{F}_q$ otherwise.

Now, if the code contains any such profile, then there is a space A of dimension 1 in $\mathbb{F}_q^k$, say spanned by the element $a \neq 0$, and an isomorphism $\varphi_A : \mathbb{F}_q \to A^*$ such that $\varphi_A(\mathcal{V}_i)^\circ \subseteq \ker(\mathsf{Enc}_i)$. Now, for any $s \in S$, we must thus have that $\{0\}^\circ \subseteq \ker(\mathsf{Enc}_s)$. But, the 0 map identically maps everything to 0, thus, we must have that $A \subseteq \ker(\mathsf{Enc}_s)$ for all $s \in S$. Thus, $a_S = 0$ i.e., $\Delta(a, 0) \leqslant 1 - \frac{|S|}{n} < \delta$. Similarly, we know that for linear and additive codes, it is sufficient to consider distance from the 0 codeword, we see that this definition of local properties captures distance of a code.

Natural extensions of the above characterizations extend to list-decoding and list-recovery as well, as is demonstrated in later sections.

Lemma 2.6. *Let $\alpha \in (0,1)$ be a constant. Let V be a linear space and $(\mathcal{V}_1, \ldots, \mathcal{V}_n)$ be a local profile. Let $W \subseteq V$.*

If a code $\mathcal{C} = \{(\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x)) \mid x \in \mathbb{F}_q^k\}$ contains $\mathcal{V} = (\mathcal{V}_1, \ldots, \mathcal{V}_n)$, then it also contains $((\mathcal{V}_1 + W)/W, \ldots, (\mathcal{V}_n + W)/W) \in \mathcal{L}(V/W)^n$.

Proof. Now, if $\mathcal{C}$ contains $(\mathcal{V}_1, \ldots, \mathcal{V}_n)$, then there exists a subspace $A \subseteq \mathbb{F}_q^k$ and an isomorphism $\varphi : V \to A^*$ and $(\varphi\mathcal{V}_i)^\circ \subseteq \ker(\mathsf{Enc}_i)$. Let $(\varphi W)^\circ = A'$. We now define a map $M : A^* \to A'^*$ given by restricting evaluations of the functionals to only be on A'. Note that $\ker(M \circ \varphi) = W$. Thus, $M \circ \varphi\mathcal{V}_i \cong (\mathcal{V}_i + W)/W$. Additionally, note that $A'^* \cong V/W$.

Thus, it is sufficient to prove that $(M\varphi\mathcal{V}_i)^\circ \subseteq \ker(\mathsf{Enc}_i)$.

Let $a \in A'$ be such that $(M\varphi\mathcal{V}_i)(a) = 0 \implies \varphi\mathcal{V}_i(a) = 0$ since M only restricts to evaluating on A' but does not change values. In particular, $a \in (\varphi\mathcal{V}_i)^\circ \implies a \in \ker(\mathsf{Enc}_i)$ as desired. □

Theorem 2.7. *Let V be a linear space such that the local profile $\mathcal{V} = (\mathcal{V}_1, \ldots, \mathcal{V}_n) \in \mathcal{L}(V)^n$ satisfies $\Phi(V, \mathcal{V}, \alpha) \leqslant 0$. Then letting $k = \alpha sn - \beta$, and $\mathsf{Enc}_1, \ldots, \mathsf{Enc}_n : \mathbb{F}_q^k \to \mathbb{F}_q^s$ be independent uniformly random linear maps, we have*

$$\Pr_{\mathsf{Enc}_1, \ldots, \mathsf{Enc}_n}[\mathcal{C} \text{ contains } (\mathcal{V}_1, \ldots, \mathcal{V}_n)] \leqslant q^{-\beta \cdot \dim V}$$

where $\mathcal{C} = \{(\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x)) \mid x \in \mathbb{F}_q^k)\}$.

Proof. Let $d = \dim V$. Additionally, let $v_1, \ldots, v_d$ be a basis of V.

Note that if $\mathcal{C}$ contains $(\mathcal{V}_1, \ldots, \mathcal{V}_n)$ then, there exist linearly independent $a_1, \ldots, a_d \in \mathbb{F}_q^k$ with $\mathbf{a} = (a_1, \ldots, a_d)$ and an isomorphism $\varphi_{\mathbf{a}} : V \to \mathrm{span}(a_1, \ldots, a_d)^*$ satisfying $(\varphi_{\mathbf{a}} v_i)(a_j)$equals 1 if $i = j$ and 0 otherwise, and further $\varphi_{\mathbf{a}}(\mathcal{V}_i)^\circ \subseteq \ker(\mathsf{Enc}_i)$.

Therefore,

$$\Pr[\mathcal{C} \text{ contains } (\mathcal{V}_1, \ldots, \mathcal{V}_n)] \leqslant \sum_{\text{linear independent } a_1, \ldots, a_d \in \mathbb{F}_q^k} \Pr[\forall i \in [n], (\varphi_{\mathbf{a}}\mathcal{V}_i)^\perp \subseteq \ker(\mathsf{Enc}_i)] \ .$$

Fix a linearly independent choice of $a_1, \ldots, a_d$ in $\mathbb{F}_q^k$. Now,

$$\Pr[\forall i \in [n], (\varphi_{\mathbf{a}}\mathcal{V}_i)^\circ \subseteq \ker(\mathsf{Enc}_i)] = \prod_{i \in [n]} \Pr[(\varphi_{\mathbf{a}}\mathcal{V}_i)^\circ \subseteq \ker(\mathsf{Enc}_i)] = \prod_{i \in [n]} q^{-s \dim(\varphi_{\mathbf{a}}\mathcal{V}_i)^\circ}$$

The first equality holds since Enc_i are all independent, and the second since Enc_i is a uniformly random map from $\mathbb{F}_q^k \mapsto \mathbb{F}_q^s$. Now, $\dim(\varphi_{\mathbf{a}}\mathcal{V}_i)^\circ = \dim V - \dim \mathcal{V}_i$, so

$$\Pr[\forall i \in [n], (\varphi_{\mathbf{a}}\mathcal{V}_i)^\circ \subseteq \ker(\mathsf{Enc}_i)] = q^{-s\sum_{i=1}^n (\dim V - \dim \mathcal{V}_i)} = q^{ns\Phi_V(V,\mathcal{V},\alpha) - \alpha ns \dim V} \leqslant q^{-\alpha nsd} \ .$$

Finally, a union bound over the at most q^{kd} choices of $\mathbf{a}$ gives us

$$\Pr[\mathcal{C} \text{ contains } (\mathcal{V}_1, \ldots, \mathcal{V}_n)] \leqslant q^{kd} \cdot q^{-\alpha n s \cdot d} = q^{-\beta d} \ . \qquad \square$$

3 List-decoding alphabet size bounds

We begin by discussing how [AGG+25]'s agreement hypergraphs help capture the properties of average-radius list-decoding that we require and how weakly-partition connected hypergraphs can be utilized.

3.1 Agreement hypergraphs to list-decoding

Definition 16. A code $\mathcal{C} \subseteq \Sigma^n$ is (α, L) strong average-agreement list-decodable if for every subset of m distinct codewords $\{c_1, \ldots, c_m\} \subseteq \mathcal{C}$ where $2 \leqslant m \leqslant L$, and every sequence of subsets $e_1, \ldots, e_n \subseteq [m]$ satisfying

$$\sum_{i=1}^{n} \max(0, |e_i| - 1) \geqslant \alpha \cdot n \cdot (m-1),$$

there exists at least one index $i \in [n]$ such that not all the codeword symbols $c_{j,i}$, $j \in e_i$, are equal.

Theorem 3.1. *If a rate R code $\mathcal{C}$ is $(\alpha, L+1)$-strong average-agreement list-decodable, then $\mathcal{C}$ is $(\alpha - R, L')-$GSB decodable for all $L' \leqslant L$.*

Proof. For the sake of contradiction, assume that $\mathcal{C}$ is not $(\alpha - R, L')-$GSB decodable. Then, there exist distinct $c_1, \ldots, c_{L'+1} \in \mathcal{C}$ and an element $y \in \Sigma^n$ such that

$$\sum_{i=j}^{L'+1} \Delta(c_j, y) \leqslant L'(1-\alpha).$$

Let $e_i = \{j \in [L+1] \mid c_{j,i} = y_i\}$. Now, note that

$$\sum_{i=1}^{n} \max(0, |e_i| - 1) \geqslant -n + \sum_{j=1}^{L'+1} \sum_{i=1}^{n} \mathbf{1}(c_{j,i} = y_i) \geqslant n(-1 + \sum_{j=1}^{L'+1} (1 - \Delta(c_i, y))) \geqslant nL'\alpha$$

But, then we must have by the $(\alpha, L+1)$-strong average-agreement list-decodability of the code, that there exists an $i \in [n]$ such that $\{c_{j,i} : j \in e_i\} = \{y_i\}$ has size at least 2 which is a contradiction. $\square$

Lemma 3.2 (Definition 16+Lemma 2.2)**.** *A code $\mathcal{C} \subseteq \Sigma^n$ is (α, L)-strong average-agreement average list-decodable, if for all t-WPC hypergraphs $\mathcal{H} = (X, E)$ with $t \geqslant \alpha n$, and $E = \{e_1, \ldots, e_n\}$, there do not exist distinct codewords $\{c_j\}_{j \in X} \in \mathcal{C}$ such that for each $i \in [n]$, the i'th symbols of the codewords c_j, $j \in e_i$, are all equal.*

Proof. Assume for contradiction that $\mathcal{C}$ is not (α, L)-strong average-agreement list-decodable. By Definition 16, there exists a hypergraph $\mathcal{H} = (X, E)$ with $2 \leqslant |X| \leqslant L$ and distinct codewords $\{c_j\}_{j \in X} \in \mathcal{C}$ such that for all $i \in [n]$, the symbols $c_{j,i}$, $j \in e_i$ are all equal, and

$$\sum_{i=1}^{n} \max(|e_i| - 1, 0) \geqslant \alpha n(|X| - 1).$$

Let $t = \frac{\sum_{i=1}^{n} \max(|e_i|-1,0)}{|X|-1}$. We know that $t \geqslant \alpha n$. By Lemma 2.2, there exists a subset $X' \subseteq X$ such that the induced hypergraph $\mathcal{H}' = (X', \{e_i \cap X'\}_{i=1}^{n})$ is t-WPC.

Since $X' \subseteq X$, the codewords indexed by X' remain distinct, and $|\{c_{j,i} \mid j \in e_i \cap X'\}| \leqslant 1$ for all $i \in [n]$. This provides a t-WPC hypergraph(where $t \geqslant \alpha n$) contradicting the hypothesis. □

3.2 Partitions from bad list-decoding configurations

The definition of weakly partitioned hypergraphs enables us to worry only about counting the number of constraints imposed by the list-decoding property on extremal configurations. But this requires coming up with a correct partitioning of the vertices to count how many constraints are imposed.

For simplicity, let us begin by assuming that $v_1, \cdots, v_m \in \mathbb{F}_q^k$ are linearly independent and their encodings are close to some element $y \in \Sigma^n$ i.e., $\Delta(\mathsf{Enc}(v_j), y)$ is small for each v_j. Then for every pair $i_1 \neq i_2 \in [m]$ and index $j \in [n]$, $\mathsf{Enc}_j(v_{i_1}) = \mathsf{Enc}_j(v_{i_2})$ is a new linear constraint on the encoding map. Therefore, if $e_j = \{i \mid \mathsf{Enc}_j(v_i) = y_i\}$, the number of constraints on Enc_j is precisely $\max(|e_j|-1, 0)$. Since $\mathsf{Enc}(v_i)$ is close to y, a large number of constraints are imposed. Now, we can hope that these constraints would not be simultaneously satisfied if Enc_js are all uniformly random linear maps.

In contrast, when $v_1, \cdots, v_m$ are not linearly independent, the number of constraints is not so obvious to count. Indeed this is the central difficulty in analyzing list-decodability of random linear, as opposed to fully random, codes. To be able to count constraints even when $v_1, \cdots, v_m$ are not linearly independent, we employ the following partition of $v_1, \cdots, v_m$ which was also used in [CZ25].

Definition 17 (Constraint counting partitions)**.** Given vectors $v_1, v_2, \ldots, v_m$ in some vector space V with $v_1 = 0$, $v_2, \ldots, v_{r+1}$ linearly independent, and $\mathsf{dim}(\mathrm{span}(v_1, \ldots, v_m)) = r$, the partition $\mathcal{P}(v_1, \ldots, v_m) = \mathcal{P}_0 \sqcup \mathcal{P}_1 \sqcup \cdots \sqcup \mathcal{P}_r$ of $[m]$ is given by

$$\mathcal{P}_j = \{i \in [m] \mid v_i \in A_{j+1} \setminus A_j\} \text{ for } j \in \{0, 1, \ldots, r\} ,$$

where $A_0 = \emptyset$ and $A_j = \mathrm{span}(v_1, \ldots, v_j)$ for $j \in \{1, \ldots, r+1\}$.

In particular, we again do have that any sets of elements from distinct parts are linearly independent. Thus, the number of constraints on Enc_j is at least $\max\big(\sum_{i=0}^{r} \mathbf{1}(e_j \cap \mathcal{P}_i \neq \emptyset) - 1, 0\big)$. Additionally, note that weakly partition hypergraphs (See Definition 8) enable us to count exactly this quantity! Motivated by the above counting, we understand that once a partition is fixed, we only need to care about the first place an edge intersects the partition and nowhere else. Thus, we make the following definition for an induced hypergraph given a partition.

