Combinatorial Bounds for List Recovery via Discrete Brascamp–Lieb Inequalities

Joshua Brakensiek* Yeyuan Chen† Manik Dhar‡ Zihan Zhang§

Abstract

In coding theory, the problem of list recovery asks one to find all codewords c of a given code C which such that at least $1-\rho$ fraction of the symbols of c lie in some predetermined set of ℓ symbols for each coordinate of the code. A key question is bounding the maximum possible list size L of such codewords for the given code C.

In this paper, we give novel combinatorial bounds on the list recoverability of various families of linear and folded linear codes, including random linear codes, random Reed–Solomon codes, explicit folded Reed–Solomon codes, and explicit univariate multiplicity codes. Our main result is that in all of these settings, we show that for code of rate R, when $\rho = 1 - R - \varepsilon$ approaches capacity, the list size L is at most $(\ell/(R+\varepsilon))^{O(R/\varepsilon)}$. These results also apply in the average-radius regime. Our result resolves a long-standing open question on whether L can be bounded by a polynomial in ℓ. In the zero-error regime, our bound on L perfectly matches known lower bounds.

The primary technique is a novel application of a discrete entropic Brascamp–Lieb inequality to the problem of list recovery, allowing us to relate the local structure of each coordinate with the global structure of the recovered list. As a result of independent interest, we show that a recent result by Chen and Zhang (STOC 2025) on the list decodability of folded Reed–Solomon codes can be generalized into a novel Brascamp–Lieb type inequality.

1 Introduction

Error-correcting codes ensure reliable communication over noisy channels by embedding messages $m \in \Sigma^k$ into redundant codewords $c \in \Sigma^n$. At a high level, a fundamental goal in coding theory is to understand the optimal trade-off between the rate of a code and its resilience to errors. As a basic example, a code $\mathcal{C} \subseteq \Sigma^n$ with rate $R = k/n$ and minimum relative Hamming distance δ can be uniquely decoded from up to a $\delta/2$ fraction of adversarial symbol errors. The breakthrough idea of *list decoding*, introduced by Elias [Eli57] in the 1950s, further extended this capability, allowing decoding beyond the unique decoding radius by outputting a small list of candidate messages. Over the past several decades, list decoding has become a core topic in modern coding theory, with far-reaching influence across theoretical computer science — including, but not limited to, the theory of pseudorandomness [STV99], hard-core predicates [GL89], complexity theory [CPS99], and probabilistically checkable proofs [AS97].

In this work, we focus on the notion of *list recovery*, a powerful generalization of list decoding, in which the decoder must output a short list of candidate codewords consistent with multiple possible

*University of California, Berkeley. josh.brakensiek@berkeley.edu
†Department of EECS, University of Michigan, Ann Arbor. yeyuanch@umich.edu
‡Department of Mathematics, Massachusetts Institute of Technology. dmanik@mit.edu
§Department of Computer Science and Engineering, The Ohio State University. zhang.13691@osu.edu

(potentially corrupted) symbols at each coordinate. Formally, for a code $\mathcal{C} \subseteq \Sigma^n$, we say $\mathcal{C}$ is (ρ, ℓ, L) list recoverable if, for any product set $S = S_1 \times \cdots \times S_n \in \binom{\Sigma}{\leq \ell}^n$ with $|S_1|, \ldots, |S_n| \leq \ell$, there are at most L codewords $c \in \mathcal{C}$ such that

$$\operatorname{dist}(c, S_1 \times \cdots \times S_n) \leq \rho n,$$

where $\operatorname{dist}(c, S)$ denotes the number of indices $i \in [n]$ such that $c_i \notin S_i$. In particular, list decoding is the special case of list recovery when $\ell = 1$.

During the past several decades, determining the optimal list recoverability of fundamental code families, such as linear codes, Reed–Solomon (RS) codes, and their variants, has remained a central challenge in coding theory. This challenge is not only of intrinsic interest, but also of great significance due to its profound impact on broader areas such as pseudorandomness [Tre99, TSUZ07, GUV09, TSU12, KTS22] and algorithm design [INR10, NPR11, LNNT16, DW22].

Similarly to the list decoding case, the Johnson-type bound [GS01] guarantees that any maximum distance separable codes are $\left(1 - \sqrt{\ell R}, \ell, \operatorname{poly}(n)\right)$ list recoverable. Moreover, the notion of list recovery capacity has been formally established in [GI01, Gur01, Res20]. Specifically, in the large alphabet regime, when $q \geq 2^{\Omega(\log \ell/\varepsilon)}$, plain random codes of rate R and block length n are $(\rho, \ell, O(\ell/\varepsilon))$ list recoverable with high probability, satisfying $\rho \geq 1 - R - \varepsilon$ (see [Res20, Theorem 2.4.12] for more details). However, inspired by the work of Chen and Zhang [CZ25], it was recently shown that the output list size of random linear codes [LMS25] and arbitrary linear codes [LS25] is lower bounded by $\ell^{\Omega(R/\varepsilon)}$, thereby establishing a separation between plain random codes and linear codes in the context of list recovery.

Over the past decades, a long line of influential work [ZP81, Gur01, GR06, GW13, RW18, KRZSW18, KRZSW23, LP20, GLS+24, GST22, Tam24, CZ25, LMS25, LS25] has advanced our understanding of the list recoverability of random linear codes, randomly punctured and explicit Reed–Solomon (RS) codes, as well as their variants, achieving parameters beyond the Johnson radius. More fine-grained introductions of these developments are listed below. For a more comprehensive history of list recovery, we refer the reader to the recent survey by Resch and Venkitesh [RV25].

List Recovery for Random Structured Codes. It has long been of significant interest to study the list recoverability of random linear codes. Initially, the argument of Zyablov and Pinsker [ZP81] showed that random linear codes of rate R over alphabet Σ of size $\ell^{O(1/\varepsilon)}$ are $(1 - R - \varepsilon, \ell, |\Sigma|^{O(\ell/\varepsilon)})$ list recoverable (see [Gur01] for more details). Subsequent advances reduced the output list size to $|\Sigma|^{O(\log^2 \ell/\varepsilon)}$ in the work of Rudra and Wootters [RW18], and later to $(\ell/\varepsilon)^{O(\ell/\varepsilon)}$ in the recent work of Li and Shagrithaya [LS25], which represents the current state of the art.

Owing to a long line of influential works [RW14, ST23, BGM23, GZ23, AGL24, AGG+25], the optimal list decodability of random RS codes is now fully understood. However, comparatively little is known about the list recoverability of random RS codes. Lund and Potukuchi [LP20] were the first to show that random RS codes are list recoverable beyond the Johnson bound. In particular, they proved that that random RS codes over the alphabet $\mathbb{F}_q$ of rate $O\left(\frac{1}{\sqrt{\ell} \log q}\right)$ are $\left(1 - \frac{1}{\sqrt{2}}, \ell, O(\ell)\right)$ list recoverable. This was later improved by Guo et al. [GLS+24], who showed that the codes are $(1 - \varepsilon, \ell, O(\ell/\varepsilon))$ list recoverable with rate $O\left(\frac{\varepsilon}{\sqrt{\ell} \log(1/\varepsilon)}\right)$. Based on the reduction developed in [LMS25], the recent work of Li and Shagrithaya [LS25] also applies to random RS codes. Specifically, random RS codes of rate R over alphabet of size $n \cdot (\ell/\varepsilon)^{(\ell/\varepsilon)^{O(\ell/\varepsilon)}}$ are $\left(1 - R - \varepsilon, \ell, (\ell/\varepsilon)^{O(\ell/\varepsilon)}\right)$ list recoverable with high probability.

Codes	Alphabet size $\lvert\Sigma\rvert$	List size L	Explicit?
Random Linear Codes [ZP81, Gur01]	$\ell^{O(1/\varepsilon)}$	$\lvert\Sigma\rvert^{O(\ell/\varepsilon)}$	No
Random Linear Codes [RW18]	$\ell^{O(1/\varepsilon)}$	$\lvert\Sigma\rvert^{O(\log^2(\ell)/\varepsilon)}$	No
Random Linear Codes [LS25]	$\ell^{O(1/\varepsilon)}$	$(\ell/\varepsilon)^{O(\ell/\varepsilon)}$	No
Random RS Codes [LS25]	$O_{\varepsilon,\ell,L,R}(n)$	$(\ell/\varepsilon)^{O(\ell/\varepsilon)}$	No
Random Linear Codes (This Work)	$\ell^{(\ell/(R+\varepsilon))^{O(R/\varepsilon)}/\varepsilon}$	$\left(\frac{\ell}{R+\varepsilon}\right)^{O(R/\varepsilon)}$	No
Random RS Codes (This Work)	$O_{\varepsilon,\ell,L,R}(n)$	$\left(\frac{\ell}{R+\varepsilon}\right)^{O(R/\varepsilon)}$	No
Folded RS Codes [GR06]	$\left(\frac{n}{\varepsilon^2}\right)^{O(\log(\ell)/\varepsilon^2)}$	$\left(\frac{n}{\varepsilon^2}\right)^{O(\log(\ell)/\varepsilon^2)}$	Yes
Univariate Multiplicity Codes [Kop15]	$\left(\frac{n}{\varepsilon^2}\right)^{O(\log(\ell)/\varepsilon^2)}$	$\left(\frac{n}{\varepsilon^2}\right)^{O(\log(\ell)/\varepsilon^2)}$	Yes
Folded RS/Univariate Multiplicity Codes [GW13]	$\left(\frac{n\ell}{\varepsilon^2}\right)^{O(\ell/\varepsilon^2)}$	$\left(\frac{n\ell}{\varepsilon}\right)^{O(\ell/\varepsilon)}$	Yes
Folded RS/Univariate Multiplicity Codes [KRZSW18, KRZSW23, Tam24]	$\left(\frac{n\ell}{\varepsilon^2}\right)^{O(\ell/\varepsilon^2)}$	$(\ell/\varepsilon)^{O((1+\log\ell)/\varepsilon)}$	Yes
Folded AG Codes [GX13, GK16]	$\exp\left(\frac{\ell\log(\ell/\varepsilon)}{\varepsilon^2}\right)$	$2^{2^{2^{O_{\varepsilon,\ell}(\log^*(n))}}}$	Yes
Codes Based on the AEL Framework [ST25]	$\exp(\exp(\ell/\varepsilon\log(\ell/\varepsilon)))$	$\exp(\exp(\ell/\varepsilon\log(\ell/\varepsilon)))$	Yes
Codes Based on the AEL Framework [JS25]	$\exp((\ell/\varepsilon)^{(\ell/\varepsilon)^{(\ell/\varepsilon)}})$	$(\ell/\varepsilon)^{O(\ell/\varepsilon)}$	Yes
Folded RS/Univariate Multiplicity Codes (This Work)	$\left(\frac{n\ell}{\varepsilon^2}\right)^{O(\ell/\varepsilon^2)}$	$\left(\frac{\ell}{R+\varepsilon}\right)^{O(R/\varepsilon)}$	Yes
Any Linear Code [GLM+22, CZ25, LMS25, LS25]	Any	$\ell^{\Omega(R/\varepsilon)}$	Lower Bound

Table 1: Adapted from [KRZSW23]. Constructions of (α,ℓ,L) list recoverable codes of rate $R = R^* - \varepsilon$, where $R^* = 1-\alpha$ is list-recovering capacity (when $|\Sigma| \geq (1+\ell)^{\Omega(1/\varepsilon)}$). We assume that $R^* \in (0,1)$ is constant (independent of n,ε,ℓ).