Definition 18 (Partition induced sub-hypergraph)**.** For any hypergraph $\mathcal{H} = (X, E)$, and an ordering [4] $>_X$ on X, and partition $\mathcal{P} = \mathcal{P}_0 \sqcup \mathcal{P}_1 \sqcup \cdots \sqcup \mathcal{P}_r$ of X, we define $\mathcal{H}_{\mathcal{P}}$ as follows:

For each $i \in [n]$, let $e_i' = \{\min(e_i \cap \mathcal{P}_j) \mid j \in \{0, 1, \ldots, r\}, |e_i \cap \mathcal{P}_j| \geqslant 1\}$ and let $\mathcal{H}_{\mathcal{P}} = (X, E')$ where E' are the hyperedges given by $e_1', \ldots, e_n'$.

Remark 1 (Simpler proof [CZ25] list-decoding result)**.** In Appendix B, we present a self-contained short proof of Chen and Zhang's [CZ25] result establishing optimal list-size bounds for subspace-design codes, based on working with Definition 8 and Definition 17.[5]

[4] Usually, X will be identified with a set of integers, so the ordering will be the canonical one. Hence, we omit the ordering from the definitions.

[5] We note that [KRZ26] also present an alternative presentation of [CZ25]'s proof. We believe ours is arguably

3.3 Local profiles from bad list-decoding configurations

In the previous subsections, we have managed to connect constraint counting for list-decoding with weakly partitioned hypergraphs and suitably defined partitions. Now, to prove that random linear and additive codes do not satisfy the constraints that are imposed on them, we need to abstract out the local profiles each of these configurations impose.

Definition 19 (Good vectors)**.** Let m be a positive integer and fix any integer $0 \leqslant r \leqslant m-1$. We define

$$S_{m,r} = \{(w_1, \ldots, w_m) \in (\mathbb{F}_q^r)^m \mid w_1 = 0, w_2, \ldots, w_{r+1} \text{ form the canonical basis of } \mathbb{F}_q^r,\ \forall i \neq j, w_i \neq w_j\}.$$

Definition 20 (Local profiles from t-WPCs)**.** Let r, m be positive integers such that $r \leqslant m-1$.

Fix any $\mathbf{w} = (w_1, \ldots, w_m) \in S_{m,r}$. Let $\mathcal{P}_0 \sqcup \mathcal{P}_1 \sqcup \cdots \sqcup \mathcal{P}_r = \mathcal{P}(w_1, \ldots, w_m) = \mathcal{P}(\mathbf{w})$. Fix any hypergraph $\mathcal{H}' = ([m], E')$ with $E' = \{e'_1, \ldots, e'_n\}$. Let $V = (\mathbb{F}_q^r)^*$. Now, define

$$\mathcal{V}_{i,\mathcal{H}',\mathbf{w}} = \{v \in V \mid v(w_{j_1} - w_{j_2}) = 0 \ \ \forall j_1, j_2 \in e'_i\}.$$

Let

$$\mathcal{T}_{r,m,t} = \{(\mathcal{V}_{1,\mathcal{H}',\mathbf{w}}, \ldots, \mathcal{V}_{n,\mathcal{H}',\mathbf{w}}) \mid \mathbf{w} \in S_{m,r}, \mathcal{H}' \in \{\mathcal{H}_{\mathcal{P}(\mathbf{w})} \mid \mathcal{H} = ([m], E) \text{ is } t\text{-WPC}\}\}.$$

where $\mathcal{H}_{\mathcal{P}(\mathbf{w})}$ is as defined in Definition 18.

Now, that we have defined the relevant local profiles, we demonstrate that if a code is not strong average agreement list-decodable, then it must contain one of these profiles.

Claim 3.3. *Suppose an additive code $\mathcal{C} = \{(\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x)) \mid x \in \mathbb{F}_q^k\}$ is not (α, L)-strong average-agreement list-decodable. Then $\mathcal{C}$ contains the local profile $\mathcal{V} \in \mathcal{T}_{r,m,\alpha n}$ for some $0 \leqslant r \leqslant m-1$.*

Proof. If $\mathcal{C}$ is not (α, L)-strong average-agreement list-decodable, by Lemma 3.2 we know that there exists a positive integer $m \leqslant L$ and m distinct elements $a_1, \ldots, a_m \in \mathbb{F}_q^k$, along with a $t \geqslant \alpha n$ and a t-weakly partition connected hypergraph $\mathcal{H} = ([m], E)$ such that for all $i \in [n]$, $\{\mathsf{Enc}_i(a_j) \mid j \in e_i\}$ is constant, Now, observe that $\mathcal{H}$ must also be αn-weakly partition connected.

Without loss of generality, we can also assume that $a_1 = 0$ since the code is additive, and $a_2, \ldots, a_{r+1}$ are linearly independent, and $r = \dim \operatorname{span}(a_1, \ldots, a_m)$. Let $A = \operatorname{span}(a_1, \ldots, a_m)$, $W = \mathbb{F}_q^r$, and let $w_2, \ldots, w_{r+1}$ be its canonical basis.

Let $\varphi : \operatorname{span}(a_1, \ldots, a_m) \to \mathbb{F}_q^r$ be an isomorphism with $\varphi(a_i) = w_i$ for all $2 \leqslant i \leqslant r+1$.

Now, observe that $\mathcal{P}(\varphi(a_1, \ldots, a_m)) = \mathcal{P}(a_1, \ldots, a_m)$ and $\varphi(a_1, \ldots, a_m) \in S_{m,r}$. Let $\mathcal{H}' = \mathcal{H}_{\mathcal{P}(a_1,\ldots,a_m)}$.

To show $\mathcal{C}$ contains the local profile $(\mathcal{V}_{1,\mathcal{H}',\mathbf{w}}, \ldots, \mathcal{V}_{n,\mathcal{H}',\mathbf{w}})$, we use the dual map. Let $V = W^*$. The isomorphism $\varphi : A \to W$ induces an isomorphism $\varphi^* : V \to A^*$ defined by $(\varphi^* v)(x) = v(\varphi x)$ for $v \in V$ and $x \in A$.

Fix any $i \in [n]$. We would like to show that $(\varphi^* \mathcal{V}_{i,\mathcal{H}',\mathbf{w}})^\circ \subseteq \ker(\mathsf{Enc}_i)$. By definition, $\mathcal{V}_{i,\mathcal{H}',\mathbf{w}}$ is the annihilator of $\operatorname{span}\{w_{j_1} - w_{j_2} \mid j_1, j_2 \in e'_i\}$, which means $(\mathcal{V}_{i,\mathcal{H}',\mathbf{w}})^\circ = \operatorname{span}\{w_{j_1} - w_{j_2} \mid j_1, j_2 \in e'_i\}$. Since φ is an isomorphism between W and A, this means $(\varphi^* \mathcal{V}_{i,\mathcal{H}',\mathbf{w}})^\circ = \operatorname{span}\{a_{j_1} - a_{j_2} \mid j_1, j_2 \in e'_i\}$. Since the original codewords were constant on e_i, and $e'_i \subseteq e_i$, we know $\mathsf{Enc}_i(a_{j_1} - a_{j_2}) = 0$ for all $j_1, j_2 \in e'_i$. It follows that $(\varphi^* \mathcal{V}_{i,\mathcal{H}',\mathbf{w}})^\circ \subseteq \ker(\mathsf{Enc}_i)$. □

even simpler and more modular, and helps to capture some of the ideas that aid us in our list-decoding results for RLCs.

3.4 Alphabet size bounds for list-decoding of random linear codes

Before proceeding to the main bound, we present a simple reduction for ε-relaxed generalized singleton-bound demonstrating that the $L = (1-R)/\varepsilon$ is the critical regime for the ε-relaxed generalized-singleton bound.

Lemma 3.4. *Let $R, \varepsilon_0 \in (0,1)$. If a rate R code $\mathcal{C} \subseteq \Sigma^n$ is $(\varepsilon_0, L')-$GSB decodable for all $L' \leqslant \lfloor (1-R-\varepsilon_0)/\varepsilon_0 \rfloor$, then it is $(2\varepsilon_0, L)-$GSB decodable for all $L \in \mathbb{N}$.*

Proof. Fix any $y \in \Sigma^n$, and codewords $c_1, c_2, \cdots, c_{L+1} \in \mathcal{C}$ such that $\Delta(c_1, y) \leqslant \Delta(c_2, y) \leqslant \cdots \leqslant \Delta(c_{L+1}, y)$.

Note that, if $L \leqslant \lfloor (1-R-\varepsilon_0)/\varepsilon_0 \rfloor$, then

$$\sum_{i=1}^{L+1} \Delta(c_i, y) > L(1-R-\varepsilon_0) > L(1-R-2\varepsilon_0)$$

as desired.

Now, if $L > \lfloor (1-R-\varepsilon_0)/\varepsilon_0 \rfloor$, let $L' = \lfloor (1-R-\varepsilon_0)/\varepsilon_0 \rfloor$, now

$$\begin{aligned}
\sum_{i=1}^{L+1} \Delta(c_i, y) &\geqslant \sum_{i=1}^{L'+1} \Delta(c_i, y) + (L-L')\Delta(c_{L'+1}, y) \\
&> L'(1-R-2\varepsilon_0) + \left(\frac{L-L'}{L'+1}\right)\left(\sum_{i=1}^{L'+1} \Delta(c_i, y)\right) \\
&> L'(1-R-2\varepsilon_0) + \left(\frac{L-L'}{L'+1}\right) L(1-R-\varepsilon_0) \\
&= L'(1-R-2\varepsilon_0) + (L-L')\left(1 - \frac{1}{L'+1}\right)(1-R-\varepsilon_0) \\
&= L'(1-R-2\varepsilon_0) + (L-L')\left(1-R-\varepsilon_0 - \frac{1-R-\varepsilon_0}{L'+1}\right) \\
&> L'(1-R-2\varepsilon_0) + (L-L')(1-R-2\varepsilon_0) \\
&= L(1-R-2\varepsilon_0)
\end{aligned}$$

□

We are now ready to prove our alphabet size bounds. The proof here proceeds by counting the number of local profiles defined in Definition 20, and then instantiating Theorem 2.7 for each of these profiles to union bound the probability that our random code contains one of the local profiles.

What enables our improvement here over previous works is the better counting we do of number of local profiles via our restriction to induced hypergraphs from partitions (Definition 18) instead of counting all possible hypergraphs (See Claim 3.8), and using the rank of the spaces we are working over when counting and applying Theorem 2.7 (See the summation based on r in the below statement.).

Theorem 3.5. *Let s, n, L be natural numbers and $R, \varepsilon \in (0,1)$ be real numbers such that Rsn and $(R+\varepsilon)n$ are positive integers. Let $\mathbb{F}_q$ be a finite field whose size q satisfies $q^s > 2(L+1)/(1-R-\varepsilon)$. Denote $k = Rsn$. Let $\mathsf{Enc}_1, \ldots, \mathsf{Enc}_n : \mathbb{F}_q^k \to \mathbb{F}_q^s$ be uniformly random linear maps and $\mathcal{C} = \{(\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x)) \mid x \in \mathbb{F}_q^k\}$ be the associated $\mathbb{F}_q$-additive code. Then,*

$$\Pr\left[\mathcal{C} \text{ is not } (\varepsilon, L')-\text{GSB decodable for all } L' \leqslant L.\right]$$
$$\leqslant \sum_{r=1}^{L} 4 \cdot q^{r(L-r+1)} \cdot \left(32 \cdot \min(L+1, q) \cdot q^{-\varepsilon s}\right)^{rn} \quad (2)$$

Proof. We know that if $\mathcal{C}$ is not $(\varepsilon, L')-$GSB decodable for all $L' \leqslant L$, then by Theorem 3.1 $\mathcal{C}$ is not $(\alpha, L+1)$-strong average-agreement list-decodable for $\alpha = R + \varepsilon$. Thus, by Claim 3.3, there exist $0 \leqslant r \leqslant m-1 \leqslant L$ and a local profile $\mathcal{V} \in \mathcal{T}_{r,m,\alpha n}$ such that $\mathcal{C}$ contains the local profile $\mathcal{V}$.

Define $t = \alpha n$. For $t' \geqslant t$, let us define a set of local profiles as follows:

$$\mathcal{T}_{r,m,t',t} = \Big\{(\mathcal{V}_{1,\mathcal{H}',\mathbf{w}}, \ldots, \mathcal{V}_{n,\mathcal{H}',\mathbf{w}}) \mid \mathbf{w} \in S_{m,r}, \mathcal{H}' \in \{\mathcal{H}_{\mathcal{P}(\mathbf{w})} \mid \mathcal{H} = ([m], E) \text{ is } t\text{-WPC and } \sum_{e \in E} \max(|\{j \mid e \cap P_j \neq \emptyset\}| - 1, 0) = t'r\}\Big\}$$

Claim 3.6. *For each $\mathcal{V} \in \mathcal{T}_{r,m,t',t}$, we have $\Phi_{(\mathbb{F}_q^r)^*}((\mathbb{F}_q^r)^*, \mathcal{V}, t'/n) = 0$.*

Proof. Let $\mathcal{V} = (\mathcal{V}_{1,\mathcal{H}',\mathbf{w}}, \ldots, \mathcal{V}_{n,\mathcal{H}',\mathbf{w}})$ for some $\mathbf{w} \in S_{m,r}$ and $\mathcal{H}' = \mathcal{H}_{\mathcal{P}(\mathbf{w})} = ([m], E')$ for a t-WPC hypergraph $\mathcal{H} = ([m], E)$. We have

$$\begin{aligned}
\Phi_{(\mathbb{F}_q^r)^*}((\mathbb{F}_q^r)^*, \mathcal{V}, t'/n) &= \frac{t'r}{n} - \frac{\sum_{i=1}^{n} \dim(\mathcal{V}_{i,\mathcal{H}',\mathbf{w}}^{\perp})}{n} \\
&= \frac{t'r}{n} - \frac{\sum_{e' \in E'} \max(|\{j \mid e' \cap P_j \neq \emptyset\}| - 1, 0)}{n} \quad (3) \\
&= 0, \quad (4)
\end{aligned}$$

where (3) follows because $\dim(\mathcal{V}_{i,\mathcal{H}',\mathbf{w}}^{\perp}) = \dim \operatorname{span}(w_{j_1} - w_{j_2})_{j_1, j_2 \in e_i'}$ and because of the definition of e_i', each vector in the edge is from a different part and the parts are defined so that vectors from distinct parts are linearly independent (See Definition 17). The equality (4) follows from the definition of t'. □

We are now ready to apply Theorem 2.7 and a union bound.

Claim 3.7.

$$\sum_{\mathcal{V} \in \mathcal{T}_{r,m,\alpha n,t'}} \Pr[\mathcal{C} \text{ contains } \mathcal{V}] \leqslant |\mathcal{T}_{r,m,\alpha n,t'}| \cdot q^{rs(Rn-t')}$$

Proof. For each $\mathcal{V} \in \mathcal{T}_{r,m,\alpha n,t'}$, using Theorem 2.7 and Claim 3.6 we have

$$\Pr[\mathcal{C} \text{ contains } \mathcal{V}] \leqslant q^{sn \cdot \Phi_{(\mathbb{F}_q^r)^*}((\mathbb{F}_q^r)^*, \mathcal{V}, R)} = q^{rs(Rn-t')} \ .$$ □

Thus, we now just need a bound on $|\mathcal{T}_{r,m,\alpha n,t'}|$.

Claim 3.8. *For any $t' \geqslant \alpha n$,*

$$|\mathcal{T}_{r,m,t',\alpha n}| \leqslant \binom{n}{\alpha n}^{r+1} \cdot \binom{nm}{n - \alpha n} \cdot \left(\frac{m}{1-\alpha}\right)^{(t'-\alpha n)r} \cdot q^{(m-r-1)r} \ .$$

Proof. We begin by fixing $\mathbf{w} = (w_1, \ldots, w_m) \in S_{m,r}$. There are at most $q^{(m-1-r)r}$ such choices in $S_{m,r}$. Now, this fixes $\mathcal{P}(w_1, \ldots, w_m) = \mathcal{P}_0 \sqcup \mathcal{P}_1 \cdots \sqcup \mathcal{P}_r$.

Since $\mathcal{H}' = \mathcal{H}_{\mathcal{P}(w_1,\ldots,w_m)}$ for some t-WPC hypergraph $\mathcal{H}$, by Lemma 2.1 we have $|\{i \in [n] \mid j \in e_i\}| \geqslant \alpha n$ for each $j \in [r+1]$. Let us thus count the number of hypergraphs $\mathcal{H}' = ([m], E')$ for which $\sum_{e' \in E'} \max(|\{j \mid e' \cap \mathcal{P}_j \neq \emptyset\}| - 1, 0) = t'r$, each edge intersects each part at most once, and $|\{i \in [n] \mid j \in e'_i\}| \geqslant \alpha n$ for each $j \in [r+1]$.

Thus, we first choose, for each $j \in [r+1]$, αn distinct values of $i \in [n]$ for which $j \in [r+1]$ belongs to e'_i. There are $\binom{n}{\alpha n}^{r+1}$ such choices.

Since $\sum_{e' \in E} \max(|\{j \mid e' \cap \mathcal{P}_j \neq \emptyset\}| - 1, 0) = t'r$, we have at most $t'r + n - \alpha n(r+1) = n - \alpha n + r(t' - \alpha n)$ incidences to choose between $j \in [m]$ and edges $e'_i \in [n]$. There are at most $\binom{nm}{n-\alpha n+r(t'-\alpha n)}$ such choices for these incidences.

Finally, we can bound $\binom{nm}{n-\alpha n+r(t'-\alpha n)} \leqslant \binom{nm}{(1-\alpha)n} \cdot \left(\frac{m}{1-\alpha}\right)^{(t'-\alpha n)r}$ by properties of the binomial coefficient. Here we bound the binomial coefficient $\binom{a}{b+c} = \binom{a}{b} \cdot \prod_{i=1}^{c} \left(\frac{a+1-b-i}{b+i}\right) \leqslant \binom{a}{b} \cdot \left(\frac{a}{b}\right)^c$ with $a = nm, b = (1-\alpha)n, c = r(t' - \alpha n)$. □

Remark 2. We note that our use of WPC hypergraphs and restricting to partition induced sub-hypergraphs enables the above significantly better bound on the number of relevant local profiles in comparison to counting over all list-decoding configurations in a way independent of the rank of the space.

Claim 3.9. *The following bound holds:*

$$\sum_{\mathcal{V} \in \mathcal{T}_{r,m,\alpha n}} \Pr[\mathcal{C} \textit{ contains } \mathcal{V}] \leqslant 2m \cdot q^{r(m-r-1)} \left(16 \cdot \left(\frac{m}{(1-\alpha)}\right)^{1/r} \cdot q^{-\varepsilon s}\right)^{rn}.$$

Proof. We have

$$\begin{aligned}
\sum_{\mathcal{V} \in \mathcal{T}_{r,m,\alpha n}} \Pr[\mathcal{C} \text{ contains } \mathcal{V}] &\leqslant \Big(\sum_{t' \geqslant \alpha n} \left(\frac{m}{1-\alpha} \cdot q^{-s}\right)^{r(t'-\alpha n)}\Big) \cdot \\
&\qquad \cdot \left(\binom{n}{\alpha n}^{r+1} \cdot \binom{nm}{n(1-\alpha)} \cdot q^{-\varepsilon n \cdot rs} \cdot q^{(m-r-1)r}\right) \\
&\leqslant \Big(\sum_{t' \geqslant \alpha n} (1/2)^{t'-\alpha n}\Big) \left(\binom{n}{\alpha n}^{r+1} \cdot \binom{nm}{n(1-\alpha)} \cdot q^{-\varepsilon n \cdot rs} \cdot q^{(m-r-1)r}\right) \\
&\leqslant \frac{1}{1-2^{-1/m}} \left(\binom{n}{\alpha n}^{r+1} \cdot \binom{nm}{n(1-\alpha)} \cdot q^{-\varepsilon n \cdot rs} \cdot q^{(m-r-1)r}\right) \\
&\leqslant 2m \cdot q^{r(m-r-1)} \left(4 \cdot \left(\frac{4m}{(1-\alpha)}\right)^{(1-\alpha)/r} \cdot q^{-\varepsilon s}\right)^{rn} \\
&\leqslant 2m \cdot q^{r(m-r-1)} \left(16 \cdot \left(\frac{m}{(1-\alpha)^{1-\alpha}}\right)^{1/r} \cdot q^{-\varepsilon s}\right)^{rn}. \\
&\leqslant 2m \cdot q^{r(m-r-1)} \left(32 \cdot m^{1/r} \cdot q^{-\varepsilon s}\right)^{rn}
\end{aligned}$$

Above, the second step uses the lower bound hypothesis on q^s, and the third step uses the fact that $t'm$ is always an integer, and we have a geometric sequence. In the next step, we used the fact that

$2^{1/m} \geqslant 1 + 1/2m$ along with the upper bound $\binom{a}{b} \leqslant \frac{a^b}{b!} \leqslant \frac{a^b}{(b/4)^b} \leqslant (4a/b)^b$. Finally, we used the fact that $x^x > 1/2$ for all $x \in (0,1)$. □

We are now ready to complete the proof of Theorem 3.5. To do so, we sum the bound of Claim 3.9 over the choices of m. Observe that $m \leqslant L+1$ but also $m \leqslant q^r$. Thus, the total sum is at most

$$\sum_{r=1}^{L} \sum_{m=r+1}^{\min(L+1,q^r)} \sum_{\mathcal{V} \in \mathcal{T}_{r,m,\alpha n}} \Pr[\mathcal{C} \text{ contains } \mathcal{V}] \leqslant \sum_{r=1}^{L} 4q^r \cdot q^{r(L-r)} \cdot \left(32 \cdot \min((L+1)^{1/r}, q) \cdot q^{-\varepsilon s}\right)^{rn}.$$

$$\leqslant \sum_{r=1}^{L} 4q^{r(L-r+1)} \cdot (32 \min(L+1, q) \cdot q^{-\varepsilon s})^{rn} \,. \qquad \square$$

We are now ready to state our main results concerning list-decodability of random linear codes, by instantiating the previous theorem in two ways utilizing the choice of $\min((L+1)^{1/r}, q)$.

Theorem 3.10. *Let s, n, L be natural numbers and $R, \varepsilon \in (0,1)$ be real numbers satisfying $ns > L/\varepsilon$ such that Rsn and $(R+\varepsilon)n$ are positive integers. Let $\mathbb{F}_q$ be a finite field and denote $k = Rsn$ such that $q^s > 2(L+1)/(1-R-\varepsilon)$. Let $\mathsf{Enc}_1, \ldots, \mathsf{Enc}_n : \mathbb{F}_q^k \to \mathbb{F}_q^s$ be uniformly random linear maps and $\mathcal{C} = \{(\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x)) \mid x \in \mathbb{F}_q^k\}$ be the associated $\mathbb{F}_q$-additive code. Then, if either:*

- *$q^s \geqslant (32 \cdot (L+1))^{2/\varepsilon}$; or*
- *$s \geqslant 12/\varepsilon$,*

then the following holds:

$$\Pr\left[\mathcal{C} \text{ is not } (\varepsilon, L')\text{−GSB decodable for all } L' \leqslant L.\right] \leqslant 8 \cdot q^{-\varepsilon s n/4}$$

Proof. Denoting $p = \Pr[\mathcal{C}$ is not (ε, L')−GSB decodable for all $L' \leqslant L.]$, we have, by Theorem 3.5,

$$\begin{aligned} p &\leqslant 4 \sum_{r=1}^{L} q^{r(L-r+1)} \cdot \left(32 \cdot \min(L+1, q) \cdot q^{-\varepsilon s}\right)^{rn} \\ &\leqslant 4 \cdot \sum_{r=1}^{L} \left(q^{L-r+1-\varepsilon s n/2}\right)^r \\ &\leqslant 8 \cdot q^{-\varepsilon s n/4} \,. \end{aligned}$$

For going from the first equation to the second, we used the fact that in case of the first hypothesis, we have that $32(L+1) \leqslant q^{\varepsilon s/2}$. In the second case, we used the fact that $32q = q^{1+\log_q 32} \leqslant q^6 \leqslant q^{\varepsilon s/2}$.

Going from the second equation to the third, we used the fact that $q^{L-r+1-\varepsilon s n/2} \leqslant q^{-\varepsilon s n/4} \leqslant 1/2$ since $\varepsilon s n/4 > L \geqslant 1$. Thus, Theorem 3.10 follows. □

Corollary 3.11. *Let $R, \varepsilon \in (0,1)$ and n, L be positive integers such that Rn and εn are positive integers and $n > 4L/\varepsilon$. Then, for any finite field $\mathbb{F}_q$ with $q \geqslant \max((32 \cdot (L+1))^{2/\varepsilon}, 2(L+1)/(1-R-\varepsilon))$, a random linear code $\mathcal{C}$ of rate R and block length n is (ε, L')−GSB decodable for all $L' \leqslant L$ with high probability $1 - 8q^{-\varepsilon s n/4}$.*

Additionally, setting $L' = \lfloor (1 - R - \varepsilon/2)/(\varepsilon/2) \rfloor$, *we get that as long as* $n > 8/\varepsilon^2$, *then for any finite field with* $q > (64 \cdot (1-R)/\varepsilon)^{4/\varepsilon}$, *a random linear code of rate* R *and block length* n *is* $(\varepsilon, L)-$*GSB decodable for all* $L \in \mathbb{N}$ *with probability at least* $1 - 8q^{-\varepsilon s n/4}$.

Proof. The first part follows by setting $s = 1$ in Theorem 3.10. The second part of the corollary is simply a consequence of Lemma 3.4. □

Corollary 3.12. *Let* $R, \varepsilon \in (1/2n, 1)$ *such that* $R + \varepsilon \leqslant 1$, *let* $\mathbb{F}_q$ *be a finite field, and* n, s *be positive integers such that* Rsn *and* $(R+\varepsilon/2)n$ *are positive integers and* $s \geqslant 32/\varepsilon$. *Then, a random* $\mathbb{F}_q$*-additive code* $\mathcal{C}$ *of rate* R, *block length* n, *and* $\Sigma = \mathbb{F}_q^s$ *is* $(\varepsilon, L)-$*GSB decodable for all positive integers* L *with probability at least* $\geqslant 1 - 8 \cdot q^{-4n}$.

Proof. Let $\varepsilon_0 = \varepsilon/2$ and $L' = \lfloor (1 - R - \varepsilon_0)/\varepsilon_0 \rfloor \geqslant \lfloor (\varepsilon - \varepsilon_0)/\varepsilon_0 \rfloor \geqslant 1$.