List Recovery for Explicit Structured Codes. Explicit list recoverable codes such as folded RS [Kra03, GR06] and univariate multiplicity codes [Kop15] have been extensively studied over the past two decades. Guruswami and Rudra [GR06] first showed that folded RS codes of rate R over alphabet of size $\left(\frac{n}{\varepsilon^2}\right)^{O(\log(\ell)/\varepsilon^2)}$ are $\left(1-R-\varepsilon,\ell,\left(\frac{n}{\varepsilon^2}\right)^{O(\log(\ell)/\varepsilon^2)}\right)$ list recoverable. A similar result was extend to univariate multiplicity codes by the work of Kopartty [Kop15]. During the same period, a linear-algebraic decoding framework was promoted by Guruswami and Wang [GW13], which implies that both folded RS and univariate multiplicity codes of rate R achieve $\left(1-R-\varepsilon,\ell,\left(\frac{n\ell}{\varepsilon}\right)^{O(\ell/\varepsilon)}\right)$ list recoverablility over alphabet of size $\left(\frac{n\ell}{\varepsilon^2}\right)^{O(\ell/\varepsilon^2)}$. A subsequent line of work [KRZSW18, KRZSW23, Tam24] further improved the output list size from $\left(\frac{n\ell}{\varepsilon}\right)^{O(\ell/\varepsilon)}$ to $\left(\frac{\ell}{\varepsilon}\right)^{O((1+\log\ell)/\varepsilon)}$, which remains the state of the art.

For other structured codes, the work of [GX13, GK16] shows that folded algebraic geometry (AG) codes of rate R attain $\left(1-R-\varepsilon,\ell,2^{2^{2^{O_{\varepsilon,\ell}(\log^*(n))}}}\right)$ list recoverablility over alphabet of size $\exp\left(\frac{\ell\log(\ell/\varepsilon)}{\varepsilon^2}\right)$. Most recently, Srivastava and Tulsiani [Sri25] showed that explicit codes based on the AEL framework [AEL95] with rate R can achieve $\left(1-R-\varepsilon,\ell,\exp\left(\exp\left(\frac{\ell}{\varepsilon}\log\left(\frac{\ell}{\varepsilon}\right)\right)\right)\right)$ over alphabet of size $\exp\left(\exp(\frac{\ell}{\varepsilon}\log\left(\frac{\ell}{\varepsilon}\right))\right)$.

A Crucial Open Problem. For codes of rate R that are $(1-R-\varepsilon,\ell,L)$ list recoverable, the best known bound [KRZSW18, KRZSW23, Tam24] on the output list size L for all the aforementioned structured codes over the past few decades is $\left(\frac{\ell}{\varepsilon}\right)^{O((1+\log\ell)/\varepsilon)}$. Meanwhile, by the most recent work [CZ25, LMS25, LS25], the output list size of all these structured linear codes is lower bounded by $\ell^{\Omega(R/\varepsilon)}$. Therefore, a substantial gap remains between the best known upper and lower bounds

on the list recoverability of these codes. A crucial open problem, stated below and proposed multiple times in [RW18, KRZSW18, KRZSW23, LS25, RV25], will be resolved in this work.

Open Problem 1.1 (See [RW18, KRZSW18, KRZSW23, LS25, RV25]). *Can random linear codes, random RS codes, or explicit folded RS and univariate multiplicity codes of rate R achieve $(1-R-\varepsilon, \ell, \mathrm{poly}_{\varepsilon,R}(\ell))$ list recoverability? Moreover, can the output list size be further reduced from $\mathrm{poly}_{\varepsilon,R}(\ell)$ to approach the lower bound $\ell^{\Omega(R/\varepsilon)}$ as closely as possible?*

A Conjecture of Chen and Zhang. One potential approach to Open Problem 1.1 is to determine the optimal relationship among the radius ρ, rate R, input list size ℓ, and output list size L in the context of list recovery for these structured codes. In particular, Chen and Zhang [CZ25] proposed a conjecture concerning the optimal list recoverability of folded RS and univariate multiplicity codes. To formally state this conjecture for folded RS codes, we first recall their definition for convenience. Formally, given any parameters $s, n, k > 0$, a finite field $\mathbb{F}_q$, where $|\mathbb{F}_q| > sn > k$, a generator γ of $\mathbb{F}_q^\times$, and any sequence of n elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_q$, the corresponding (s,γ)-folded RS code over the alphabet $\mathbb{F}_q^s$ with block length n and rate $R = \frac{k}{sn}$ is defined as

$$\mathsf{FRS}^{s,\gamma}_{n,k}(\alpha_1, \alpha_2, \ldots, \alpha_n) := \left\{ \mathcal{C}(f) : f \in \mathbb{F}_q[x], \ \deg f < k \right\} \subseteq \left(\mathbb{F}_q^s\right)^n,$$

where $\mathcal{C}(f) := (F_1, F_2, \ldots, F_n) \in \left(\mathbb{F}_q^s\right)^n$, with $F_i := \left(f(\alpha_i), f(\gamma\alpha_i), \ldots, f(\gamma^{s-1}\alpha_i)\right)$, denotes the encoder of this code. The formal statement of the Chen–Zhang conjecture is stated below.

Conjecture 1.2 (See [CZ25, Conjecture 3.6]). *For any constants $\varepsilon > 0, \ell \geq 2, L+1 = \ell^a, a \in \mathbb{N}^{\geq 2}, R \leq \frac{a-1}{a}$ and generator γ of $\mathbb{F}_q^\times$ there exists a constant C such that: if $s \geq C$, $\frac{k-1}{s} \geq a$, and n is suffciently large, then any rate $R = \frac{k}{sn}$ folded RS code $\mathsf{FRS}^{s,\gamma}_{n,k}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ with appropriate evaluation points in $\mathbb{F}_q$ is $(\rho^* - \varepsilon, \ell, L)$ list-recoverable, where*

$$\rho^* = \frac{L+1-\ell}{L+1}\left(1 - \frac{aR}{a-1}\right).$$

In a recent work [BCDZ25], it was shown that list-recoverability of random linear codes over large alphabets is essentially the same as the list-recoverability of nearly optimal subspace designable codes, so a proof or refutation of Conjecture 1.2 that only relies on the "subspace design" nature of folded RS codes[1] is equivalent to resolving the same conjecture for random linear codes.

Beyond the trivial instances, our understanding of this conjecture in the genuine list-recovery regime (when $\ell \geq 2$) remains extremely limited. Prior to our work, the only two nontrivial pieces of evidence supporting Conjecture 1.2 came from [CZ25, Theorem 1.8] and [CCSZ25], which established the conjecture for the specific parameters $\ell = 2, L = 3$ and $\ell = 2, \rho^* = 0$ with arbitrary L, respectively.

1.1 Our Results

Our main contribution in this paper is a positive resolution of Open Problem 1.1. A more precise statement of our results is as follows.

Theorem 1.3 (Main Results). *For constants $\ell \geq 2, R, \varepsilon \in (0,1), L = (\frac{\ell}{R+\varepsilon})^{O(R/\varepsilon)}$. The following codes are $(1-R-\varepsilon, \ell, L)$ list-recoverable.*

[1] We name a few (non)-examples here: The proof of [CZ25] only relies on the subspace design property, while [GW13, KRZSW23, Tam24, Sri25] use additional interpolation techniques that are tailored for folded RS codes.

- *Explicit s-folded Reed–Solomon codes when $s \geq 16\ell/\varepsilon^2$* (Corollary 4.5).
- *Explicit s-order univariate multiplicity codes when $s \geq 32\ell/\varepsilon^2$* (Corollary 4.6).
- *Random $\mathbb{F}_q$-linear codes with high probability when $q \geq \exp(\log(\ell)L/\varepsilon)$* (Corollary 4.3).
- *Random Reed–Solomon codes over $\mathbb{F}_q$ with high probability when $q \geq cn$ for some constant $c = O_{\varepsilon,\ell,L,R}(1)$* (Corollary 4.4).

See Table 1 for a comparison of our results with prior work. The lower bound for output list size is $L \geq \ell^{\Omega(R/\varepsilon)}$. Therefore, our bound $(\frac{\ell}{R+\varepsilon})^{O(R/\varepsilon)}$ is nearly optimal up to a constant multiplicative factor on the exponent when we consider the rate R is a constant, which basically resolved Open Problem 1.1. We also comment that the denominator $R+\varepsilon$ is crucial when the rate R approaches to 0. It guarantees the denominator does not vanish as long as we have some slack $\varepsilon > 0$ away from the threshold.

The above bound is nearly optimal asymptotically for radius $1-R-\varepsilon$. However, if we fix $\ell, L \geq 2, R \in (0,1)$, it remains elusive to decide the exact radius ρ such that linear codes could be (ρ, ℓ, L) list-recoverable. A conjecture on the exact value of ρ is formulated as in Conjecture 1.2. In [CZ25], it was proved that the radius ρ must be upper bounded by the conjectured value ρ^*, so an ideal result is to prove $\rho \geq \rho^* - \varepsilon$ for arbitrarily small slack $\varepsilon > 0$ and close the gap. In this work, we prove this for **zero-error** case.

Theorem 1.4 (Corollary 3.2)**.** Conjecture 1.2 *is true when* $\rho^* = 0$.

This parameterized exact bound can be seen as the counterpart of the famous "generalized singleton bound [ST23]" in zero-error list-recovery regime. We comment that there is a reduction Theorem 2.5 by [BCDZ25] from list-recoverability of optimal subspace designable codes to that of random linear codes, so a direct corollary from Theorem 1.4 and their reduction Theorem 2.5 is that Conjecture 1.2 is also true for random linear codes when $\rho^* = 0$.

Remark 1.5. There is still a gap between our upper bound and the lower bound conjectured in Conjecture 1.2. We comment that it is impossible that our upper bound in this paper is optimal in general. To see why, [CZ25, Theorem 1.8] has shown that these codes can be $(\frac{R}{2} - \varepsilon, 2, 3)$ list-recoverable for arbitrarily small $\varepsilon > 0$, which proves Conjecture 1.2 in a very special case. However, directly using proof techniques in this paper and plug in this set of parameter would only give worse bound, which is not optimal. We note that [CZ25, Theorem 1.8] is the only known special case of Conjecture 1.2 that was proved but not follows from Theorem 1.4. Although Theorem 1.3 already gives nearly optimal bound for the radius $1-R-\varepsilon$, we still think the fine-grained parameterized bound conjectured in Conjecture 1.2 is a very interesting open problem.

As we will discuss later, our main techniques is a discrete entropic Brascamp-Lieb inequality stated in Theorem 1.6. This inequality quantifies Shannon entropy.

Inspired by a recent result of Chen and Zhang [CZ25] for list decoding, we prove in Section 5 a novel "Brascamp–Lieb-like" inequality, see Theorem 1.7. However, instead of bounding the entropy of a probability distribution, we instead look at the "remainder" of a probability distribution $X \leftarrow \Omega$, which we define to be $r(X) := 1 - \max_{u \in \Omega}(X(u))$. In Section 5.1, we show how this inequality can be used to recover Chen and Zhang's result that subspace designable codes asymptotically achieve the generalized Singleton bound [ST23].

Finally, in Section 6 we give a self-contained proof of our main technique, discrete entropic Brascamp-Lieb inequality Theorem 1.6. Its original proof [CDK+13, CCE09] requires heavy hammers stemmed from pure mathematics community. We encourage readers to check our self-contained proof to get crucial ideas necessary in this discrete entropic form. We hope that could reveal some main intuitions behind this proof and make the result more accessible.

1.2 Technical Overview

The primary technical contribution of this paper is novel connection between discrete Brascamp–Lieb inequalities and list-recovery. The original continuous Brascamp–Lieb inequality [BL76] is used to prove various results in functional analysis (such as hypercontractivity) by relating some "global" continuous structure with many "local" projections of the same data. The functional analysis community has taken much interest in proving many generalizations of the original Brascamp–Lieb inequality [BCCT05, BCCT08, CCE09, BT24], including in discrete settings [CDK+13, Chr13, BT24, CDK+24]. Such inequalities have many applications in TCS including the study of matrix multiplication [CDK+13], non-commutative linear algebra [GGOW20,FSG23], quantum information theory [BSW23] among other topics [DR16, BJ22].