To appeal to Theorem 3.10 with parameters L', ε_0, it is sufficient to have $sn > 4L'/\varepsilon_0$ i.e. to have that $n > L'/4$ i.e. but $4n > 2/\varepsilon \geqslant 1/\varepsilon_0 \geqslant L$, along with $q^s \geqslant 2(L+1)/(1-R-\varepsilon_0)$ but $q^s \geqslant 2^{32/\varepsilon} \geqslant 32/\varepsilon_0 \geqslant 32L/(1-R-\varepsilon_0) \geqslant 2(L+1)/(1-R-\varepsilon_0)$. Thus, by Theorem 3.10, we have that

$$\Pr\left[\mathcal{C} \text{ is not } (\varepsilon_0, L'')-\text{GSB decodable for all } L'' \leqslant L'.\right] \leqslant 8 \cdot q^{-\varepsilon_0 sn/4}$$

Now, note that by Lemma 3.4, we have that if $\mathcal{C}$ is $(\varepsilon_0, L')-$GSB decodable for all $L'' \leqslant L'$ then, it is (ε, L)-GSB decodable for all $L \in \mathbb{N}$.

Thus,

$$\Pr\left[\mathcal{C} \text{ is not } (\varepsilon, L)-\text{GSB decodable for all } L \in \mathbb{N}.\right] \leqslant 8 \cdot q^{-\varepsilon_0 sn/4} \leqslant 8 \cdot q^{-4n} \ .$$ □

Remark 3. Note that the second corollary works for any finite field $\mathbb{F}_q$ (including $q = 2$).

4 List-recovery

We begin by coming up with local profiles that capture (ρ, ℓ, L) list-recovery in the style of [LMS25].

Lemma 4.1. *Suppose the additive code* $\mathcal{C} = \{(\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x)) \mid x \in \mathbb{F}_q^k\}$ *is* not (ρ, ℓ, L) *list-recoverable. Then, there exist linear spaces* V *and* A *with* $\dim V \leqslant L$, *an isomorphism* $\varphi : V \to A^*$, *and a subset* $S \subseteq A$ *of size* $L+1$ *with the following guarantee. For each* $i \in [n]$, *there exist partitioned subsets* $S_i = S_{i,1} \sqcup \cdots \sqcup S_{i,\ell} \subseteq S$ *satisfying*

$$\frac{1}{n} \sum_{i=1}^{n} |S_i| \geqslant (1-\rho)(L+1) \ ,$$

such that $\mathcal{C}$ *contains the* V*-local profile* $\mathcal{V} = (\mathcal{V}_1, \ldots, \mathcal{V}_n)$ *given by*

$$\mathcal{V}_i = \{v \in V \mid \varphi(v)(s_1 - s_2) = 0 \text{ for all } j \in [\ell] \text{ and } s_1, s_2 \in S_{i,j}\} \ .$$

Proof. If $\mathcal{C}$ is not (ρ, ℓ, L) list-recoverable, there exist sets $T_1, \ldots, T_n \subseteq \mathbb{F}_q^s$ with $|T_i| \leqslant \ell$, and distinct messages $a_1, \ldots, a_{L+1} \in \mathbb{F}_q^k$ such that:

$$\sum_{j=1}^{L+1} \frac{|\{i \in [n] \mid \mathsf{Enc}_i(a_j) \in T_i\}|}{n} \geqslant (1-\rho)(L+1).$$

Let $A = \text{span}(0, a_2 - a_1, \ldots, a_L - a_1)$. Let $S = \{0, a_2 - a_1, \ldots, a_{L+1} - a_1\}$ and $S_i = \{a_j - a_1 \mid \mathsf{Enc}_i(a_j) \in T_i\}$. Since $|T_i| \leqslant \ell$, we can index the elements of each set as $T_i = \{y_{i,1}, \ldots, y_{i,\ell}\}$ (allowing for empty partition pieces if $|T_i| < \ell$).

We partition each S_i based on which element of T_i the original message maps to: let $S_{i,m} = \{a_j - a_1 \mid \mathsf{Enc}_i(a_j) = y_{i,m}\}$.

Let $V = A^*$, φ be the identity isomorphism, and let $\mathcal{V}_i = \{a^* \in A^* \mid a^*(s_1 - s_2) = 0 \ \ \forall m \in [\ell], s_1, s_2 \in S_{i,m}\}$. To see that $\mathcal{C}$ contains $(\mathcal{V}_1, \ldots, \mathcal{V}_n)$, observe that if $s_1, s_2 \in S_{i,m}$, then $s_1 = a_{j_1} - a_1$ and $s_2 = a_{j_2} - a_1$ for some j_1, j_2 where $\mathsf{Enc}_i(a_{j_1}) = \mathsf{Enc}_i(a_{j_2}) = y_{i,m}$. By linearity, $\mathsf{Enc}_i(s_1 - s_2) = \mathsf{Enc}_i(a_{j_1} - a_{j_2}) = 0$. This implies that the annihilator of $\mathcal{V}_i$ in A is spanned by vectors entirely contained within $\ker(\mathsf{Enc}_i)$, thereby satisfying the containment definition. Finally, we have

$$\sum_{i=1}^{n} \frac{|S_i|}{n} = \sum_{j=1}^{L+1} \sum_{i=1}^{n} \frac{\mathbf{1}(\mathsf{Enc}_i(a_j) \in T_i)}{n} \geqslant (1-\rho)(L+1)$$

as desired. □

Now, to show that a code $\mathcal{C}$ is (ρ, ℓ, L) list-recoverable, it suffices to show that it does not contain any of the local profiles detailed above.

Let V be a vector space and $\mathcal{V} = (\mathcal{V}_1, \cdots, \mathcal{V}_n)$ be a V-local profile as in Lemma 4.1, then to show that a rate R random linear or additive code does not include this profile with high probability, it is necessary and sufficient to have a $W \subsetneq V$ such that $\Phi_V(W, (\mathcal{V}_1, \cdots, \mathcal{V}_n), R) > \Phi_V(V, (\mathcal{V}_1, \cdots, \mathcal{V}_n), R)$.

Such a W can only be guaranteed to exist when L, i.e. the target list size, is larger than the best possible list-recovery list size for random linear codes. More formally, we can make the following definition:

Definition 21. Let $\alpha, \varepsilon \in (0,1)$ such that $\alpha + \varepsilon \leqslant 1$, and let ℓ be a positive integer. We define $L_{\ell,\alpha,\varepsilon}$ to be the minimal integer L satisfying the following property:

For any positive integer n, linear spaces V and A, isomorphism $\varphi : V \to A^*$, and subset $S \subseteq A$ with $|S| > L$, suppose we are given subsets $S_1, \ldots, S_n \subseteq S$ satisfying

$$\frac{1}{n} \sum_{i=1}^{n} |S_i| > |S|(\alpha + \varepsilon) \ .$$

Then, for any choice of partitions $S_i = S_{i,1} \sqcup \cdots \sqcup S_{i,\ell}$ for each $i \in [n]$, if we define the V-local profile $\mathcal{V} = (\mathcal{V}_1, \ldots, \mathcal{V}_n)$ by

$$\mathcal{V}_i = \{v \in V \mid \varphi(v)(s_1 - s_2) = 0 \text{ for all } j \in [\ell] \text{ and } s_1, s_2 \in S_{i,j}\} \ ,$$

there exists a subspace $W \subsetneq V$ such that

$$\Phi_V(W, (\mathcal{V}_1, \ldots, \mathcal{V}_n), \alpha) > \Phi_V(V, (\mathcal{V}_1, \ldots, \mathcal{V}_n), \alpha) \ .$$

Remark 4. We note that, by appealing to [LMS25]'s threshhold theorem results, one can also conclude that $L_{\ell,R,\varepsilon}$ must also be the optimal list size bound for average-radius list-recovery of rate R random linear codes over arbitrarily large alphabet sizes. Since, this is not relevant for the body of our paper, we do not expand on this connection. [CZ25, LMS25, LW18, Che26]'s lower bounds on list-recovery of linear and additive do show that $L_{\ell,\alpha,\varepsilon}$ must be exponential in ℓ.

We now turn to bounding $L_{\ell,\alpha,\varepsilon}$ from above using the discrete entropic Brascamp-Lieb inequality.

4.1 List size bounds for list recovery and the Brascamp-Lieb inequality

The following usage of the discrete entropic Brascamp-Lieb inequality for understanding list-size bounds is due to [BCDZ25a]. Our presentation of the bound is inspired by their usage and [GG25b]'s presentation.

Theorem 4.2. *Let $\alpha, \varepsilon \in (0,1)$ be constants such that $\alpha + \varepsilon \leqslant 1$, and let ℓ be a positive integer. Then,*

$$L_{\ell,\alpha,\varepsilon} \leqslant (\ell/(\alpha+\varepsilon))^{(\alpha+\varepsilon)/\varepsilon}$$

Proof. Let V, A be linear spaces, n be a positive integer, $\varphi : V \to A^*$ be an isomorphism, $S \subseteq A$ be a set, $S_i = S_{i,1} \sqcup \cdots \sqcup S_{i,\ell}$ be subsets of S with

$$\frac{1}{n}\sum_{i=1}^{n} |S_i| > |S|(\alpha+\varepsilon) \ .$$

Let $(\mathcal{V}_1, \cdots, \mathcal{V}_n)$ be the V-local profile where

$$\mathcal{V}_i = \{v \in V \mid \varphi(v)(s_1 - s_2) = 0 \text{ for all } j \in [\ell] \text{ and } s_1, s_2 \in S_{i,j}\} \ ,$$

and such that for all $W \subseteq V$,

$$\Phi_V(W, (\mathcal{V}_1, \ldots, \mathcal{V}_n), \alpha) \leqslant \Phi_V(V, (\mathcal{V}_1, \ldots, \mathcal{V}_n), \alpha) \ ,$$

or in other words

$$\dim V - \dim W \leqslant \frac{\sum_{i=1}^{n} [\dim \mathcal{V}_i - \dim(W \cap \mathcal{V}_i)]}{(1-\alpha)n} \ .$$

Let $L = |S|$, and for $i \in [n]$, let $\rho_i = \frac{|S_i|}{|S|}$. Thus, by the discrete entropic Brascamp-Lieb inequality (Theorem 2.4), applied with the choice $E = \varphi V$, $E_i = \varphi \mathcal{V}_i$ and $F = \varphi W$, we can conclude that if Z is the uniform distribution over S, then

$$H(Z) \leqslant \sum_{i=1}^{n} \frac{H(\varphi \mathcal{V}_i(Z))}{(1-R)n}.$$

Now, $H(Z) = \log L$, and, let Y_i be the indicator variable for whether $Z \in S_i$.

$$\begin{aligned}
H(\varphi \mathcal{V}_i(Z)) &\leqslant H(\varphi \mathcal{V}_i(Z), Y_i) \\
&= H(Y_i) + H(\varphi \mathcal{V}_i(Z) \mid Y_i) \\
&\leqslant h(\rho_i) + \rho_i H(\varphi \mathcal{V}_i(Z) \mid Z \in S_i) + (1-\rho_i) H(\varphi \mathcal{V}_i(Z) \mid Z \notin S_i) \\
&\leqslant h(\rho_i) + \rho_i \log \ell + (1-\rho_i)(\log L(1-\rho_i)) \\
&= -\rho_i \log \rho_i + \rho_i \log \ell + (1-\rho_i) \log L
\end{aligned}$$

Let $\rho = \frac{\sum_{i=1}^{n} \rho_i}{n}$. By assumption, we have that $\rho \geqslant \alpha + \varepsilon$. Thus,

$$\log L \leqslant \frac{\sum_{i=1}^{n} -\rho_i \log \rho_i + \rho_i \log \ell + (1-\rho_i) \log L}{(1-\alpha)n}$$

$$\leqslant \frac{-\rho\log\rho + \rho\log\ell + (1-\rho)\log L}{(1-\alpha)},$$

where the second inequality follows from Jensen's inequality applied to the concave function $x \mapsto -x\log x$. Thus,

$$\begin{aligned}(1-\alpha)\log L &\leqslant (1-\rho)\log L + \rho\log(\ell/\rho)\\ &\leqslant (1-\rho)\log L + \rho\log(\ell/(\alpha+\varepsilon))\\ &= (1-\alpha-\varepsilon)\log L + (\alpha+\varepsilon)\log(\ell/(\alpha+\varepsilon)) + (\alpha+\varepsilon-\rho)\log(L(\alpha+\varepsilon)/\ell)\\ &\leqslant (1-\alpha-\varepsilon)\log L + (\alpha+\varepsilon)\log(\ell/(\alpha+\varepsilon)),\end{aligned}$$

where we used the fact that $\rho \geqslant \alpha+\varepsilon$ and $L > \ell/(\alpha+\varepsilon)$.

Finally, we get by reorganizing

$$\varepsilon\log L \leqslant (\alpha+\varepsilon)\log(\ell/(\alpha+\varepsilon))\ .$$

But then $|S| = L \leqslant \left(\frac{\ell}{\alpha+\varepsilon}\right)^{(\alpha+\varepsilon)/\varepsilon}$ as desired. □

4.2 Local profiles from bad list-recovery configurations

In the list-decoding section, we defined local profiles from list-decoding configurations after restricting to weakly partitioned hypergraphs. We will likewise define here a family of local profiles that correspond to bad list-recovery configurations, in a manner that can yields us improved results.

Note that we have shown in the previous subsection that if a code $\mathcal{C}$ is not $(1-\alpha-\varepsilon, \ell, L_{\ell,\alpha,\varepsilon})$ decodable then there exists a linear space V, a V-local profile $\mathcal{V} = (\mathcal{V}_1, \cdots, \mathcal{V}_n)$ as described in Lemma 4.1 and Definition 21 and a vector space $W \subsetneq V$ such that $\Phi_V(W, (\mathcal{V}_1, \ldots, \mathcal{V}_n), \alpha) > \Phi_V(V, (\mathcal{V}_1, \ldots, \mathcal{V}_n), \alpha)$.

Then, $\mathcal{C}$ must also contain the V/W-local profile $((\mathcal{V}_1+W)/W, \cdots, (\mathcal{V}_1+W)/W)$ by Lemma 2.6 but also $\Phi_{V/W}(V/W, ((\mathcal{V}_1+W)/W, \cdots, (\mathcal{V}_1+W)/W), \alpha) < 0$ by Theorem 2.5.

We can thus restrict our focus only to the profiles that we obtain post quotienting by W. Note that to talk about the joint kernel of $(V_i+W)/W$ $(\mathcal{V}_i+W)/W$, we need a canonical map $M_{r,L} : (\mathbb{F}_q^L)^* \to (\mathbb{F}_q^r)^*$ where r is the rank of V/W.

Definition 22. For $r \leqslant L$, define $M_{r,L} : (\mathbb{F}_q^L)^* \to (\mathbb{F}_q^r)^*$, by just restricting the functionals on $\mathbb{F}_q^L$ to $\mathbb{F}_q^r$.[6]

Now, we are ready to describe the kinds of profiles that arrive after quotienting.

Definition 23 (Local profiles from list-recovery configurations)**.** For any natural ℓ, reals $\alpha, \varepsilon \in (0,1)$, let $L = L_{\ell,\alpha,\varepsilon}$, and for any $r \leqslant L$, define

$$\begin{aligned}\mathcal{W}_{\ell,\alpha,\varepsilon,r} = \{(\mathcal{W}_1, \ldots, \mathcal{W}_n) \in \mathcal{L}(\mathbb{F}_q^{r*})^n \mid &\exists S \in \binom{\mathbb{F}_q^L}{\leqslant L+1}, \forall i \in [n], \exists S_i \subseteq S, S_i = S_{i,1} \sqcup \cdots \sqcup S_{i,\ell} \text{ s.t.}\\ &\mathcal{V}_i = \{v \in (\mathbb{F}_q^L)^* \mid v(s_1 - s_2) = 0 \forall j \in [\ell], s_1, s_2 \in S_{i,j}\},\\ &\mathcal{W}_i = M_{r,L}\mathcal{V}_i,\\ &\Phi_{(\mathbb{F}_q^r)^*}(U, (\mathcal{W}_1, \ldots, \mathcal{W}_n), \alpha) < 0 \ \ \forall\, U \subseteq (\mathbb{F}_q^r)^* \setminus \{\{0\}\}\}.\end{aligned}$$

[6]Here we assume that there's a canonical embedding of $\mathbb{F}_q^r$ in $\mathbb{F}_q^L$.

We now need to show that if $\mathcal{C}$ is not $(1-\alpha-\varepsilon, \ell, L)$ list-recoverable, then it must contain one of the above described profiles.

Lemma 4.3. *For any natural ℓ, reals $\alpha, \varepsilon \in (0,1)$, let $L = L_{\ell,\alpha,\varepsilon}$. If $\mathcal{C} = \{\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x) \mid x \in \mathbb{F}_q^k\}$ is not $(1-\alpha-\varepsilon, \ell, L)$ list recoverable, then there exists an $r \leqslant L$ and $\mathcal{W} = (\mathcal{W}_1, \ldots, \mathcal{W}_n) \in \mathcal{W}_{\ell,\alpha,\varepsilon,r}$ such that $\mathcal{C}$ contains $\mathcal{W}$.*

Proof. If $\mathcal{C} = \{\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x) \mid x \in \mathbb{F}_q^k\}$ is not $(1-\alpha-\varepsilon, \ell, L)$ list recoverable, then by Lemma 4.1, there exists a linear space V such that $\mathcal{C}$ contains the V-local profile $(\mathcal{V}_1, \ldots, \mathcal{V}_n) \in \mathcal{L}(V)^n$ where there exists a set $S \subseteq V^*$ with $|S| = L+1$, and for all $i \in [n]$, there exist partitioned subsets $S_i = S_{i,1} \sqcup \cdots \sqcup S_{i,\ell} \subseteq S$, such that $\mathcal{V}_i = \{v \in V \mid v(s_1 - s_2) = 0 \ \forall j \in [\ell], s_1, s_2 \in S_{i,j}\}$, and $\frac{\sum |S_i|}{n} > (\alpha+\varepsilon)(L+1)$ along with $\dim V \leqslant L$.

Let W be the maximal element of $\arg\max \Phi_V(*, (\mathcal{V}_1, \ldots, \mathcal{V}_n), \alpha)$. By Theorem 4.2 (since $|S| = L+1 > L_{\ell,\alpha,\varepsilon}$), $W \neq V$.

Now, by Lemma 2.6, we know that $\mathcal{C}$ also contains the V/W-local profile $\big((\mathcal{V}_1+W)/W, \ldots, (\mathcal{V}_n+W)/W\big)$. Additionally, for all U such that $U+W \neq W$, we have that:

$$\begin{aligned}\Phi_{V/W}\left((U+W)/W, (\mathcal{V}_1+W)/W, \ldots, (\mathcal{V}_n+W)/W), \alpha\right) \\ &= \Phi_V(U+W, (\mathcal{V}_1, \ldots, \mathcal{V}_n), \alpha) - \Phi_V(W, (\mathcal{V}_1, \ldots, \mathcal{V}_n), \alpha) \\ &< 0\end{aligned}$$

The inequality is by the assumption on W (being the maximal element) and the equality is by Theorem 2.5.

Let $r = \dim V/W$. Note that since $\dim W^\circ = \dim V/W$, we must have that $\dim W^\circ = r$. Thus, we can take an injective homomorphism $\varphi_1 : V^* \to \mathbb{F}_q^L$ such that $\varphi_1(W^\circ)$ is the canonical embedding of $\mathbb{F}_q^r$ in $\mathbb{F}_q^L$. Let $\varphi_1^* : (\mathbb{F}_q^L)^* \to V$ be the dual map of φ_1. Because φ_1 is injective, φ_1^* is surjective. We recall that the dual map is defined as follows: for any $\hat{v} \in (\mathbb{F}_q^L)^*$ and $s_1 \in V^*$, we have that $\varphi_1^*(\hat{v})(s_1) = \hat{v}(\varphi_1(s_1))$. Let $(\varphi^*)^{-1} : V \mapsto (\mathbb{F}_q^L)^*$ be any linear inverse map.

We now construct the explicit sets required by the definition of $\mathcal{W}_{\ell,\alpha,\varepsilon,r}$. We map the agreement set to the explicit field via the injection: let $S' = \varphi_1(S) \subseteq \mathbb{F}_q^L$. Since φ_1 is injective and $|S| = L+1$, we have $|S'| = L+1$. For each $i \in [n]$ and $j \in [\ell]$, we map the partitions naturally as $S'_{i,j} = \varphi_1(S_{i,j})$.

Next, we lift the local profiles into $(\mathbb{F}_q^L)^*$. Let $\widehat{\mathcal{V}}_i = (\varphi_1^*)^{-1}(\mathcal{V}_i) \subseteq (\mathbb{F}_q^L)^*$. To verify the functional evaluation condition, consider any $\widehat{v} \in \widehat{\mathcal{V}}_i$ and any $s'_1, s'_2 \in S'_{i,j}$ (where $s'_k = \varphi_1(s_k)$ for $s_k \in S_{i,j}$). We have:

$$\widehat{v}(s'_1 - s'_2) = \widehat{v}(\varphi_1(s_1 - s_2)) = (\varphi_1^*(\widehat{v}))(s_1 - s_2) \ .$$

By definition, $\varphi_1^*(\widehat{v}) \in \mathcal{V}_i$. Since $\mathcal{V}_i$ annihilates differences in $S_{i,j}$, we get $(\varphi_1^*(\widehat{v}))(s_1 - s_2) = 0$. Thus, $\widehat{\mathcal{V}}_i$ strictly satisfies the annihilator condition over $\mathbb{F}_q^L$. Now we apply the restriction map. By definition, $M_{r,L}$ restricts a functional in $(\mathbb{F}_q^L)^*$ to $\mathbb{F}_q^r$. Under our embedding, this is equivalent to restricting $\widehat{v} \in (\mathbb{F}_q^L)^*$ to $\varphi_1(W^\circ)$. Evaluating $\widehat{v}$ on $\varphi_1(W^\circ)$ is identical to taking its projection $v = \varphi_1^*(\widehat{v}) \in V$ and evaluating v on W°. By duality, the kernel of the evaluation map from V onto W° is exactly W. Therefore, the image of any subspace $U \subseteq V$ under restriction to W° is canonically isomorphic to the quotient $(U+W)/W$. Let $\mathcal{W}_i = M_{r,L}(\widehat{\mathcal{V}}_i)$. By the duality established above, we have the canonical isomorphism:

$$(\mathcal{W}_1, \ldots, \mathcal{W}_n) \cong ((\mathcal{V}_1 + W)/W, \ldots, (\mathcal{V}_n + W)/W) \ .$$

Because $\mathcal{C}$ contains the quotient profile, it contains the isomorphic profile $\mathcal{W} = (\mathcal{W}_1, \dots, \mathcal{W}_n) \in \mathcal{L}((\mathbb{F}_q^r)^*)^n$. Any non-trivial subspace $U' \subseteq (\mathbb{F}_q^r)^*$ where $U' \neq \{0\}$ corresponds isomorphically to some subspace $(U+W)/W \neq \{0\}$ in V/W. We have already shown that:

$$\Phi_{V/W}\left((U+W)/W, ((\mathcal{V}_1+W)/W, \dots, (\mathcal{V}_n+W)/W), \alpha\right) < 0 \ .$$

Because Φ is strictly invariant under isomorphism, we deduce that for all $\{0\} \neq U' \subseteq (\mathbb{F}_q^r)^* \setminus \{0\}$,

$$\Phi_{(\mathbb{F}_q^r)^*}(U', (\mathcal{W}_1, \dots, \mathcal{W}_n), \alpha) < 0 \ .$$

All conditions are satisfied, i.e. $\mathcal{W} \in \mathcal{W}_{\ell,\alpha,\varepsilon,r}$ and $\mathcal{C}$ contains $\mathcal{W}$. □

4.3 Alphabet size bounds for list-recovery of random linear codes

Now, we are ready to prove our alphabet bounds for list-recovery of random linear codes. As in the list-decoding section, we will first count the number of local profiles in Definition 23 and then instantiate Theorem 2.7 for each of them and then union bound the probability that our code contains any of the local profiles.

In this section, we are again enabled by our improved methods of counting via restriction to the profiles described in Definition 23 instead of over all list-recovery configurations. In particular, we only count each constraint once and not multiple times. Additionally, our method uses the rank r over which we are working over both while counting and applying Theorem 2.7.

Theorem 4.4. *Let s, n, ℓ be natural numbers and $R, \varepsilon, \varepsilon_0 \in (0,1)$ be real numbers such that $R+\varepsilon \leqslant 1$, let $L = L_{\ell,R,\varepsilon}$ and let $\mathbb{F}_q$ be a finite field such that $q^s > (2L)^{4/\varepsilon_0}$. Let $k = (R-\varepsilon_0)sn$. Let $\mathsf{Enc}_1, \dots, \mathsf{Enc}_n : \mathbb{F}_q^k \to \mathbb{F}_q^s$ be uniformly random linear maps.*

$$\Pr\left[\mathcal{C} \text{ is not } (1-R-\varepsilon, \ell, L) \text{ list-recoverable}\right] \leqslant q^{L^2 + L - \frac{\varepsilon_0 sn}{2}}$$

Proof. If $\mathcal{C}$ is not list-recoverable then, it contains $(\mathcal{W}_1, \dots, W_n) = \mathcal{W} \in \mathcal{W}_{\ell,\alpha,\varepsilon,r}$ for some $1 \leqslant r \leqslant L$ and $\alpha \geqslant R$. Now, if we consider a similar family of profiles as $\mathcal{W}_{\ell,\alpha,\varepsilon,r}$ with the final constraint replaced simply by $\Phi_{(\mathbb{F}_q^r)^*}((\mathbb{F}_q^r)^*, (\mathcal{W}_1, \dots, \mathcal{W}_n), \alpha) = 0$.

Definition 24. For any natural ℓ, reals $\alpha, \varepsilon \in (0,1)$, let $L = L_{\ell,\alpha,\varepsilon}$, and for any $r \leqslant L$, define

$$\begin{aligned}\mathcal{W}'_{\ell,\alpha,\varepsilon,r} = \{(\mathcal{W}_1, \dots, \mathcal{W}_n) \in \mathcal{L}(\mathbb{F}_q^{r*})^n \mid & \exists S \in \binom{\mathbb{F}_q^L}{\leqslant L+1}, \forall i \in [n], \exists S_i \subseteq S, S_i = S_{i,1} \sqcup \dots \sqcup S_{i,\ell} \text{ s.t.} \\ & \mathcal{V}_i = \{v \in (\mathbb{F}_q^L)^* \mid v(s_1 - s_2) = 0 \forall j \in [\ell], s_1, s_2 \in S_{i,j}\}, \\ & \mathcal{W}_i = M_{r,L}\mathcal{V}_i, \\ & \Phi_{(\mathbb{F}_q^r)^*}((\mathbb{F}_q^r)^*, (\mathcal{W}_1, \dots, \mathcal{W}_n), \alpha) = 0.\end{aligned}$$

then $\mathcal{C}'$ must also contain a profile from $\mathcal{W}'_{\ell,\alpha,\varepsilon,r}$ for some $\alpha > R$ since for any $(\mathcal{W}_1, \cdots, \mathcal{W}_n) \in W_{\ell,\alpha_1,\varepsilon,r}$ with $\alpha_1 \geqslant R$, then if $\alpha > \alpha_1$ is such that $\Phi_{(\mathbb{F}_q^r)^*}((\mathbb{F}_q^r)^*, (\mathcal{W}_1, \dots, \mathcal{W}_n), \alpha) = 0$ then $(\mathcal{W}_1, \cdots, \mathcal{W}_n) \in W'_{\ell,\alpha,\varepsilon,r}$ as well. Now, note that we can directly use Theorem 2.7 on $W'_{\ell,\alpha,\varepsilon,r}$.