We crucially make use of a discrete Brascamp–Lieb inequality due to Christ, Demmel, Knight, Scanlon, and Yelick [CDK+13, CDK+24]. However, For convenience, we use a "discrete entropic" variant of their inequality based on a duality theorem of Carlen et al. [CCE09] (see also Remark 1.13 of [BT24]).

Theorem 1.6 (Discrete Entropic Brascamp–Lieb [CDK+13, CDK+24, CCE09])**.** *Let V be a d-dimensional vector space over $\mathbb{F}_q$. For each $i \in [m]$, consider a scalar $s_i \geq 0$ and a linear map $\pi_i : V \to V_i$, where V_i is a d_i-dimensional vector space over $\mathbb{F}_q$. Assume further that for all subspaces $U \subseteq V$ we have that*

$$\dim(U) \leq \sum_{i=1}^{m} s_i \dim(\pi_i(U)) \tag{1}$$

Then, for every probability distribution X over V, we have that

$$H(X) \leq \sum_{i=1}^{m} s_i H(\pi_i(X)). \tag{2}$$

As the fundamental ideas behind the proof of Theorem 1.6 are rather elementary, we give a self-contained proof of this inequality in Section 6.

The novel step we take in this paper is to relate the linear maps $\pi_i : V \to V_i$ as encoding maps of a subspace design code. More precisely, we pick V to be a suitable subcode of our subspace design code, and let each π_i denote projection onto the ith coordinate. It turns out with an appropriate choice of the parameters $s_i \geq 0$, the equation (1) is *equivalent* to a strong subspace design condition! As such, if the dimension of the subcode V is bounded by the subspace design parameters, we get that (2) holds for *any* probability distribution X over V for *any* bounded-dimension subcode V of *any* subspace design code.

In our application to list recovery, we pick X to (essentially) be the uniform distribution over a maximal recovered list (with V being the span of the support of X). Then, each $H(\pi_i(X))$ can be bounded in terms of the local list size ℓ and the local error ρ_i–see Equation (9). Furthermore, since X is a uniform distribution, $H(X)$ can be expressed in terms of the maximum list size L. As such, we near-immediately get an equation relating the global list size L with local list size ℓ and the recovery error ρ. A careful asymptotic computation, yields our bound that L is bounded by a polynomial function of ℓ.

Since explicit folded Reed–Solomon codes and univariate multiplicity codes yield nearly optimal subspace designs [GK16], we immediately get sharp combinatorial list recovery bounds for these codes. In a recent work [BCDZ25], the authors showed an equivalence between list-recoverability of subspace designs and random linear codes. Therefore, the list-recoverability of random linear

codes directly follows from their reduction. Finally, the list-recoverability of random Reed–Solomon codes follows from a "local equivalence" between random RS and random linear codes established by [LMS25].

Remainder BL Inequality. To strengthen the connections between coding theory and Brascamp-Lieb inequalities, we aim to prove a novel Brascamp-Lieb-style inequality inspired by a recent result of Chen and Zhang [CZ25] for list decoding. However, instead of bounding the entropy of a probability distribution, we look at a different quantity which we call *remainder*. For any distribution $X \leftarrow \Omega$, let the remainder $r(X) := 1 - \max_{u \in \Omega}(X(u))$.

Theorem 1.7 (Brascamp-Lieb inequality for remainder)**.** *Let V be any linear space over $\mathbb{F}_q$. Let $\pi_i \colon V \to V/W_i, i \in [n]$ denote n linear maps such that $\ker(\pi_i) = W_i \subseteq V$ satisfying the following*

$$\forall W \subseteq V, \dim(W) \leq \sum_{i=1}^{n} s_i \dim(\pi_i(W)). \tag{3}$$

Then, for any distribution $X \leftarrow V$, we know that

$$r(X) \leq \sum_{i=1}^{n} s_i r(\pi_i(X)).$$

We will see in Section 5.1 how the above result gives a proof of [CZ25]. Note that although the entropic form Theorem 1.6 proves Theorem 1.4, it does not produce generalized singleton bound for list-decoding. Readers that are familiar with [CZ25] should think the original proof of [CZ25] as a special case of Theorem 1.7 on uniform distributions only.

Streamlined Proof of Theorem 1.6. We conclude the technical overview by briefly describing an elementary proof we give of Theorem 1.6 in Section 6. It largely follows the proof strategy of [CDK+13, CDK+24], but replaces some (relatively) complex L^p inequalities with some standard facts about entropy as well as essentially eliminates the need to use facts about polyhedral geometry.

The proof proceeds by a double induction on $\dim(V)$ and n. The base cases are straightforward to handle. Observe that decreasing the parameters $s_i \geq 0$ only makes (2) stronger. Thus, without loss of generality we may always assume that (1) is an equality for some nonzero $U \subseteq V$. Such a space is called a *critical* in the BL inequality literature (e.g., [BCCT08, BCCT05]). The proof now splits into two cases: (A) $U \subsetneq V$ and (B) $U = V$.

Case (A) is handled using a divide-and-conquer, where we assume Theorem 1.6 holds for the spaces U and V/U. Combining these smaller cases to yield (2) for every distribution over V makes crucial use of the entropy chain rule. We remark this recursion on the critical subspace also appears in proofs of the GM-MDS theorem that the generator matrices of random Reed-Solomon codes attain all possible zero patterns [YH19, Lov21]. Case (B) is handled by perturbing the parameters $s_i \geq 0$ until some $U \subsetneq V$ is also critical, letting us reduce to case (A).

1.3 Open Questions

We conclude the introduction with a few open questions.

1. Our Theorem 1.4 establishes Conjecture 1.2 in the zero-error regime. However, beyond this regime, it remains open whether Conjecture 1.2 holds. In particular, we do not yet know in general the optimal trade-off among the decoding radius ρ, rate R, input list size ℓ, and output list size L for list recovery of such codes.

2. Recall that in [ST25], their list-recovery result was not only combinatorial but also algorithmic. A natural question is whether our combinatorial guarantees in this work can likewise be made algorithmic.

3. Corollary 4.3 requires the alphabet size to be at least $q = \ell^{\Omega(L/\varepsilon)}$, where $L = (\ell/(R+\varepsilon))^{\Theta(R/\varepsilon)}$. This lower bound is from a union bound over local profiles required to characterize list-recoverability [LMS25, Proposition 2.2]. Is it possible to prove similar results for smaller alphabets? By list-recovery capacity theorem [Res20], all alphabets $q \geq \ell^{\Omega(1/\varepsilon)}$ are possible to achieve $1 - R - \varepsilon$ radius.

4. We also leave open explicitly construct a code over alphabet size $q = \ell^{O(1/\varepsilon)}$ which achieves our $L = (\ell/(R+\varepsilon))^{O(R/\varepsilon)}$ bound.

Organization

In Section 2, we outline our notation as well as facts about subspace designs and entropy. In Section 3, we prove Corollary 3.2. In Section 4, we prove Theorem 1.3. In Section 5, we prove Theorem 1.7 and show how it connects to the list-decodability of codes. In Section 6, we give a streamlined proof of Theorem 1.6.

2 Preliminaries

Notations. For a code $\mathcal{C} \subseteq \Sigma^n$, we say $\mathcal{C}$ is (ρ, ℓ, L) list recoverable if, for any product set $S = S_1 \times \cdots \times S_n \in \binom{\Sigma}{\leq \ell}^n$ with $|S_1|, \ldots, |S_n| \leq \ell$, there are at most L codewords $c \in \mathcal{C}$ such that

$$\operatorname{dist}(c, S_1 \times \cdots \times S_n) \leq \rho n,$$

where $\operatorname{dist}(c, S)$ denotes the number of indices $i \in [n]$ such that $c_i \notin S_i$. We use $\mathsf{LIST}_{\mathcal{C}}(\rho, S_1 \times \cdots \times S_n) \subseteq \mathcal{C}$ to denote the set of codewords satisfying the above condition.

2.1 Subspace Designs

We now describe some standard notation for subspace designs (from, e.g., [GK16, CZ25]). Let $H_1, \ldots, H_m \subseteq \mathbb{F}_q^k$ be spaces with codimension s. We say that these spaces form an (d, A)- subspace design if for all d-dimensional subspaces $U \subseteq \mathbb{F}^k$ we have that

$$\sum_{i=1}^{m} \dim(U \cap H_i) \leq A.$$

A standard construction of a subspace design due to Guruswami and Kopparty [GK16] is to pick sm distinct points $\alpha_1, \ldots, \alpha_{sm} \in \mathbb{F}_q$ such that for all $i \in [m]$,

$$H_i := \{x \in \mathbb{F}_q^k : \sum_{i=0}^{k-1} x_i \alpha_j^{i-1} = 0 \text{ for all } j \in \{s(i-1)+1, \ldots, si\}\}.$$

They prove the following.

Theorem 2.1 ([GK16, Theorem 7]). *For all $d \in \{0, 1, \ldots, s\}$, $(H_1, \ldots, H_m)$ is a $\left(d, \frac{d(k-1)}{s-d+1}\right)$ subspace design.*

Remark 2.2 (Optimal parameters for subspace designs)**.** Very recently, [BCDZ25, Theorem 6.1] improved this bound to $\left(d, \frac{d(k-d)}{s-d+1}\right)$, and showed that this bound is tight for algebraically closed fields [BCDZ25, Theorem 6.2].

Definition 2.3 (Subspace Designable Code, [CZ25, Definition B.2])**.** For any $s \geq 1$, given an $\mathbb{F}$-linear code $C \subseteq (\mathbb{F}^s)^n$ with message length k and block length n, we use $\mathcal{C}\colon \mathbb{F}^k \to (\mathbb{F}^s)^n$ to denote the $\mathbb{F}$-linear encoder of C. For any $i \in [n]$, let $H_i \subseteq \mathbb{F}^k$ denote the $\mathbb{F}$-linear subspace such that for any message $f \in \mathbb{F}^k$, there is $\mathcal{C}(f)_i = 0$ iff $f \in H_i$. We say C is a (ℓ, A) subspace designable code if $\mathcal{H} := \{H_1, \ldots, H_n\}$ is an (ℓ, A) subspace design.

Theorem 2.4 ([GK16], as stated in [CZ25])**.** *For any $s, n \geq 1, q \geq sn \geq k$, there are explicit constructions of $\mathbb{F}_q$-linear codes $\mathcal{C} \subseteq (\mathbb{F}_q^s)^n$ such that for all $d \in \{0, 1, \ldots, s\}$, $\mathcal{C}$ is a $(d, \frac{d(k-1)}{s-d+1})$ subspace designable code. In particular, explicit folded RS codes and univariate multiplicity codes are such constructions*

We call an s-folded $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq (\mathbb{F}_q^s)^n$ with rate R **d-subspace designable** iff for all $1 \leq d' \leq d$, $\mathcal{C}$ is a $(d', Rd'n + 1)$ subspace designable code (see [BCDZ25]). Asymptotically, these parameters match the lower bound for algebraically closed fields as discussed in Remark 2.2.

We now quote a handful of results on the list recovery of various families of codes, which we use to prove Theorem 1.3 in Section 4. The first result is a recent result on reducing the list recoverability of random linear codes to the list recoverability of subspace designable codes.

Theorem 2.5 ([BCDZ25, Corollary 4.3])**.** *Fix constants $\ell, L, d \geq 1, \varepsilon, \rho, R \in (0, 1), q \geq (3\ell)^{2(L+1)/\varepsilon}$. Suppose for all large enough n, all d-subspace designable codes with rate R are (ρ, ℓ, L) list-recoverable, then random $\mathbb{F}_q$-linear codes with rate $R - (L^2 + 2L + 2)/n - \varepsilon$ are (ρ, ℓ, L) list-recoverable with probability at least $1 - o_n(1)$.*

Next, we cite a theorem on relating the list recoverability of random linear codes to the list recoverability of random Reed-Solomon codes.

Theorem 2.6 ([LMS25, Corollary 3.11], Reformulated)**.** *Fix constants $\rho \in [0, 1], L \geq \ell \geq 2$. There exists a constant c such that the following holds. For any constants $\varepsilon, R \in (0, 1)$ and prime power $q \geq 2^{c/\varepsilon} n$, if random $\mathbb{F}_q$-linear code with rate R is (ρ, ℓ, L) list-recoverable with probability at least $1 - o_n(1)$, then random RS code over $\mathbb{F}_q$ with rate $R - \varepsilon$ is (ρ, ℓ, L) list-recoverable with probability at least $1 - o_n(1)$.*

We also cite the following facts on the list recoverability of folded Reed-Solomon codes and univariate multiplicity codes.

Theorem 2.7 ([GW13, Theorem 7])**.** *For any constant $R, \varepsilon \in (0, 1), \ell \geq 2$ and $s \geq 16\ell/\varepsilon^2$, s-folded RS codes $\mathcal{C} \subseteq (\mathbb{F}_q^s)^n$ with rate $R = k/(sn)$ and appropriate evaluation points have the following property. For any received table $S_1, \times \cdots \times S_n \in \binom{\mathbb{F}_q^s}{\leq \ell}$, the set $\{f \in \mathbb{F}_q^k \colon \mathcal{C}(f) \in \mathsf{LIST}_{\mathcal{C}}(1 - R - \varepsilon, S_1 \times \cdots \times S_n)\}$ is contained in some affine subspace of $\mathbb{F}_q^k$ with dimension $4\ell/\varepsilon$.*

Theorem 2.8 ([KRZSW23, Theorem 3.7], Reformulated)**.** *For any constant $R, \varepsilon \in (0, 1), \ell \geq 2$ and $s \geq 32\ell/\varepsilon^2$, s-folded univariate multiplicity codes $\mathcal{C} \subseteq (\mathbb{F}_p^s)^n$ over prime field $p \geq sn$ with rate $R = k/(sn)$ and appropriate evaluation points have the following property. For any received table $S_1, \times \cdots \times S_n \in \binom{\mathbb{F}_p^s}{\leq \ell}$, the set $\{f \in \mathbb{F}_p^k \colon \mathcal{C}(f) \in \mathsf{LIST}_{\mathcal{C}}(1 - R - \varepsilon, S_1 \times \cdots \times S_n)\}$ is contained in some affine subspace of $\mathbb{F}_p^k$ with dimension $8\ell/\varepsilon$.*

2.2 Entropy

Given a probability distribution X over a ground set V, for each $v \in V$, we let $\Pr[X = v]$ denote the probability that v is sampled from X. We define the entropy of X to be

$$H(X) := \sum_{v \in V} \Pr[X = v] \log\left(\frac{1}{\Pr[X = v]}\right),$$

where by standard convention we assume that $0 \log(1/0) = 0$.

Given a function $f : V \to W$, we define $f(X)$ to be the distribution such that for all $w \in W$,

$$\Pr[f(X) = w] = \sum_{\substack{v \in V \\ f(v) = w}} \Pr[X = v].$$

Observe that if f is an injection, then $H(f(X)) = H(X)$.

Given a distributions X over V and Y over W (potentially correlated), we define the joint entropy $H(X, Y)$ to be

$$H(X, Y) := \sum_{v \in V} \sum_{w \in W} \Pr[X = v \wedge Y = w] \log\left(\frac{1}{\Pr[X = v \wedge Y = w]}\right),$$

Likewise, we define the conditional entropy $H(X \mid Y)$ to be

$$H(X \mid Y) = H(X, Y) - H(Y) = \sum_{v \in V} \sum_{w \in W} \Pr[X = v \wedge Y = w] \log\left(\frac{\Pr[Y = w]}{\Pr[X = v \wedge Y = w]}\right), \tag{4}$$

We also use that

$$H(X \mid Y) = \sum_{y \in W} \Pr[Y = w] H(X \mid Y = w). \tag{5}$$

2.3 Applying Brascamp–Lieb to Subspace Designs

We now prove an interface between subspace design conditions and the Brascamp-Lieb inequalities.

Proposition 2.9. *Let $\pi_1, \ldots, \pi_n : \mathbb{F}_q^k \to \mathbb{F}_q^s$ be linear maps, and let $H_i := \ker \pi_i$ for all $i \in [n]$. Assume that $H_1, \ldots, H_n$ form a $(d, \frac{d(k-1)}{s-d+1})$ subspace design for all $d \in \{0, 1, \ldots, s\}$. Let $V \subseteq \mathbb{F}_q^k$ subspace with $\dim(V) \leq s$. Then, we have that*

$$\dim(U) \leq \frac{1}{n - \frac{k-1}{s-\dim(V)+1}} \sum_{i=1}^{n} \dim(\pi_i(U)) \tag{6}$$

As such, for every probability distribution X over V, we have that

$$H(X) \leq \frac{1}{n - \frac{k-1}{s-\dim(V)+1}} \sum_{i=1}^{n} H(\pi_i(X)). \tag{7}$$

Proof. Observe from the subspace design condition that

$$\begin{aligned}\sum_{i=1}^{n} \dim(\pi_i(U)) &= n\dim(U) - \sum_{i=1}^{n} \dim(U \cap H_i) \\ &\geq n\dim(U) - \dim(U)\frac{k-1}{s-\dim(U)+1} \\ &\geq \dim(U)\left(n - \frac{k-1}{s-\dim(V)+1}\right),\end{aligned}$$

from which (6) follows. We have that (7) immediately follows from (6) and Theorem 1.6. □

3 Warm-up: Tight Analysis for Zero-error LR

To demonstrate the strength of our method, we show in the zero-error regime our results tightly match the lower bound established by Chen and Zhang [CZ25], which gives an affirmative answer to Conjecture 1.2 when the target radius $\rho^* = 0$.

Theorem 3.1. *For all $i \in [n]$, let $\pi_i : \mathbb{F}^k \to \mathbb{F}^s$ be a linear map whose kernel is H_i. Assume that $H_1, \ldots, H_n$ form a $\left(\ell, \frac{\ell(k-1)}{s-\ell+1}\right)$ subspace design for all $\ell \in \{0, 1, \ldots, s\}$. Let $C := \{(\pi_1(x), \ldots, \pi_n(x)) \mid x \in \mathbb{F}^k\}$. Then, for all $L \geq \ell \geq 2$, and integers $m \geq 1$, we have that C is $(0, \ell, L)$-list-recoverable if*

$$\frac{k-1}{n(s-L+1)} < 1 - \frac{\log \ell}{\log(L+1)}. \tag{8}$$

Proof. Assume for sake of contradiction that there exists a bad list $E \subseteq C$ of size $L+1$ such that for all $i \in [n]$, the set $\{c_i : i \in E\}$ has cardinality at most ℓ. Let $F \subseteq \mathbb{F}^k$ be the preimage of E with respect to $(\pi_1, \ldots, \pi_n)$. That is, $x \in F$ if and only if $(\pi_1(x), \ldots, \pi_n(x)) \in E$. Note that $|F| = |E| = L+1$.

By a suitable translation, we may assume that $0 \in F$ without changing the cardinality of any set $\pi_i(F)$. Let V be the linear span of F. Note that $\dim(V) \leq L$. By, Proposition 2.9, we have that for any probability distribution X over V, we have that

$$H(X) \leq \frac{1}{n - \frac{k-1}{s-L+1}} \sum_{i=1}^{n} H(\pi_i(X)).$$

Let X be the uniform distribution over F. Then, $H(X) = \log(L+1)$. Further, since $|\pi_i(F)| \leq \ell$ for all $i \in [n]$, we have that $H(\pi_i(X)) \leq \log \ell$ for all $i \in [n]$. Thus,

$$\log(L+1) \leq \frac{n}{n - \frac{k-1}{s-L+1}} \log \ell.$$

This contradicts (8), so the bad list E does not exist. □

Corollary 3.2. *For all $\varepsilon > 0$, if C as in Theorem 3.1 has rate $R \in (0,1)$ and $n, k, s = \Omega_{\ell,\varepsilon}(1)$ are sufficiently large, then C is $(0, \ell, \ell^{1/(1-R-\varepsilon)})$ list recoverable.*

Proof. Let $L := \lfloor \ell^{1/(1-R-\varepsilon)} \rfloor$ and assume that $s \geq (\frac{R}{\varepsilon}+1)(L-1)$. Then, $\frac{Rs}{s-L+1} \leq R+\varepsilon$. So, $\frac{k-1}{n(s-L+1)} < \frac{Rs}{s-L+1} \leq R+\varepsilon$. Further,

$$1 - \frac{\log \ell}{\log(L+1)} \geq 1 - \frac{\log \ell}{\log \ell^{1/(1-R-\varepsilon)}} = R+\varepsilon.$$

We have that (8) holds, so C is $(0, \ell, \ell^{1/(1-R-\varepsilon)})$ list recoverable. □

Fix any $\ell, a \geq 2$, for arbitrarily small slack $\varepsilon > 0$, we can choose any $R < \frac{a-1}{a} - \varepsilon$ and invoke the above result, this yields $(0, \ell, \ell^a - 1)$ list-recoverable. Since the rate R could be arbitrarily close to $\frac{a-1}{a}$, this gives an affirmative answer to Conjecture 1.2 in zero-error case $\rho^* = 0$.

4 Asymptotic Bound

Fix any $d \geq 1, \mu \in (0,1)$, we call an s-folded $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq (\mathbb{F}_q^s)^n$ with rate R **μ-slacked d-subspace designable** iff for any $1 \leq d' \leq d$, $\mathcal{C}$ is $(d', (R+\mu)d'n)$ subspace-designable. Note that for any constants $\mu, R > 0$, when n approaches to infinity, d-subspace designable codes are automatically μ-slacked d-subspace designable codes. Let $W(z)$ be the Lambert W function that $W(z)e^{W(z)} = z$.

Theorem 4.1. *For any $\ell, m \geq 2, L = \ell^m - 1, s, d \geq 1, \mu, R, \rho \in (0,1)$ such that the following holds*

$$\rho < 1 - \frac{R' \ln(L+1)}{W(R'(L+1)\ln(L+1)/\ell)}, \text{ where } R' = R+\mu$$

Suppose $\rho \leq 1 - \frac{\ell}{L+1}$[2]*. Let $\mathcal{C} \subseteq (\mathbb{F}_q^s)^n$ be an $\mathbb{F}_q$-linear and μ-slacked d-subspace designable code with rate $R = k/(sn)$. If for any received table $S_1, \times \cdots \times S_n \in \binom{\mathbb{F}_q^s}{\leq \ell}$, the set $\{f \in \mathbb{F}_q^k : \mathcal{C}(f) \in \mathsf{LIST}_{\mathcal{C}}(\rho, S_1 \times \cdots \times S_n)\}$ is contained in some affine subspace of $\mathbb{F}_q^k$ with dimension d, or $d \geq L$, then $\mathcal{C}$ is (ρ, ℓ, L) list-recoverable.*

Proof. Suppose by contrapositive there exist a received table $S_1, \ldots, S_n \in \binom{\mathbb{F}_q^s}{\leq \ell}$ and distinct $f_1, \ldots, f_{L+1} \in \{f \in \mathbb{F}_q^k : \mathcal{C}(f) \in \mathsf{LIST}_{\mathcal{C}}(\rho, S_1 \times \cdots \times S_n)\}$. Then, if we define $\rho_i = |\{j \in [L+1] : \mathcal{C}(f_j)[i] \in S_i\}|/(L+1)$ for each $i \in [n]$, there is $\frac{1}{n}\sum_{i=1}^n \rho_i \leq \rho$. Since S_i is allowed to picked as a set with size ℓ and the condition is an upper bound on $\sum_{i=1}^n \rho_i$. Without loss of generality we can always choose some $S_1, \ldots, S_n$ satisfying the above conditions such that $\rho_i \leq 1 - \frac{\ell}{L+1}$ for each $i \in [n]$. If $f_1 \neq 0$, we subtract f_1 from each of $f_1, \ldots, f_{L+1}$ and subtract $\mathcal{C}(f_1)[i]$ from each element of S_i for all $i \in [n]$. One can check that after these subtractions the above conditions still hold, so without loss of generality, we can always assume $f_1 = 0$.