Claim 4.5.

$$\sum_{\mathcal{W} \in \mathcal{W}'_{\ell,\alpha,m,r}} \Pr[\mathcal{C} \text{ contains } \mathcal{W}] \leqslant |\mathcal{W}'_{\ell,\alpha,m,r}| \cdot q^{rsn(R-\alpha-\varepsilon_0)}$$

Proof. For each $\mathcal{W} \in \mathcal{W}'_{\ell,\alpha,m,r}$, using Theorem 2.7, we have

$$\Pr[\mathcal{C} \text{ contains } \mathcal{W}] \leqslant q^{sn\cdot\Phi_{(\mathbb{F}_q^r)^*}((\mathbb{F}_q^r)^*,\mathcal{W},R-\varepsilon_0)} = q^{rsn(R-\varepsilon_0-\alpha)} \ . \qquad \square$$

Now, it remains to just compute $|\mathcal{W}'_{\ell,\alpha,\varepsilon,r}|$ for us to union bound.

Lemma 4.6.

$$|\mathcal{W}'_{\ell,\alpha,\varepsilon,r}| \leqslant \binom{\binom{L+1}{2}n}{\alpha\cdot r\cdot n}\cdot\binom{q^L}{L+1}$$

Proof. We begin by picking S, there are $\binom{q^L}{L+1}$ choices of S.

Now, let $W = \mathbb{F}_q^{r*}$. We know by the hypothesis that

$$\frac{\sum_{i=1}^n \dim \mathcal{W}_i^{\perp}}{n} = \alpha r.$$

Note that if $\dim(W_i^{\perp}) = r_i$ then it is sufficient to choose r_i pairs of elements of S, the equality constraints on which completely specify $\mathcal{W}_i$ and we do not need to pick all of S_i! Note that not all r_i pairs of elements of S impose r_i constraints, but here we are over counting since some r_i pairs must have specified $\mathcal{W}_i$.

Thus, the total choices is at most

$$\sum_{r_1+\cdots+r_n=\alpha\cdot r\cdot n}\prod_{i=1}^{n}\binom{\binom{L+1}{2}}{r_i} \leqslant \binom{\binom{L+1}{2}n}{\alpha\cdot r\cdot n} \ ,$$

where the final relation follows due to Vandermonde's identity. $\square$

Thus, we can now implement the union bound.

Let $p = \Pr[\mathcal{C} \text{ is not } (1-R-\varepsilon,\ell,L) \text{ average radius list-recoverable}]$.

$$\begin{aligned}
p &\leqslant \sum_{\alpha>R}\binom{q^L}{L+1}\cdot\sum_{r=1}^{L}\binom{\binom{L+1}{2}n}{\alpha rn}\cdot q^{r\cdot sn(R-\varepsilon_0-\alpha)}\\
&\leqslant \binom{q^L}{L+1}\cdot\sum_{\alpha>R}\sum_{r=1}^{L}\left(4L^2\right)^{rn}\cdot q^{r\cdot sn(R-\alpha-\varepsilon_0)}\\
&= \binom{q^L}{L+1}\cdot\sum_{r=1}^{L}\left(q^{-\varepsilon_0 s}4L^2\right)^{rn}\left(\sum_{\alpha>R}q^{r\cdot sn(R-\alpha)}\right)\\
&\leqslant 2\binom{q^L}{L+1}\cdot\sum_{r=1}^{L}q^{-\varepsilon_0 snr/2}\\
&\leqslant 2L\cdot\binom{q^L}{L+1}\cdot\cdot q^{-\varepsilon_0\cdot sn/2}\\
&\leqslant q^{L^2+L-\frac{\varepsilon_0 sn}{2}} \ .
\end{aligned}$$

To go from the first equation to the second, we observe that when $L=1$, we just need $\binom{n}{\alpha n} \leqslant 2^n$ which is sufficient. Now, when $L \geqslant 2$, we have that $\binom{\binom{L+1}{2}n}{\alpha rn} \leqslant \binom{L^2 n}{\alpha rn} \leqslant \binom{L^2 n}{rn}$ and thus we could use

the fact that $\binom{a}{b} \leqslant (\frac{4a}{b})^b$ i.e. $\binom{\binom{L+1}{2}n}{\alpha rn} \leqslant \left(\frac{4L^2}{r}\right)^{rn} \leqslant (4L^2)^{rn}$. Then, we just reorganize and use the fact that $\alpha > R$ and αrsn is always an integer to evaluate the geometric sum which we can then bound by 2.

Finally, we used the fact that each term is less than 1 and $2L\binom{q^L}{L+1} \leqslant (q^L)^{L+1}$. □

Theorem 4.7. *A random s-additive code of rate $R-\varepsilon_0$ is $(1-R-\varepsilon, \ell, L_{\ell,R,\varepsilon})$ list recoverable with high probability when $q^s > (2L_{\ell,R,\varepsilon})^{4/\varepsilon_0}$ and $sn > 4L^2_{\ell,R,\varepsilon}/\varepsilon_0$. Additionally, $L_{\ell,R,\varepsilon} \leqslant (\ell/(R+\varepsilon))^{(R+\varepsilon)/\varepsilon}$.*

Proof. Follows from Theorem 4.4 and Theorem 4.2. □

5 Conclusion and Further Questions

We conclude with several directions for future work.

Fully linear codes. A natural question is whether the gap in list-decoding guarantees can be closed for fully linear codes, i.e., whether one can remove the $\log 1/\varepsilon$ factor for random linear codes bringing down the alphabet size to the optimal $\exp(O(1/\varepsilon))$? Could better counting techniques suffice to resolve this?

Extensions to random LDPCs. Our results should extend naturally to random low-density parity-check codes via the framework of [MRRZ+20]. For list-decoding, this would yield LDPC codes over an alphabet of size $\exp(\widetilde{O}(1/\varepsilon))$ with $\mathrm{poly}(1/\varepsilon)$ sparsity. It remains unclear, however, whether the techniques of [MRRZ+20] extend to the additive code setting.

Randomness reduction. The expander-based techniques of [PP24] for reducing randomness appear directly applicable to our setting. Currently, RLCs require $Rn^2 \cdot \widetilde{O}(1/\varepsilon)$ bits of randomness, while our additive codes require $O(Rn^2/\varepsilon^2)$ bits. The techniques of [PP24] should reduce both to $O(n \cdot \mathrm{poly}(1/\varepsilon))$. Notably, via the "unfolding" view of [BCDZ25b], their approach should also be applicable to additive codes.

Constructions based on RLCs. Random linear codes serve as the base code in many code constructions. It would be interesting to understand whether our improved list-size bound leads to concrete improvements in such downstream applications. Additionally, is it ever useful to use random additive codes as the basis of such constructions? The only application we are aware of random additive codes instead of linear is in [GGH26].

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 would like to thank Joshua Brakensiek and Jun-Ting (Tim) Hsieh for various illuminating discussions on the problem.

V.G. is supported by a Simons Investigator award, a UC Noyce initiative 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] N. Alon, J. Bruck, J. Naor, M. Naor, and R.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. 3

[AEL95] N. Alon, J. Edmonds, and M. Luby. Linear time erasure codes with nearly optimal recovery. In *Proceedings of IEEE 36th Annual Foundations of Computer Science*, pages 512–519, 1995. 3

[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. 1, 2, 5, 7, 11, 30, 33

[AGL24] Omar Alrabiah, Venkatesan Guruswami, and Ray Li. *AG codes have no list-decoding friends: Approaching the generalized Singleton bound requires exponential alphabets*, pages 1367–1378. SIAM, 2024. 2

[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. 2, 4, 5, 7, 20, 32

[BCDZ25b] Joshua Brakensiek, Yeyuan Chen, Manik Dhar, and Zihan Zhang. From random to explicit via subspace designs with applications to local properties and matroids, 2025. To appear in STOC 2026. 1, 2, 3, 4, 5, 8, 9, 25, 29, 32, 33

[BDG24] Joshua Brakensiek, Manik Dhar, and Sivakanth Gopi. Improved field size bounds for higher order MDS codes. *IEEE Transactions on Information Theory*, 70(10):6950–6960, 2024. 1, 2

[BDGZ25] Joshua Brakensiek, Manik Dhar, Sivakanth Gopi, and Zihan Zhang. AG codes achieve list-decoding capacity over constant-sized fields. *IEEE Trans. Inf. Theory*, 71(8):5935–5956, 2025. 1

[BG25] Joshua Brakensiek and Venkatesan Guruswami. Maximal recoverability: A nexus of coding theory. *IEEE BITS the Information Theory Magazine*, pages 1–13, 2025. 1

[BGM23] Joshua Brakensiek, Sivakanth Gopi, and Visu Makam. Generic reed-solomon codes achieve list-decoding capacity. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, page 1488–1501, New York, NY, USA, 2023. Association for Computing Machinery. 1, 2

[CC09] Eric A. Carlen and Dario Cordero–Erausquin. Subadditivity of the entropy and its relation to brascamp-lieb type inequalities. *Geometric and Functional Analysis*, 19(2):373–405, September 2009. Funding Information: Keywords and phrases: Entropy, Brascamp-Lieb inequalities 2000 Mathematics Subject Classification: 26D15, 94A17 E.A.C's work is partially supported by US National Science Foundation grant DMS 06-00037. 7

[CDK+13] Michael Christ, James Demmel, Nicholas Knight, Thomas Scanlon, and Katherine Yelick. Communication lower bounds and optimal algorithms for programs that reference arrays – Part 1. *arXiv preprint arXiv:1308.0068*, 2013. 7

[CDK+24] Michael Christ, James Demmel, Nicholas Knight, Thomas Scanlon, and Katherine A. Yelick. On multilinear inequalities of Holder-Brascamp-Lieb type for torsion-free discrete Abelian groups. *J. Log. Anal.*, 16, 2024. 7

[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. 1

[Che26] Yeyuan Chen. List-recovery lower bound for folded linear codes, 2026. Manuscript: https://yeyuanch.github.io/files/folded_linear_lower_bound%20(1).pdf. 2, 19

[CZ25] Yeyuan Chen and Zihan Zhang. Explicit folded Reed-Solomon and multiplicity codes achieve relaxed generalized singleton bound. In Michal Koucký and Nikhil Bansal, editors, *Proc. 57th ACM Symp. on Theory of Computing (STOC)*, pages 1–12, 2025. 1, 2, 5, 7, 12, 19, 30, 31, 32

[Eli91] P. Elias. Error-correcting codes for list decoding. *IEEE Transactions on Information Theory*, 37(1):5–12, Jan 1991. 1

[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. 8, 30

[GG25b] Rohan Goyal and Venkatesan Guruswami. Structure theorems (and fast algorithms) for list recovery of subspace-design codes, 2025. *arXiv preprint arXiv:2512.08017*. 20

[GGH26] Rohan Goyal, Venkatesan Guruswami, and Jun-Ting Hsieh. Explicit constant-alphabet subspace design codes, 2026. *arXiv preprint arXiv:2604.15218*. 25

[GHK10] Venkatesan Guruswami, Johan Hastad, and Swastik Kopparty. On the list-decodability of random linear codes. In *Proceedings of the Forty-Second ACM Symposium on Theory of Computing*, STOC '10, page 409–416, New York, NY, USA, 2010. Association for Computing Machinery. 1

[GHSZ02] V. Guruswami, J. Hastad, M. Sudan, and D. Zuckerman. Combinatorial bounds for list decoding. *IEEE Transactions on Information Theory*, 48(5):1021–1034, 2002. 1

[GI01] Venkatesan Guruswami and Piotr Indyk. Expander-based constructions of efficiently decodable codes. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, pages 658–667, 2001. 3

[GI05] V. Guruswami and P. Indyk. Linear-time encodable/decodable codes with near-optimal rate. *IEEE Transactions on Information Theory*, 51(10):3393–3400, 2005. 3

[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 Transactions on Information Theory*, 68(2):923–939, February 2022. 1

[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. 1, 8

[GMR+22] Venkatesan Guruswami, Jonathan Mosheiff, Nicolas Resch, Shashwat Silas, and Mary Wootters. Threshold rates for properties of random codes. *IEEE Trans. Inf. Theory*, 68(2):905–922, 2022. 1, 8

[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). 1, 3

[GRZ22] 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. 1, 3

[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). 3

[GX22] Venkatesan Guruswami and Chaoping Xing. Optimal rate list decoding over bounded alphabets using algebraic-geometric codes. *J. ACM*, 69(2), January 2022. 1, 3

[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. 1, 3

[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. 3

[KMRZS17] Swastik Kopparty, Or Meir, Noga Ron-Zewi, and Shubhangi Saraf. High-rate locally correctable and locally testable codes with sub-polynomial query complexity. *J. ACM*, 64(2), May 2017. 3

[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. 1, 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). 1