For any $i \in [n]$, let $H_i \subseteq \mathbb{F}_q^k$ denote the $\mathbb{F}_q$-linear subspace such that for any message $f \in \mathbb{F}_q^k$, there is $\mathcal{C}(f)_i = 0$ iff $f \in H_i$. Let $V = \mathrm{Span}(f_1, \ldots, f_{L+1})$, and $s_1, \ldots, s_n = \frac{1}{(1-R-\mu)n}$. For each $i \in [n]$ let $\pi_i : V \to V/(V \cap H_i)$ denote the natural linear map from V to its quotient space. From the statement we know $\dim(V) \leq d$ Now we check that these choices satisfy (1) so we can invoke Theorem 1.6. For any linear subspace $U \subseteq V$, we aim to prove that

$$\dim(U) \leq \sum_{i=1}^n s_i \dim(\pi_i(U)).$$

[2] If $\rho > 1 - \frac{\ell}{L+1}$, then any code cannot be (ρ, ℓ, L) list-recoverable, so this condition does not weaken our result.

The above inequality is equivalent to

$$(1-R-\mu)n\dim(U) \le \sum_{i=1}^{n}(\dim(U)-\dim(U\cap H_i))$$
$$\Leftrightarrow \sum_{i=1}^{n}\dim(U\cap H_i) \le (R+\mu)n\dim(U).$$

This inequality follows since $\mathcal{C}$ is μ-slacked d-subspace designable and $\dim(U) \le \dim(V) \le d$.

Let X be the uniform distribution over $f_1, \ldots, f_{L+1} \in V$, from Theorem 1.6 we know that

$$(1-R')n\ln(L+1) = (1-R-\mu)nH(X) \le \sum_{i=1}^{n} H(\pi_i(X)).$$

Fix any $i \in [n]$, we know that for $a \neq b \in [L+1]$, if $\mathcal{C}(f_a)[i] = \mathcal{C}(f_b)[i]$, then there must be $\mathcal{C}(f_a - f_b)[i] = 0$ and therefore $f_a - f_b \in H_i \cap V$ which implies $\pi_i(f_a) = \pi_i(f_b)$. Let $E_i \in \{0,1\}$ denote the indicator event that $E_i = [\mathcal{C}(X)[i] \in T_i]$. Recall the definition of ρ_i that $\Pr[E_i] = 1-\rho_i$, let $h(\cdot)$ denote the binary entropy function, by chain rule (see (4) and (5)) we know that

$$\begin{aligned} H(\pi_i(X)) &= H(\pi_i(X), E_i) \\ &= H(E_i) + H(\pi_i(X) \mid E_i) \\ &\le h(\rho_i) + (1-\rho_i)\ln\ell + \rho_i \ln(\rho_i(L+1)) \\ &= (1-\rho_i)\ln\ell + \rho_i\ln(L+1) - (1-\rho_i)\ln(1-\rho_i) \end{aligned} \tag{9}$$

Let $g(x) = (1-x)\ln\ell + x\ln(L+1) - (1-x)\ln(1-x)$, by direct calculation, we know that $g'(x) = \ln(\frac{L+1}{\ell}) + 1 + \ln(1-x)$, $g''(x) = -\frac{1}{1-x}$. When $x \in [0, 1-\frac{\ell}{L+1}]$, we know that $g'(x) > 0$ and $g''(x) < 0$. This implies $g(x)$ is concave and monotone increasing in this range. Therefore, recall that $\rho, \rho_1, \ldots, \rho_n \in [0, 1-\frac{\ell}{L+1}]$. Since $\sum_{i=1}^{n}\rho_i \le \rho n$, we know that

$$\sum_{i=1}^{n} H(\pi_i(X)) \le \sum_{i=1}^{n} g(\rho_i) \le ng(\rho) = n((1-\rho)\ln\ell + \rho\ln(L+1) - (1-\rho)\ln(1-\rho)).$$

Therefore, it follows that

$$(1-R')\ln(L+1) \le (1-\rho)\ln\ell + \rho\ln(L+1) - (1-\rho)\ln(1-\rho).$$

Rearrange this inequality, it follows that

$$R'\ln(L+1) \ge (1-\rho)\ln\frac{(1-\rho)(L+1)}{\ell}$$

Let $t = 1-\rho \ge \frac{\ell}{L+1}$, it implies that

$$R'\ln(L+1) \ge t\ln t + t\ln\frac{(L+1)}{\ell}.$$

Let $h = \frac{t(L+1)}{\ell} \ge 1$, we know that

$$\frac{R'(L+1)\ln(L+1)}{\ell} \ge h\ln h$$

Let $C = \frac{R'(L+1)\ln(L+1)}{\ell} > 0$ and $h' = \exp(W(C))$. From the definition of Lambert W function we know $h' \ln h' = C > 0$ so $h' > 1$. Since $h \ln h$ is increasing with respect to $h \geq 1$, the above inequality implies $h \leq h'$. However, we can compute that

$$h = \frac{(1-\rho)(L+1)}{\ell} > C/W(C) = h'$$

This is a contradiction, so we complete the proof. □

Theorem 4.2. *For any $\ell \geq 2, d \geq 1, \varepsilon \in (0,1)$, let $L = \left(\frac{\ell}{R+\varepsilon/2}\right)^{3+2R/\varepsilon}$. Let $\mathcal{C} \subseteq (\mathbb{F}_q^s)^n$ be an $\mathbb{F}_q$-linear and $\varepsilon/3$-slacked d-subspace designable code with rate $R = k/(sn)$. If for any received table $S_1, \times \cdots \times S_n \in \binom{\mathbb{F}_q^s}{\leq \ell}$, the set $\{f \in \mathbb{F}_q^k \colon \mathcal{C}(f) \in \mathsf{LIST}_{\mathcal{C}}(1-R-\varepsilon, S_1 \times \cdots \times S_n)\}$ is contained in some affine subspace of $\mathbb{F}_q^k$ with dimension d, or $d \geq L$, then $\mathcal{C}$ is $(1-R-\varepsilon)$ list-recoverable.*

Proof. We set $\mu = \varepsilon/3$ and $R' = R + \mu$. It suffices to find $m \geq 2$ such that $\ell^m \leq L$ and $\rho = 1 - \frac{R'm\ln\ell}{W(R'm\ell^{m-1}\ln\ell)} - \varepsilon/6 \geq 1 - R - \varepsilon = 1 - R' - 2\varepsilon/3$ and then invoke Theorem 4.1 to get the bound. Then we calculate a valid choice of m.

Let $K = R' + \varepsilon/2$, then we need $K \geq \frac{R'm\ln\ell}{W(R'm\ell^{m-1}\ln\ell)}$, so $W(R'm\ell^{m-1}\ln\ell) \geq \frac{R'm\ln\ell}{K}$.

Since $W(z)e^{W(z)} = z$ and $\frac{R'm\ln\ell}{K} > 0$. Since xe^x is monotone increasing when $x > 0$, this implies $\frac{R'm\ln\ell}{K}\exp(\frac{R'm\ln\ell}{K}) \leq R'm\ell^{m-1}\ln\ell$. It follows that

$$\ell^{m-1} \geq \frac{1}{R'+\varepsilon/2}\exp(\frac{R'm\ln\ell}{R'+\varepsilon/2}) \Rightarrow \ell^m \geq \frac{\ell}{R'+\varepsilon/2}\exp(m\ln\ell(1-\frac{\varepsilon/2}{R'+\varepsilon/2}))$$

Therefore, it is necessary to have

$$\ell^m \geq (\frac{\ell}{R'+\varepsilon/2})^{(R'+\varepsilon/2)/(\varepsilon/2)}$$

The above inequality is satisfied when we choose m such that

$$\ell^m \geq (\frac{\ell}{R+\varepsilon/2})^{2+2R/\varepsilon}$$

It follows that there must be a valid choice of m satisfying the above condition and $\ell^m \leq L$. □

We now use Theorem 4.2 to bound the list recovery of the families of codes mentioned in Theorem 1.3. We start with random linear codes.

Corollary 4.3. *For constants $\ell \geq 2, R, \varepsilon \in (0,1), L = (\frac{\ell}{R+\varepsilon/2})^{5+4R/\varepsilon}, q \geq (3\ell)^{6(L+1)/\varepsilon}$, random $\mathbb{F}_q$-linear codes with rate R are $(1-R-\varepsilon, \ell, L)$ list-recoverable with probability at least $1 - o_n(1)$.*

Proof. Let $d = L$, from Theorem 4.2, any $\varepsilon/6$-slacked d-subspace designable code with rate $R + \varepsilon/2$ is $(1-R-\varepsilon, \ell, L)$ list-recoverable. Since $\varepsilon > 0$ is a constant, when n approaches to infinity any d-subspace designable codes is a $\varepsilon/6$-slacked d-subspace designable code. Therefore, for large enough n, any d-subspace designable code with rate $R + \varepsilon/2$ is $(1-R-\varepsilon, \ell, L)$ list-recoverable. Then, by Theorem 2.5, for all large enough n, random $\mathbb{F}_q$-linear code codes with rate $R + \varepsilon/2 - \varepsilon/3 - (L^2+2L+2)/n = R + \varepsilon/6 - o_n(1) \geq R$ is $(1-R-\varepsilon, \ell, L)$ list-recoverable with probability at least $1 - o_n(1)$. □

Next, we prove Theorem 1.3 for random Reed-Solomon codes.

Corollary 4.4. *For constants $\ell \geq 2, R, \varepsilon \in (0,1), L = (\frac{\ell}{R+\varepsilon/2})^{9+8R/\varepsilon}$, there exists a constant c such that for any prime power $q \geq cn$, random RS codes over $\mathbb{F}_q$ with rate R are $(1-R-\varepsilon, \ell, L)$ list-recoverable with probability at least $1 - o_n(1)$.*

Proof. By Corollary 4.3, there exists a constant C such that for any prime power $q > C$, random $\mathbb{F}_q$-linear code with rate $R + \varepsilon/2$ is $(1-R-\varepsilon, \ell, L)$ list-recoverable. Then, by Theorem 2.6, there exists a constant c such that for any prime power $q \geq cn$, random RS codes over $\mathbb{F}_q$ with rate R are $(1-R-\varepsilon, \ell, L)$ list-recoverable. □

We now prove Theorem 1.3 for folded Reed-Solomon codes.

Corollary 4.5. *For constants $\ell \geq 2, R, \varepsilon \in (0,1), L = (\frac{\ell}{R+\varepsilon/2})^{3+2R/\varepsilon}, s \geq 16\ell/\varepsilon^2$, any s-folded RS code $\mathcal{C} \subseteq (\mathbb{F}_q^s)^n$ with rate $R = k/(sn)$ and appropriate evaluation points is $(1-R-\varepsilon, \ell, L)$ list-recoverable.*

Proof. Let $d = 4\ell/\varepsilon$, by Theorem 2.7, for any received table $S_1, \times \cdots \times S_n \in \binom{\mathbb{F}_q^s}{\leq \ell}$, the set $\{f \in \mathbb{F}_q^k \colon \mathcal{C}(f) \in \mathsf{LIST}_{\mathcal{C}}(1-R-\varepsilon, S_1 \times \cdots \times S_n)\}$ is contained in some affine subspace of $\mathbb{F}_q^k$ with dimension d. Now it suffices to check that $\mathcal{C}$ is a $\varepsilon/3$-slacked d subspace designable code so that we can apply Theorem 4.2 and finish the proof. For any $1 \leq d' \leq d$, we aim to prove that $\mathcal{C}$ is $(d', (R+\varepsilon/3)d'n)$ subspace designable. By Theorem 2.4, $\mathcal{C}$ is $(d', \frac{Rsd'n}{s-d'+1})$ subspace designable. By direct calculation, it follows that $\frac{Rs}{s-d'+1} \leq R + \varepsilon/3$ when $s \geq 16\ell/\varepsilon^2$ and we achieve the required parameter. □

Finally, we prove Theorem 1.3 for univariate multiplicity codes.

Corollary 4.6. *For constants $\ell \geq 2, R, \varepsilon \in (0,1), L = (\frac{\ell}{R+\varepsilon/2})^{3+2R/\varepsilon}, s \geq 32\ell/\varepsilon^2$, any s-order univariate multiplicity code $\mathcal{C} \subseteq (\mathbb{F}_p^s)^n$ over prime field $p \geq sn$ with rate $R = k/(sn)$ and appropriate evaluation points is $(1-R-\varepsilon, \ell, L)$ list-recoverable.*

Proof. By replacing Theorem 2.7 with Theorem 2.8, the proof is the same as the previous proof for Corollary 4.5. □

Remark 4.7. All these results can be generalized to a slightly stronger notion of average-radius list-recovery. However, in the above folded RS codes (Corollary 4.5) and univariate multiplicity codes (Corollary 4.6) cases, in order to reduce the folding parameter s, we used two facts Theorem 2.7 [GW13] and Theorem 2.8 [KRZSW23] that do not apply to average-radius list-recovery. Therefore, to ensure the same average-radius list-recoverability, we need a larger folding requirement $s \geq L(3R/\varepsilon + 1)$ so that explicit folded RS and univariate multiplicity codes are $\varepsilon/3$-slacked L-subspace designable codes guaranteed by Theorem 2.4.

5 Remainder Version of Brascamp–Lieb Inequality

In this section, our target is to show the Brascamp-Lieb inequality for remainder and see how it derives the main result of [CZ25].

Theorem 5.1 (Restatement of Theorem 1.7)**.** *Let V be any linear space over $\mathbb{F}_q$. Let $\pi_i \colon V \to V/W_i, i \in [n]$ denote n linear maps such that $\ker(\pi_i) = W_i \subseteq V$ satisfying the following*

$$\forall W \subseteq V, \dim(W) \leq \sum_{i=1}^{n} s_i \dim(\pi_i(W)). \tag{10}$$

Then, for any distribution $X \leftarrow V$, we know that

$$r(X) \le \sum_{i=1}^{n} s_i r(\pi_i(X)).$$

5.1 Application to List-Decoding

To gain some intuition for Theorem 5.1, we show that it implies as a corollary, a result by Chen and Zhang [CZ25] on the list decodability of folded Reed–Solomon codes. The following theorem is equivalent to [CZ25, Theorem B.5], which is a more general form of its main result.

Theorem 5.2. *For all $i \in [n]$, let $\pi_i : \mathbb{F}^k \to \mathbb{F}^s$ be a linear map whose kernel is H_i. Assume that $H_1, \dots, H_n$ form a $\left(\ell, \frac{\ell(k-1)}{s-\ell+1}\right)$ subspace design for all $\ell \in \{0, 1, \dots, s\}$. Let $C := \{(\pi_1(x), \dots, \pi_n(x)) \mid x \in \mathbb{F}^k\}$. Then, for all $L \le s$, we have that C is (ρ, L)-list-recoverable if*

$$\rho < \frac{L}{L+1}\left(1 - \frac{k-1}{n(s-L+1)}\right). \tag{11}$$

Proof. Assume for sake of contradiction that there exists a bad list $E \subseteq C$ of size $L+1$ and a point $y \in (\mathbb{F}^s)^n$ such that

$$\sum_{c \in E} \sum_{i=1}^{n} \mathbf{1}[c_i \ne y_i] \le \rho(L+1)n. \tag{12}$$

For each $i \in [n]$, let $\rho_i := \frac{1}{L+1} \sum_{c \in E} \mathbf{1}[c_i \ne y_i]$. Let $F \subseteq \mathbb{F}^k$ be the preimage of E with respect to $(\pi_1, \dots, \pi_n)$. That is, $x \in F$ if and only if $(\pi_1(x), \dots, \pi_n(x)) \in E$. Note that $|F| = |E| = L+1$.

By a suitable translation of E and F, we may assume that $0 \in F$ such that (12) still holds for a suitably translated y. Let V be the linear span of F. Note that $\dim(V) \le L$. By Theorem 5.1 and Proposition 2.9, we have that for any probability distribution X over V, we have that

$$r(X) \le \frac{1}{n - \frac{k-1}{s-L+1}} \sum_{i=1}^{n} r(\pi_i(X)).$$

Let X be the uniform distribution over F. Then, $r(X) = \frac{L}{L+1}$. Further, for all $i \in [n]$, we have that $r(\pi_i(F)) \le \rho_i$. Thus,

$$\frac{L}{L+1} \le \frac{1}{n - \frac{k-1}{s-L+1}} \sum_{i=1}^{n} \rho_i = \frac{1}{n - \frac{k-1}{s-L+1}} \cdot \frac{1}{L+1} \sum_{c \in E} \sum_{i=1}^{n} \mathbf{1}[c_i \ne x_i] \le \frac{\rho n}{n - \frac{k-1}{s-L+1}}.$$

This contradicts (11), so the bad list E does not exist. □

5.2 Proof of Theorem 5.1

We restate Theorem 5.1 as follows. Given a function $F : V \to \mathbb{R}$ and a function $\pi_i : V \to V_i$, we let $F^{/\pi_i} : V_i \to \mathbb{R}$ denote the function

$$F^{/\pi_i}(v) := F(\pi^{-1}(v)) := \sum_{u \in \pi_i^{-1}(v)} F(u).$$

It suffices to prove that if (10) holds, then for any function $F : V \to \mathbb{R}_{\geq 0}$, we have that

$$\|F\|_1 - \|F\|_\infty \leq \sum_{i=1}^{n} s_i \left[\|F\|_1 - \|F^{/\pi_i}\|_\infty \right]. \tag{13}$$

We prove this result by induction on the size of the support of F. Without loss of generality we can also assume that V is spanned by the vectors in the support of F. The base case of $|\operatorname{supp} F| \leq 1$ is trivial. Now, assume without loss of generality that $\|F\|_\infty = F(0)$. Pick a basis $v_1, \ldots, v_d$ of V such that for all $i \in [d]$, $F(v_i)$ is maximized conditioned on $v_1, \ldots, v_{i-1}$. Let $v_0 = 0$, and for all $i \in \{0, 1, \ldots, d\}$, let $U_i = \operatorname{span}\{v_0, \ldots, v_i\}$. We next decompose $F = F_0 + \cdots F_d$ such that for all $i \in \{0, 1, \ldots, d\}$,

$$F_i(v) = \begin{cases} F(v) & v \in U_i \setminus U_{i-1} \\ 0 & \text{otherwise.} \end{cases}$$

Since (10) holds, for all $i \in \{0, 1, \ldots, d\}$, we have that

$$\|F_i\|_1 - \|F_i\|_\infty \leq \sum_{j=1}^{n} s_j \left[\|F_i\|_1 - \|F_i^{/\pi_j}\|_\infty \right]. \tag{14}$$

Next, we apply (10) for $W \in \{U_0, \ldots, U_d\}$ to get[3]

$$\begin{aligned}
\sum_{i=1}^{d} F(v_i) &= \sum_{i=1}^{d} (F(v_i) - F(v_{i+1})) \dim(U_i) \\
&\leq \sum_{i=1}^{d} (F(v_i) - F(v_{i+1})) \sum_{j=1}^{n} s_j \dim(\pi_j(U_i)) \\
&= \sum_{j=1}^{n} s_j \sum_{i=1}^{d} (F(v_i) - F(v_{i+1})) \dim(\pi_j(U_i)). \\
&= \sum_{j=1}^{n} s_j \sum_{i=1}^{d} F(v_i)(\dim(\pi_j(U_i)) - \dim(\pi_j(U_{i-1}))) \\
&= \sum_{j=1}^{n} s_j \sum_{i=1}^{d} F(v_i) \mathbf{1}[v_i \notin \ker \pi_j + U_{i-1}].
\end{aligned}$$

Adding this inequality to (14) for all $i \in \{1, \ldots, d\}$, we get that

$$\begin{aligned}
\|F\|_1 - \|F\|_\infty &= \sum_{i=1}^{d} (\|F_i\|_1 - \|F_i\|_\infty) + \sum_{i=1}^{d} F(v_i) \\
&\leq \sum_{j=1}^{n} s_j \sum_{i=1}^{d} \left[\|F_i\|_1 - \|F_i^{/\pi_j}\|_\infty + F(v_i) \mathbf{1}[v_i \notin \ker \pi_j + U_{i-1}]. \right].
\end{aligned}$$

Thus, it suffices to prove for all $j \in [n]$ that

$$\sum_{i=1}^{d} \left[\|F_i\|_1 - \|F_i^{/\pi_j}\|_\infty + F(v_i) \mathbf{1}[v_i \notin \ker \pi_j + U_{i-1}]. \right] \leq \|F\|_1 - \|F^{/\pi_j}\|_\infty.$$

[3] We use the convention $F(v_{d+1}) = 0$.

Rearranging terms, we get the somewhat simpler expression

$$\sum_{i=0}^{d} F(v_i)\mathbf{1}[v_i \notin \ker \pi_j + U_{i-1}] \leq \sum_{i=0}^{d} \|F_i^{/\pi_j}\|_\infty - \|F^{/\pi_j}\|_\infty. \tag{15}$$

Let $u \in V$ be such that $F(u + \ker \pi_j) = \|F^{/\pi_j}\|_\infty$. Let $I \subseteq \{0, 1, \ldots, d\}$ be the set of indices for which $(u + \ker \pi_j) \cap (U_i \setminus U_{i-1}) \neq \phi$ (note this means if $u = 0$ then $0 \in I$). In other words, I is the leading columns of an (affine) echelon basis of $u + \ker \pi_j$. Therefore, $|I| = \dim \ker \pi_j + 1$.

Then, we can see that

$$\|F^{/\pi_j}\|_\infty = F(u + \ker \pi_j) = \sum_{i \in I} F((u + \ker \pi_j) \cap (U_i \setminus U_{i-1})) = \sum_{i \in I} F_i(u + \ker \pi_j) \leq \sum_{i \in I} \|F_i^{/\pi_j}\|_\infty$$

Furthermore, if $i \notin I$, then $F(v_i) \leq \|F_i^{/\pi_j}\|_\infty$ is a trivial bound. Thus, to show (15), it suffices to show

$$\sum_{\substack{i \in [d] \\ v_i \notin \ker \pi_j + U_{i-1}}} F(v_i) \leq \sum_{i \in \{0\} \cup [d] \setminus I} F(v_i)$$

or equivalently

$$\sum_{i \in I} F(v_i) \leq \sum_{\substack{i \in \{0\} \cup [d] \\ v_i \in \ker \pi_j + U_{i-1}}} F(v_i). \tag{16}$$

Since $F(v_0) \geq \cdots \geq F(v_d)$, it suffices to prove (16) when $F(v_0) = \cdots = F(v_a) = 1$ and $F(v_{a+1}) = \cdots = F(v_d) = 0$ for some $a \in \{0, 1, \ldots, d\}$.

In this setting, the LHS of (16) equals $\operatorname{affdim}(W \cap (u + \ker \pi_j))$ where $W := \operatorname{affspan}\{v_0, \ldots, v_a\} = \operatorname{span}\{v_1, \ldots, v_j\}$. The RHS of (16) is $1 + \dim(W \cap (\ker \pi_j))$ (the extra one is because of $v_0 = 0$).