[KRZ26] Mrinal Kumar and Noga Ron-Zewi. Advances in list decoding of polynomial codes. Technical Report TR26-032, Electronic Colloquium on Computational Complexity (ECCC), 2026. 3, 12

[KSY14] Swastik Kopparty, Shubhangi Saraf, and Sergey Yekhanin. High-rate codes with sublinear-time decoding. *J. ACM*, 61(5), September 2014. 1, 3

[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. 1, 2, 5, 8, 9, 18, 19

[LW18] Ray Li and Mary Wootters. Improved List-Decodability of Random Linear Binary Codes. In Eric Blais, Klaus Jansen, José D. P. Rolim, and David Steurer, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2018)*, volume 116 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 50:1–50:19, Dagstuhl, Germany, 2018. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. 1, 2, 4, 19

[MRRZ+20] 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, 2020. 1, 8, 25

[PP24] Aaron (Louie) Putterman and Edward Pyne. Pseudorandom Linear Codes Are List-Decodable to Capacity. In Venkatesan Guruswami, editor, *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*, volume 287 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 90:1–90:21, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. 1, 25

[Rot22] Ron M. Roth. Higher-order MDS codes. *IEEE Transactions on Information Theory*, 68(12):7798–7816, 2022. 1, 2

[RV25] Nicolas Resch and S. Venkitesh. List recoverable codes: The good, the bad, and the unknown (hopefully not ugly). *arXiv preprint arXiv:2510.07597*, 2025. 3

[RW14] Atri Rudra and Mary Wootters. Every list-decodable code for high noise has abundant near-optimal rate puncturings. In *Proceedings of the Forty-Sixth Annual ACM Symposium on Theory of Computing*, STOC '14, page 764–773, New York, NY, USA, 2014. Association for Computing Machinery. 1

[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. 2

[Woo13] Mary Wootters. On the list decodability of random linear codes with large error rates. In *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing*, STOC '13, page 853–860, New York, NY, USA, 2013. Association for Computing Machinery. 1

[ZP82] V. V. Zyablov and M. S. Pinsker. List cascade decoding. *Problems of Information Transmission*, 17(4):236–240, 1982. Translated from Problemy Peredachi Informatsii, 17(4):29–34, 1981. 1

A Submodular Brascamp-Lieb Inequality

We now prove the submodular Brascamp-Lieb inequality, restated below. The proof we present here is a reworking of the [BCDZ25b] proof.

Theorem A.1. *Let E be a linear space and let $E_1, E_2, \ldots, E_n \subseteq E$ be subspaces. Suppose that for some $s_1, \ldots, s_n \geqslant 0$, the following inequality holds for every linear subspace $F \subseteq E$:*

$$\dim E - \dim F \leqslant \sum_{i=1}^{n} s_i[\dim E_i - \dim(F \cap E_i)] \ .$$

Then, for every submodular function $f : \mathcal{L}(E) \to \mathbb{R}$, we have

$$f(E) \leqslant \sum s_i f(E_i) \ .$$

Proof. Let $c(F) = \sum_{i=1}^{n} s_i \dim(F \cap E_i) - \dim F$. The hypothesis is that for all $F \subseteq E$, we have

$$c(F) \leqslant c(E).$$

We will prove the claim for all submodular functions via induction on n and $\dim E$.

To prove the base case for $n = 1$, we consider $F = E_1 \implies \dim E - \dim E_1 \leqslant 0 \implies E = E_1$. Now, additionally, $F = \{0\} \implies \dim E - s_1 \dim E \leqslant 0 \implies s_1 \geqslant 1$ or $E = \{0\}$. Either way, we are done.

Now, without loss of generality, $n \geqslant 2$, and s_1, s_2 are non-zero. We begin by assuming that there exists a $\{0\} \neq W \subseteq E$ such that $c(W) = c(E)$. To show that this is okay to assume, we consider s_1 and s_2. Consider replacing s_1 with $s_1 + \alpha t$ and s_2 with $s_2 - \beta t$ where α and β are such that if the new cost function is c' then $c'(E) = c(E)$. Now, there is a positive value of t for which either there exists a space $\{0\} \neq W \subseteq E$ such that $c(W) = c(E)$ or one of the s_i's can be made 0. Similarly, there is a negative t for which there exists such a space. We will now prove the result for both these resulting sequences and averaging out their corresponding results in exactly the desired inequality.

Now, we have a $\{0\} \neq W \subseteq E$ such that $c(W) = c(E)$ and for all $U \subseteq E$, we have $c(U) \leqslant c(E)$.

Define $c_1(U) = \sum_{i=1}^{n} s_i \dim((U + W)/W \cap (E_i + W)/W) - \dim((U + W)/W)$. Note that this is equivalent to defining costs in the quotient space E/W replacing E_i with $(E_i + W)/W$.

Now, note that

$$\begin{aligned} c(U + W) &= \sum_{i=1}^{n} s_i \dim((U + W) \cap E_i) - \dim(U + W) && (5) \\ &= \sum s_i(\dim(W \cap E_i) + \dim((U + W)/W \cap (E_i + W)/W)) - \dim(U + W)/W - \dim W && (6) \\ &= c(W) + c_1(U) && (7) \end{aligned}$$

Note that we have $c(E) = c(W) + c_1(E)$ and thus $c_1(E) = 0$. Additionally, $c(U + W) \leqslant c(E) = c(W) \implies c_1(U) \leqslant 0$ i.e. $c_1(U) \leqslant c_1(E)$.

Note that, we can also view that c_1 as a cost function replacing intersections with E_i but with $(E_i + W)/W$.

Now, let $g(U) = f(U + W) - f(W)$. Note that if f is submodular, then so is g. Thus, by inductive hypothesis on W and U/W, we have

$$f(W) \leqslant \sum s_i f(E_i \cap W)$$

and

$$g(E) \leqslant \sum s_i g(E_i + W) \implies f(E) - f(W) \leqslant \sum s_i (f(E_i + W) - f(W)) \ .$$

Summing the above two inequalities, we conclude that

$$f(E) \leqslant \sum s_i (f(E_i + W) + f(E_i \cap W) - f(W)) \leqslant \sum s_i f(E_i) \ ,$$

where the second step follows from the submodularity of f. □

B Subspace-designs, Agreement Hypergraphs, and Local Profiles

We begin by restating the definition of a subspace design code in the language of [GG25a].

Definition 25 (Subspace-Design Property)**.** For any function $\tau : \mathbb{N} \to \mathbb{R}_{\leqslant 1}$, 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:

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

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

B.1 Subspace-design codes list-decoding bound

In this subsection, we provide a complete self-contained proof of [CZ25]'s optimal list-decoding bounds for subspace-design codes.

We begin by reproducing the proof of [AGG+25]'s weakly partition connected (Definition 8) lemma.

Lemma B.1. *If $\mathcal{H} = (X, E)$ is a hypergraph with $|X| \geqslant 2$ such that $\sum_{e \in E} \max(|e| - 1, 0) \geqslant t \cdot (|X| - 1)$, then there exists $X' \subseteq X$ such that $\mathcal{H}' = (X', \{e \cap X' \mid e \in E\})$ is t-WPC.*

Proof. Let X' be a minimal by inclusion subset which is not a singleton such that $\sum_{e \in E} \max(|e \cap X'| - 1, 0) \geqslant t \cdot (|X'| - 1)$. Note that such a X' exists since X itself satisfies the above property. We claim that this X' works. Let $\mathcal{H}' = (X', E' = \{e \cap X' \mid e \in E\})$.

To prove the desired property, let $\mathcal{P}_0 \sqcup \cdots \sqcup \mathcal{P}_r$ be a partition. We have

$$\begin{aligned}\sum_{e \in E} \max(|\{j \mid e \cap \mathcal{P}_j \neq \emptyset\}| - 1, 0) &= \sum_{e \in E', |e| > 0} \left(-1 + \sum_{i=0}^{r} \mathbf{1}(e \cap \mathcal{P}_i \neq \emptyset) \right) \\ &= \sum_{e \in E', |e| > 0} \left(|e| - 1 - \sum_{i=0}^{r} (|e \cap \mathcal{P}_i| - \mathbf{1}(e \cap \mathcal{P}_i \neq \emptyset)) \right)\end{aligned}$$

$$\geqslant t(|X'|-1) - t\left(\sum_{i=0}^{r}(|\mathcal{P}_i|-1)\right) \quad \text{(by minimality of } X')$$
$$= t(|X'| - \sum_{i=0}^{r}|\mathcal{P}_i| - 1 + r + 1) = tr \ . \qquad \square$$

We are now ready to prove the Chen-Zhang list-decoding bound [CZ25].

Theorem B.2 ([CZ25]). *Let $\mathcal{C}$ be τ-subspace design code where τ is non-decreasing. Then, for all $d \in \mathbb{N}$, the code $\mathcal{C}$ is $(\tau(d), d+1)$ strong average-agreement list-decodable.*[7]

Proof. If not, there exist linearly independent codewords $c_1 = 0, c_2, \ldots, c_{r+1}$ and $c_{r+2}, \ldots, c_m \in \mathrm{span}(c_2, \ldots, c_{r+1})$ and a $t > \tau(d) \cdot n$ such that $\mathcal{H} = ([m], \mathcal{E})$ is a t-weakly-partition connected hypergraph and for all $i \in [n]$, $\{c_j[i] \mid j \in e_i\}$ is a singleton or empty. Let $\mathcal{A} = \mathrm{span}(c_1, \ldots, c_t)$. Note that $\dim \mathcal{A} = r \leqslant d$.

Now, let $\mathcal{P}(c_1, \ldots, c_m)$[8] $= P_0 \sqcup P_1 \sqcup \cdots \sqcup P_r$. Observe that if $\mathcal{C}_i$ is the subspace of the code which is 0 on the ith coordinate, then we have that

$$\dim(\mathcal{A} \cap \mathcal{C}_i) \geqslant \max(|\{j \mid e_i \cap P_j \neq \emptyset\}| - 1, 0) \ .$$

Summing over both sides, we get that

$$\tau(d) \cdot r \cdot n \geqslant \sum_{i=1}^{n} \dim(\mathcal{A} \cap \mathcal{C}_i) \geqslant \max(|\{j \mid e \cap P_j \neq \Phi\}| - 1, 0) \geqslant t \cdot r$$

But then we have that $\tau(d) \cdot n \geqslant t$ which is a contradiction by the definition of t. $\square$

B.2 Subspace designs and avoidance of local profiles

Lemma B.3. *Let $\mathcal{C} = \{(\mathsf{Enc}_1(x), \ldots, \mathsf{Enc}_n(x)) \mid x \in \mathbb{F}_q^k\}$ be a τ-subspace design code. Let r be a natural number. For any vector space V of dimension $\leqslant r$, and local profile $\mathcal{V} = (\mathcal{V}_1, \ldots, \mathcal{V}_n)$ such that $\Phi(V, (\mathcal{V}_1, \ldots, \mathcal{V}_n), \tau(r)) < 0$, $\mathcal{C}$ does not contain $\mathcal{V}$.*

Proof. Let $A \subseteq \mathbb{F}_q^k$ be any subspace of dimension at most r and $\varphi : V \to A^*$ be any isomorphism.

Now, the subspace design property implies

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

On the other hand, we have

$$\sum_{i=1}^{n} \dim\ (\varphi\mathcal{V}_i)^\circ = \sum_{i=1}^{n}(\dim A - \dim \varphi\mathcal{V}_i) = \sum_{i=1}^{n}(\dim V - \dim \mathcal{V}_i) > \tau(r) \cdot \dim V \cdot n \ ,$$

where the last step follows from $\Phi(V, (\mathcal{V}_1, \ldots, \mathcal{V}_n), \tau(r)) < 0$. Combining the above facts, we can conclude that for some $i \in [n]$, we have $\dim\ (\varphi\mathcal{V}_i)^\circ > \dim \ker(\mathsf{Enc}_i)$, which implies that $\mathcal{C}$ does not contain $\mathcal{V}$ as desired. $\square$

[7] See Definition 16 and Theorem 3.1.

[8] Definition 17: Let $A_i = \mathrm{span}(e_1, \ldots, e_i)$ for $i \in \{1 \ldots, r+1\}$, $P_j = \{i \in [t] \mid e_i \in A_{j+1} \setminus A_j\}$ for $j \in \{0, 1, \ldots, r\}$. Here $A_0 = \emptyset$.

The above theorem demonstrates one of the directions of [BCDZ25b]'s reductions between random linear and subspace design codes. In particular, it shows that if there is a V-local profile $(\mathcal{V}_1, \cdots, \mathcal{V}_n)$ with $\dim V \leqslant r$ and $\Phi_V(V, (\mathcal{V}_1, \ldots, \mathcal{V}_n), \tau(r)) < 0$, so that a random additive code is unlikely to contain it, then a τ-subspace design code would also not contain this profile.

Thus, an yet alternate view of the list-size bound in [CZ25] is to establish if a code is not $(\tau(L) - R, L)$-GSB decodable, then it must contain an LCL-profile such that $\Phi_V(V, (\mathcal{V}_1, \ldots, \mathcal{V}_n), \tau(r)) < 0$. This is precisely what the profiles in Claim 3.3 capture. Now, if the code in question was already a τ-subspace design, this is an inherent contradiction.

Similarly, the [BCDZ25a] list-size bound for list-recovery of subspace-design codes follows from the above and the profiles arising from Lemma 4.3, along with the added observation that it is always sufficient to restrict to $r \leqslant O(\ell/\varepsilon)$ when thinking about list-recovery, and we do not need to worry about r as large as the output list L. We could also do the same in our work, but it does not give any gains in terms of alphabet size since our probability bounds decay geometrically with the rank r being considered anyway.