Hence, to prove (16), we want to show that $\operatorname{affdim}(W \cap (u + \ker \pi_j))$ is upper bounded by $1 + \dim(W \cap (\ker \pi_j))$ which is immediate (one vector can be used to shift $W \cap (u + \ker \pi_j)$ to the origin and the resulting subspace is contained in $W \cap (\ker \pi_j)$). This complete the proof of Theorem 5.1.

6 Self-contained Proof of Theorem 1.6

The majority of the machinery used by [CDK+13, CCE09] to prove Theorem 1.6 is unnecessary. In this section, we give a streamlined proof of Theorem 1.6.

We prove Theorem 1.6 by a double induction on d (the dimension of V) and m. The base case of $d = 0$ is trivial, as a 0-dimensional vector space is a singleton, and the entropy of any probability distribution over that vector space must be zero.

For $d = 1$, note that each map $\pi_i : V \to V_i$ is either an injection or the zero map. In the former case, $H(\pi_i(X)) = H(X) = \dim(\pi_i(V))H(X)$. While in the latter case, $H(\pi_i(X)) = 0 = \dim(\pi_i(V))H(X)$. If we multiply (1) with $U = V$ by $H(X)$, we then get that

$$H(X) \leq \sum_{i=1}^{m} s_i \dim(\pi_i(V))H(X) = \sum_{i=1}^{m} s_i H(\pi_i(X)),$$

as desired.

We now assume $d \geq 2$ and that Theorem 1.6 holds for all dimensions strictly less than d. For this fixed value of d, we perform an induction on m. We first handle the base case of $m = 1$. In order for (1) for $U = \ker \pi_1$ to hold, we need that $\dim(\ker \pi_1) = 0$. Thus, π_1 is an injection. Further, for (1) to hold for $U = V$, we must have that $s_1 \geq 1$. Then, observe that $H(X) = H(\pi_1(X)) \leq s_1 H(\pi_1(X))$, as desired.

Now assume that $m \geq 2$. To avoid degenerate situations, make two further assumptions.

- All scalars s_i are positive; else we can reduce to a smaller m by deleting i.
- All maps π_i are nonzero. If π_i is the zero map, then $\dim(\pi_i(U)) = 0$ for all $U \subseteq V$ and $H(\pi_i(X)) = 0$ for any distribution X over V, so we may delete i, reducing to a smaller m.

We say that (1) is *critical* (see [BCCT08, BCCT05]) at U if the two sides of the inequality are equal. Note that (1) is always critical at $U = 0$. Consider the possibility that (1) is not critical for every nonzero $U \subseteq V$. In that case, there exist $s'_1, \ldots, s'_m \geq 0$ such that the following three properties hold.

1. $s'_i \leq s_i$ for all $i \in [m]$.
2. (1) holds for $(s'_1, \ldots, s'_m)$.
3. (1) is critical $(s'_1, \ldots, s'_m)$ at some nonzero $U \subseteq V$.

Since entropy is nonnegative, proving Theorem 1.6 for $(s'_1, \ldots, s'_m)$ implies Theorem 1.6 for $(s_1, \ldots, s_m)$. Therefore, we may without loss of generality assume that some nonzero $W \subseteq V$ is critical for $(s_1, \ldots, s_m)$. We next split into cases based on which subspace is critical.

6.1 Nonzero $W \subsetneq V$ Is Tight

Note that (1) holds for all $U \subseteq W$. Since $\dim(W) < \dim(V)$, we have by the induction hypothesis that for all distributions Y over W, we have that

$$H(Y) \leq \sum_{i=1}^{m} s_i H(\pi_i(Y)). \tag{17}$$

Let V/W be the $\dim(V) - \dim(W)$-dimensional vector space $\{v + W : v \in V\}$. For every $i \in [m]$, we can define $\psi_i : V/W \to V_i/\pi_i(W)$ as

$$\psi_i(v + W) = \pi_i(v) + \pi_i(W).$$

Every of V/W is of the form $(U + W)/W$ for some $U \subseteq V$. We then calculate that

$$\begin{aligned}
\sum_{i=1}^{m} s_i \dim(\psi_i((U+W)/W)) &= \sum_{i=1}^{m} s_i \left[\dim(\pi_i(U+W)/\pi_i(W))\right] \\
&= \sum_{i=1}^{m} s_i \dim(\pi_i(U+W)) - \sum_{i=1}^{m} s_i \dim(\pi_i(W)) \\
&\geq \dim(U+W) - \dim(W) \\
&= \dim((U+W)/W),
\end{aligned}$$

where the third line uses (1) and the fact that it is critical at W. Since $\dim(V)-\dim(W) < \dim(V)$, by the induction hypothesis, we have that for all distributions Z over V/W, we have that

$$H(Z) \leq \sum_{i=1}^{m} s_i H(\psi_i(Z)). \tag{18}$$

We now show how (17) and (18) imply (2).

Given our distribution X over V, we define $X_{/W}$ to be the distribution over V/W defined to be

$$\Pr[X_{/W} = v + W] = \Pr[X \in v + W] = \sum_{w \in W} \Pr[X = v + w].$$

For each $v + W \in V/W$, we further define X_{v+W} to be the distribution over W defined by

$$\Pr[X_{v+W} = w] = \frac{\sum_{w' \in W} \Pr[X = v + w']}{\Pr[X \in v + W]}$$

if $\Pr[X \in v + W] > 0$. Otherwise, we define X_{v+W} to be the uniform distribution over W. We now give a crucial entropy inequality

Proposition 6.1. *For any linear map $\pi : V \to V'$ with corresponding map $\psi : V/W \to V'/\pi(W)$, we have that*

$$H(\pi(X)) \geq H(\psi(X_{/W})) + \sum_{v+W \in V/W} \Pr[X \in v + W] H(\pi(X_{v+W})), \tag{19}$$

with equality when π is an injection.

Proof. Assume that X and $X_{/W}$ are correlated so that if X samples v, then $X_{/W}$ samples $v + W$. In that case, since $\psi(v + W) = \pi(v) + \pi(W)$, we have that $\pi(X)$ determines $\psi(X_{/W})$. That is, $H(\psi(X_{/W}) \mid \pi(X)) = 0$. Thus,

$$\begin{aligned}
H(\pi(X)) - H(\psi(X_{/W})) &= H(\pi(X), \psi(X_{/W})) - H(\psi(X_{/W}) \mid \pi(X)) - H(\psi(X_{/W})) \\
&= H(\pi(X), \psi(X_{/W})) - H(\psi(X_{/W})) \\
&= H(\pi(X) \mid \psi(X_{/W})) \\
&\geq H(\pi(X) \mid X_{/W}) \\
&= \sum_{v+W \in V/W} \Pr[X_{/W} = v + W] H(\pi(X) \mid X_{/W} = v + W) \\
&= \sum_{v+W \in V/W} \Pr[X \in v + W] H(\pi(X) \mid X \in v + W) \\
&= \sum_{v+W \in V/W} \Pr[X \in v + W] H(\pi(X_{v+W})),
\end{aligned}$$

where for the last line if $\Pr[X \in v + W] = 0$, then equality holds no matter what X_{v+W} is defined to be. Note that if π is an injection, then ψ is an injection so $H(\pi(X) \mid \psi(X_{/W})) = H(\pi(X) \mid X_{/W})$, rendering (19) an equality. □

To finish this case, we observe by Proposition 6.1 that

$$\begin{aligned}\sum_{i=1}^{m} s_i H(\pi_i(X)) &\geq \sum_{i=1}^{m} s_i \left[H(\psi_i(X_{/W})) + \sum_{v+W \in V/W} \Pr[X \in v+W] H(\pi_i(X_{v+W})) \right] \\ &= \sum_{i=1}^{m} s_i H(\psi_i(X_{/W})) + \sum_{v+W \in V/W} \Pr[X \in v+W] \sum_{i=1}^{m} s_i H(\pi_i(X_{v+W})) \\ &\geq H(X_{/W}) + \sum_{v+W \in V/W} \Pr[X \in v+W] H(X_{v+W}) \\ &= H(X),\end{aligned}$$

where the third line uses (17) and (18), and the last line used the equality case of Proposition 6.1 when $\pi : V \to V$ is the identity map.

6.2 Only V Is Tight

Here, we reduce to a case in which some other $W \subsetneq V$ is also critical. Let $d_{m-1} = \dim(\pi_{m-1}(V))$ and $d_m = \dim(\pi_m(V))$. By our aforementioned assumptions, we have that $d_{m-1}, d_m \geq 1$. Now consider the maps $s'_{m-1}, s'_m : [0,1] \to \mathbb{R}_{\geq 0}$ as follows

$$\begin{aligned}s'_{m-1}(t) &= \left(s_{m-1} + \frac{d_m}{d_{m-1}} s_m \right)(1-t) \\ s'_m(t) &= \left(\frac{d_{m-1}}{d_m} s_{m-1} + s_m \right) t.\end{aligned}$$

Observe that, for all $t \in [0,1]$, we have that

$$s'_{m-1}(t) d_{m-1} + s'_m(t) d_m = (d_{m-1} s_{m-1} + d_m s_m)(1-t) + (d_{m-1} s_{m-1} + d_m s_m) t = d_{m-1} s_{m-1} + d_m s_m.$$

Let $\vec{s}(t) = (s_1, s_2, \ldots, s_{m-2}, s'_{m-1}(t), s'_m(t))$. We have by the above calculation (1) is critical for $\vec{s}(t)$ at V for all $t \in [0,1]$. Further observe at $t_0 = \frac{s_m}{\frac{d_{m-1}}{d_m} s_{m-1} + s_m} \in (0,1)$, we have that $(s'_{m-1}(t_0), s'_m(t_0)) = (s_{m-1}, s_m)$. Thus, we seek to prove (2) at $\vec{s}(t_0)$.

Let $t_- \in [0,1]$ be the minimum $t \in [0,1]$ for which (1) holds at $\vec{s}(t)$ for all $U \subseteq V$. Note that $t_- < t_0$ as (1) is not critical at any $U \subsetneq V$. Likewise, we define $t_+ \in [0,1]$ to be the maximum $t \in [0,1]$ for which (1) holds at $\vec{s}(t)$ for all $U \subseteq V$. We have that $t_+ > t_0$.

We claim that (2) holds at $\vec{s}(t_-)$ and $\vec{s}(t_+)$. If $t_- = 0$, then note that $s'_m(t_-) = 0$, so $\vec{s}(t_-)$ has support size at most $m-1$. Therefore (2) holds at $\vec{s}(t_-)$ by our induction hypothesis on m. Otherwise, $t_- > 0$, so there exists nonzero $W \subsetneq V$ for which (1) is critical at W for $\vec{s}(t_-)$. In that case, (2) holds at $\vec{s}(t_-)$ by the argument in Section 6.1. By similar logic, (2) holds at $\vec{s}(t_+)$.

To finish, we seek to prove (2) at $\vec{s}(t_0)$, but note that since $t_0 \in [t_-, t_+]$, we have that $\vec{s}(t_0)$ is a convex combination of $\vec{s}(t_-)$ and $\vec{s}(t_+)$. Thus, by taking a convex combination of (2) at $\vec{s}(t_-)$ and $\vec{s}(t_+)$, we prove (2) at $\vec{s}(t_0) = (s_1, \ldots, s_m)$, as desired.

Remark 6.2. We remark the high-level structure of the proof of Theorem 1.6 (particularly the recursion on a critical subspace) has a striking resemblance to the proofs of the GM-MDS theorem on the generating matrix zero patterns of Reed-Solomon codes [YH19, Lov21] (see also [BDG24]).