C List-decoding through BL framework

In this section, we present a method to show that the discrete remainder Brascamp-Lieb inequality tools can also indeed be used to achieve near-optimal results directly for list-decoding. Additionally, for expository and completeness purposes, we present proofs of the remainder Brascamp-Lieb inequality highlighting parallels to the proofs of list-decoding bounds.

Theorem C.1. *Let E be a linear space of functionals from a vector space A to $\mathbb{F}_q$, and let $E_1, E_2, \ldots, E_n \subseteq E$ be subspaces and $s_1, \ldots, s_n \geqslant 0$ be such that for all linear subspaces $F \subseteq E$, we have*

$$\dim E - \dim F \leqslant \sum_{i=1}^{n} s_i[\dim E_i - \dim(F \cap E_i)] \ .$$

Then, for any random variable X on A and arbitrary $v_1, \ldots, v_n \in A$, the following inequality holds:

$$1 - \max_{v \in V}(\Pr_X(X = v)) \leqslant \sum_{i=1}^{n} s_i(1 - \Pr_X(X - v_i \in E_i^{\circ})) \ .$$

We postpone the proof of the theorem to the next subsection but demonstrate how the above Brascamp-Lieb inequality can also be used as a tool to get improved alphabet sized bounds for list-decoding of random linear codes.

Theorem C.2. *Let $R \in (0, 1)$ be a constant. Let V and A be linear spaces, and let $\varphi : V \to A^*$ is an isomorphism, let $S \subseteq A$ be a subset. Let $S_1, \ldots, S_n$ be subsets of S such that*

$$\frac{\sum |S_i|}{n} > R|S| + 1 - R.$$

Let $\mathcal{V}_i = \{v \in V \mid (\varphi(v))(s_1 - s_2) = 0 \ \forall s_1, s_2 \in S_i\}$. Then, there exists a $W \subseteq V$ such that

$$\Phi_V(W, (\mathcal{V}_1, \ldots, \mathcal{V}_n), R) > \Phi_V(V, (\mathcal{V}_1, \ldots, \mathcal{V}_n), R) \ .$$

Proof. For the sake of contradiction, assume not. Then, the following holds for all $W \subseteq V$,

$$\Phi_V(W, (\mathcal{V}_1, \dots, \mathcal{V}_n), R) \leqslant \Phi_V(V, (\mathcal{V}_1, \dots, \mathcal{V}_n), R) \ ,$$

which is equivalent to

$$\dim V - \dim W \leqslant \frac{\sum_{i=1}^{n} [\dim \mathcal{V}_i - \dim(W \cap \mathcal{V}_i)]}{(1-R)n} \ .$$

Now apply Theorem C.1 with X being the uniform distribution on S, $E = \varphi V$, $E_i = \varphi \mathcal{V}_i$, and v_i being an arbitrary element from S_i. We can then conclude that

$$1 - \frac{1}{|S|} \leqslant \frac{1}{(1-R)n} \cdot \sum_{i=1}^{n} \left(1 - \frac{|S_i|}{|S|}\right) < \frac{1}{1-R}\left(1 - R - \frac{(1-R)}{|S|}\right) \ ,$$

which is a contradiction. □

Now recall the quantity $L_{\ell,R,\varepsilon}$ from Definition 21, applied to $\ell = 1$.

Corollary C.3. *For any reals $R, \varepsilon \in (0,1)$, we have $L_{1,R,\varepsilon} < \frac{1-R}{\varepsilon}$.*

Proof. Let $|S| \geqslant \frac{1-R}{\varepsilon}$ in Theorem C.2, and the conclusion follows. □

Theorem C.4. *A random s-additive code of rate R is $\left(\frac{(1-R-\varepsilon)(L-1)}{L}, L\right)$ list-decodable with high probability when $q^s > (4L)^{8/\varepsilon}$ and $ns > 16L^2/\varepsilon$.*

Proof. Follows from Corollary C.3 applied to Theorem 4.7 with $\varepsilon_0 = \varepsilon$ giving that an $R - \varepsilon$ rate random s-additive code is $\left(\frac{(1-R-\varepsilon)(L-1)}{L}, L\right)$ decodable when $q^s > (4L)^{4/\varepsilon}$ and $ns > 4L^2/\varepsilon$. Now, we can reparameterize $R - \varepsilon$ to be the new rate and $\varepsilon \leftarrow \varepsilon/2$. □

C.1 Proofs of remainder Brascamp Lieb inequality

We present two proofs of Theorem C.1. The first one is essentially the proof in [BCDZ25b] but presented in dual form. The second proof is inspired by [AGG+25]'s weakly partitioned hypergraphs (See Definition 8).

Before beginning either proof, we not that it is sufficient to prove the result for X that are uniform on some subsets.

Claim C.5. *It suffices to prove Theorem C.1 for distributions uniform over their support.*

Proof. Let X be any random variable on V. Let $V = \{w_1, \cdots, w_N\}$ such that $P(X = w_1) \geqslant P(X = w_2) \geqslant \cdots \geqslant P(X = w_n)$. Let X_i be the uniform distribution on $\{w_1, \cdots w_i\}$. Now, there are $\gamma_i \geqslant 0$ such that $X = \sum_i \gamma_i X_i$. Additionally, if we can prove the inequality for all X_i then, the γ_i weighted convex combinations of the conclusions is exactly the conclusion for X. Thus, it suffices to only focus on uniform distrbutions. □

C.1.1 Proof 1. Based on careful induction

Proof. Let P be the distribution of X. Note that P is by our assumption uniform on some set S.

Let $c(F) = \sum_{i=1}^{n} s_i \dim(F \cap E_i) - \dim F$. The hypothesis is that for all $F \subseteq E$, we have

$$c(F) \leqslant c(E) \ .$$

Our proof will now proceed by induction on the size of the support of X. Note that if X had support size 1 then the conclusion follows as all $s_i \geqslant 0$ and the left hand side is just 0. So we assume that $|\mathsf{supp}(X)| \geqslant 2$.

Let $p = 1/|S|$. Without loss of generality we assume that $u_0 \in S$ as it translating the distribution does not change anything. Thus, we set $u_0 = \{0\}$.

Let $u_1, \ldots, u_r$ be such that u_j is an arbitrary element of $S \setminus \mathrm{span}(u_1, \cdots, u_{i-1})$ and this process of picking elements stops when $S \subseteq \mathrm{span}(u_1, \cdots, u_r)$. Let $U_j = \mathrm{span}(u_1, \ldots, u_j)$. Let $\lambda_j = \Pr[X \in U_j \setminus U_{j-1}]$. Now, $X = \sum \lambda_j X_j$ where X_j is only supported on $U_j \setminus U_{j-1}$. Note that the support of X_j is now strictly smaller than that of X so we can assume by induction that we have proven the result for that distribution.

For each (v_i, E_i) pair, let $I_i = \{j \mid \exists u \in U_j \setminus U_{j-1} \text{ such that } E_i(u - v_i) = 0\}$. For $j \in I_i$, let $v_{i,j} = v_i$ and $v_{i,j} = u_j$ otherwise.

Let us now sum over these probabilities over all i for any fixed j. We get by applying the inductive hypothesis to the distribution X_j, we get:

$$\lambda_j - p \leqslant \sum_{i=1}^{n} s_i(\lambda_j - \Pr[X \in (U_j \setminus U_{j-1}) \wedge E_i(X - v_{i,j}) = 0])$$

Summing over j in 0 through r, we get

$$1 - (r+1)p \leqslant \sum_{i=1}^{n} s_i \left(1 - \sum_{j=0}^{r} \Pr[X \in (U_j \setminus U_{j-1}) \wedge E_i(X - v_{i,j}) = 0])\right) \ .$$

Let us now try to evaluate the expression for a fixed i,

$$\begin{aligned}\sum_{j=0}^{r} \Pr[X \in (U_j \setminus U_{j-1}) \wedge E_i(X - v_{i,j}) = 0])] &\geqslant \sum_{j \notin I_i} p + \sum_{j \in I_i} \lambda_j \Pr[X_j - v_i \in E_i^\circ] \\ &= p\,(r + 1 - |I_i|) + \Pr[X - v_i \in E_i^\circ]\end{aligned}$$

where for each $j \notin I_i$, we pick up at least a p term, and if $j \in I_i$, we get a term of the form: $\Pr[X \in (U_j \setminus U_{j-1}) \wedge E_i(X - v_i) = 0])$ as $v_{i,j} = v_i$ in that case. Now, note that $\Pr[X \in (U_j \setminus U_{j-1}) \wedge E_i(X - v_i) = 0]) = \lambda_j \Pr[X_j - v_i \in E_i^\circ]$.

This gives us that

$$1 - p - rp \leqslant \sum_{i=1}^{n} s_i \left(1 - \Pr[X - v_i \in E_i^\circ] - p\,(r + 1 - |I_i|)\right) \ .$$

Therefore, if we can show that

$$r \leqslant \sum_{i=1}^{n} s_i \,(r + 1 - |I_i|)$$

we will be done. Now,

$$\begin{aligned}(r+1-|I_i|) &= r - \left(-1 + \sum_{j=0}^{m} \mathbf{1}(j \in I_i)\right) \\ &\geqslant r - \dim(E_i^\circ \cap U_r) \\ &= r - (\dim E_i^\circ + \dim U_r - \dim(E_i^\circ + U_r)) \\ &= \dim(E_i^\circ + U_r) - \dim E_i^\circ \\ &= \dim(E_i) - \dim(E_i \cap U_r^\perp)\end{aligned}$$

Thus, it is sufficient if

$$r = \dim E - \dim U_r^\perp \leqslant \sum s_i(\dim E_i - \dim(E_i \cap U_r^\perp)),$$

but this is exactly the hypothesis with $F = U_r^\perp$. □

C.1.2 Proof 2. inspired by weakly-partition-connected hypergraphs

Proof. Additionally, we note that it is sufficient to prove the result for rational s_i. Now we simply repeat s_i as well to assume they are all equal. Let this common value now be ς. Let X be the distribution with the minimal support for which the conclusion does not hold. Thus, X is uniform on a set S and the conclusion holds for uniform distributions on any subset of S. Additionally, shifting the distribution does not influence the conclusion. Thus, without loss of generality, $\{0\} \in S$. As before, when S is a singleton, then the result is trivial and there is nothing to prove, so assume $|S| \geqslant 2$.

Fix $v_1, \ldots, v_n$ now for which the conclusion is false. Let $S_i = \{x \in S \mid x - v_i \in E_i^\circ\}$. We can also assume that no S_i is empty. By our assumption

$$1 - \frac{1}{|S|} > \varsigma \cdot \sum_{i=1}^{n} \left(1 - \frac{|S_i|}{|S|}\right) \iff \sum_{i=1}^{n} (|S_i| - 1) > \left(n - \frac{1}{\varsigma}\right)(|S| - 1)$$

but for every subset $S' \subsetneq S$, we have

$$\begin{aligned}1 - \frac{1}{|S'|} \leqslant \varsigma \cdot \sum_{i=1}^{n} \left(1 - \frac{\max(|S_i \cap S'| - 1, 0) + 1}{|S'|}\right) \\ \iff \sum_{i=1}^{n} \left(|S_i \cap S'| - \mathbf{1}(S' \cap S_i \neq \emptyset)\right) \leqslant \left(n - \frac{1}{\varsigma}\right)(|S'| - 1).\end{aligned}$$

Now, let $S = \{0, v_1, \ldots, v_r, t_1, \ldots, t_m\}$ where $v_1, \ldots, v_r$ are linearly independent and $t_j \in \operatorname{span}(v_1, \ldots, v_r)$ for all $j \in [m]$.

Hence, let $U_0 = \{0\}, U_j = \operatorname{span}(v_1, \ldots, v_j)$ for $j \in [r]$. Let $\mathcal{P}_j = S \cap (U_j \setminus U_{j-1})$. Let $\mathcal{P}_0 = \{0\}$.

Now, by the hypothesis, and using the fact that for subspaces $F_1, F_2 \subseteq E$, it holds that $\dim F_1 - \dim F_2 = \dim F_2^\circ - \dim F_1^\circ$ and $(F_1 \cap F_2)^\circ = F_1^\circ + F_2^\circ$, we have

$$n\varsigma r - \varsigma \sum_{i=1}^{n} (\dim E_i - \dim(U_r^\perp \cap E_i)) = \varsigma \sum_{i=1}^{n} (r - (\dim(U_r + E_i^\circ) - \dim E_i^\circ))$$

$$
\begin{aligned}
&\geqslant \varsigma \sum_{i=1}^{n} \left(-1 + \sum_{j=0}^{r} \mathbf{1}(\mathcal{P}_j \cap S_i \neq \emptyset) \right) \\
&= \varsigma \sum_{i=1}^{n} (|S_i| - 1 - \sum_{j=0}^{r} (|S_i \cap \mathcal{P}_j| - \mathbf{1}(\mathcal{P}_j \cap S_i \neq \emptyset))) \\
&> (n\varsigma - 1)\,(|S| - 1) - \sum_{j=0}^{r} (n\varsigma - 1)\,(|\mathcal{P}_j| - 1) \\
&= (n\varsigma - 1)r \ .
\end{aligned}
$$

But this means

$$
r = \dim E - \dim U_r^{\perp} > \varsigma \sum_{i=1}^{n} (\dim E_i - \dim(U_r^{\perp} \cap E_i)) \ ,
$$

which contradicts the hypothesis for $F = U_r^{\perp}$. □

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il