Acknowledgments

We thank Mahdi Cheraghchi, Sivakanth Gopi, Venkatesan Guruswami, and Madhur Tulsiani for helpful discussions and encouragement.

Joshua Brakensiek was partially supported by (Venkatesan Guruswami's) Simons Investigator award and National Science Foundation grants No. CCF-2211972 and No. DMS-2503280. Yeyuan Chen was partially supported by the National Science Foundation grant No. CCF-2236931. Zihan Zhang was partially supported by the National Science Foundation grant No. CCF-2440926.

References

[AEL95] Noga Alon, Jeff Edmonds, and Michael Luby. Linear time erasure codes with nearly optimal recovery. In *Proceedings of IEEE 36th Annual Foundations of Computer Science*, pages 512–519. IEEE, 1995. (cit. on p. 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*, oct 3 2025. doi:10.19086/aic.2025.8. (cit. on p. 2)

[AGL24] Omar Alrabiah, Venkatesan Guruswami, and Ray Li. Randomly punctured reed–solomon codes achieve list-decoding capacity over linear-sized fields. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 1458–1469, 2024. (cit. on p. 2)

[AS97] Sanjeev Arora and Madhu Sudan. Improved low-degree testing and its applications. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 485–495, 1997. (cit. on p. 1)

[BCCT05] Jonathan Bennett, Anthony Carbery, Michael Christ, and Terence Tao. Finite bounds for holder-brascamp-lieb multilinear inequalities. *arXiv preprint math/0505691*, 2005. (cit. on p. 6, 7, 19)

[BCCT08] Jonathan Bennett, Anthony Carbery, Michael Christ, and Terence Tao. The brascamp–lieb inequalities: finiteness, structure and extremals. *Geometric and Functional Analysis*, 17(5):1343–1415, 2008. (cit. on p. 6, 7, 19)

[BCDZ25] Joshua Brakensiek, Yeyuan Chen, Manik Dhar, and Zihan Zhang. From random to explicit via subspace designs with applications to local properties and matroids. 2025. (cit. on p. 4, 5, 6, 9)

[BDG24] Joshua Brakensiek, Manik Dhar, and Sivakanth Gopi. Generalized GM-MDS: Polynomial Codes Are Higher Order MDS. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 728–739, Vancouver BC Canada, June 2024. ACM. doi:10.1145/3618260.3649637. (cit. on p. 21)

[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)*, pages 1488–1501, 2023. (cit. on p. 2)

[BJ22] Jonathan Bennett and Eunhee Jeong. Fourier duality in the brascamp–lieb inequality. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 173, pages 387–409. Cambridge University Press, 2022. (cit. on p. 6)

[BL76] Herm Jan Brascamp and Elliott H Lieb. Best constants in young's inequality, its converse, and its generalization to more than three functions. *Advances in Mathematics*, 20(2):151–173, 1976. (cit. on p. 6)

[BSW23] Mario Berta, David Sutter, and Michael Walter. Quantum brascamp–lieb dualities. *Communications in Mathematical Physics*, 401(2):1807–1830, 2023. (cit. on p. 6)

[BT24] Jonathan Bennett and Terence Tao. Adjoint brascamp–lieb inequalities. *Proceedings of the London Mathematical Society*, 129(4):e12633, 2024. (cit. on p. 6)

[CCE09] 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, 2009. (cit. on p. 5, 6, 18)

[CCSZ25] Yeyuan Chen, Mahdi Cheraghchi, King-Siong Si, and Zihan Zhang. Evidence toward a conjecture in list recoverability of folded reed–solomon codes. *Manuscript*, 2025. (cit. on p. 4)

[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. (cit. on p. 5, 6, 7, 18)

[CDK+24] Michael Christ, James Demmel, Nicholas Knight, Thomas Scanlon, and Katherine Yelick. On multilinear inequalities of hölder-brascamp-lieb type for torsion-free discrete abelian groups. *Journal of Logic and Analysis*, 16, 2024. (cit. on p. 6, 7)

[Chr13] Michael Christ. The optimal constants in holder-brascamp-lieb inequalities for discrete abelian groups. *arXiv preprint arXiv:1307.8442*, 2013. (cit. on p. 6)

[CPS99] Jin-Yi Cai, Aduri Pavan, and D. Sivakumar. On the hardness of permanent. In *STACS 1999*, pages 90–99, 1999. doi:10.1007/3-540-49116-3_8. (cit. on p. 1)

[CZ25] Yeyuan Chen and Zihan Zhang. Explicit folded reed-solomon and multiplicity codes achieve relaxed generalized singleton bounds. In Michal Koucký and Nikhil Bansal, editors, *Proceedings of the 57th Annual ACM Symposium on Theory of Computing, STOC 2025, Prague, Czechia, June 23-27, 2025*, pages 1–12. ACM, 2025. doi:10.1145/3717823.3718114. (cit. on p. 2, 3, 4, 5, 7, 8, 9, 11, 15, 16)

[DR16] James Demmel and Alex Rusciano. Parallelepipeds obtaining hbl lower bounds. *arXiv preprint arXiv:1611.05944*, 2016. (cit. on p. 6)

[DW22] Dean Doron and Mary Wootters. High-probability list-recovery, and applications to heavy hitters. In *49th International Colloquium on Automata, Languages, and Programming (ICALP)*, volume 229 of *LIPIcs*, pages 55:1–55:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. (cit. on p. 2)

[Eli57] Peter Elias. List decoding for noisy channels. *Wescon Convention Record, Part 2, Institute of Radio Engineers*, pages 99–104, 1957. (cit. on p. 1)

[FSG23] Cole Franks, Tasuku Soma, and Michel X Goemans. Shrunk subspaces via operator sinkhorn iteration. In *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1655–1668. SIAM, 2023. (cit. on p. 6)

[GGOW20] Ankit Garg, Leonid Gurvits, Rafael Oliveira, and Avi Wigderson. Operator scaling: theory and applications. *Foundations of Computational Mathematics*, 20(2):223–290, 2020. (cit. on p. 6)

[GI01] Venkatesan Guruswami and Piotr Indyk. Expander-based constructions of efficiently decodable codes. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 658–667. IEEE Computer Society, 2001. (cit. on p. 2)

[GK16] Venkatesan Guruswami and Swastik Kopparty. Explicit subspace designs. *Combinatorica*, 36(2):161–185, 2016. (cit. on p. 3, 6, 8, 9)

[GL89] Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In *STOC 1989*, pages 25–32, 1989. doi:10.1145/73007.73010. (cit. on p. 1)

[GLM+22] Venkatesan Guruswami, Ray Li, Jonathan Mosheiff, Nicolas Resch, Shashwat Silas, and Mary Wootters. Bounds for list-decoding and list-recovery of random linear codes. *IEEE Trans. Inf. Theory*, 68(2):923–939, 2022. doi:10.1109/TIT.2021.3127126. (cit. on p. 3)

[GLS+24] Zeyu Guo, Ray Li, Chong Shangguan, Itzhak Tamo, and Mary Wootters. Improved list-decodability and list-recoverability of Reed–Solomon codes via tree packings. *SIAM Journal on Computing*, 53(2):389–430, 2024. (cit. on p. 2)

[GR06] Venkatesan Guruswami and Atri Rudra. Explicit capacity-achieving list-decodable codes. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing*, page 1–10, 2006. (cit. on p. 2, 3)

[GS01] Venkatesan Guruswami and Madhu Sudan. Extensions to the Johnson bound. 2001. URL: https://api.semanticscholar.org/CorpusID:9865945. (cit. on p. 2)

[GST22] Eitan Goldberg, Chong Shangguan, and Itzhak Tamo. List-decoding and list-recovery of Reed–Solomon codes beyond the Johnson radius for every rate. *IEEE Transactions on Information Theory*, 69(4):2261–2268, 2022. (cit. on p. 2)

[Gur01] Venkatesan Guruswami. *List decoding of error correcting codes*. PhD thesis, Massachusetts Institute of Technology, 2001. URL: http://dspace.mit.edu/handle/1721.1/8700. (cit. on p. 2, 3)

[GUV09] Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *Journal of the ACM*, 56(4):1–34, 2009. (cit. on p. 2)

[GW13] Venkatesan Guruswami and Carol Wang. Linear-algebraic list decoding for variants of reed–solomon codes. *IEEE Transactions on Information Theory*, 59(6):3257–3268, 2013. (cit. on p. 2, 3, 4, 9, 15)

[GX13] Venkatesan Guruswami and Chaoping Xing. List decoding reed-solomon, algebraic-geometric, and gabidulin subcodes up to the singleton bound. In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*, pages 843–852, 2013. (cit. on p. 3)

[GZ23] Zeyu Guo and Zihan Zhang. Randomly punctured reed-solomon codes achieve the list decoding capacity over polynomial-size alphabets. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 164–176. IEEE, 2023. (cit. on p. 2)

[INR10] Piotr Indyk, Hung Q Ngo, and Atri Rudra. Efficiently decodable non-adaptive group testing. In *Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete Algorithms*, pages 1126–1142. SIAM, 2010. (cit. on p. 2)

[JS25] Fernando Granha Jeronimo and Nikhil Shagrithaya. Probabilistic guarantees to explicit constructions: Local properties of linear codes. *arXiv preprint arXiv:2510.06185*, 2025. (cit. on p. 3)

[Kop15] Swastik Kopparty. List-decoding multiplicity codes. *Theory of Computing*, 11(1):149–182, 2015. (cit. on p. 3)

[Kra03] Victor Yu Krachkovsky. Reed-Solomon codes for correcting phased error bursts. *IEEE Transactions on Information Theory*, 49(11):2975–2984, 2003. (cit. on p. 3)

[KRZSW18] Swastik Kopparty, Noga Ron-Zewi, Shubhangi Saraf, and Mary Wootters. Improved decoding of folded reed-solomon and multiplicity codes. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 212–223. IEEE, 2018. (cit. on p. 2, 3, 4)

[KRZSW23] Swastik Kopparty, Noga Ron-Zewi, Shubhangi Saraf, and Mary Wootters. Improved list decoding of folded Reed-Solomon and multiplicity codes. *SIAM Journal on Computing*, 52(3):794–840, 2023. (cit. on p. 2, 3, 4, 9, 15)

[KTS22] Itay Kalev and Amnon Ta-Shma. Unbalanced expanders from multiplicity codes. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2022)*, pages 12–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2022. (cit. on p. 2)

[LMS25] Matan Levi, Jonathan Mosheiff, and Nikhil Shagrithaya. Random reed-solomon codes and random linear codes are locally equivalent, 2025. URL: https://arxiv.org/abs/2406.02238, arXiv:2406.02238. (cit. on p. 2, 3, 7, 8, 9)

[LNNT16] Kasper Green Larsen, Jelani Nelson, Huy L. Nguyen, and Mikkel Thorup. Heavy hitters via cluster-preserving clustering. In *2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 61–70, 2016. doi:10.1109/FOCS.2016.16. (cit. on p. 2)

[Lov21] Shachar Lovett. Sparse MDS Matrices over Small Fields: A Proof of the GM-MDS Conjecture. *SIAM Journal on Computing*, 50(4):1248–1262, January 2021. doi:10.1137/20M1323345. (cit. on p. 7, 21)

[LP20] Ben Lund and Aditya Potukuchi. On the list recoverability of randomly punctured codes. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms (APPROX/RANDOM)*, volume 176 of *LIPIcs*, pages 30:1–30:11. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. (cit. on p. 2)

[LS25] Ray Li and Nikhil Shagrithaya. Near-optimal list-recovery of linear code families. In Alina Ene and Eshan Chattopadhyay, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2025, August 11-13, 2025, Berkeley, CA, USA*, volume 353 of *LIPIcs*, pages 53:1–53:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2025. URL: https://doi.org/10.4230/LIPIcs.APPROX/RANDOM.2025.53, doi:10.4230/LIPICS.APPROX/RANDOM.2025.53. (cit. on p. 2, 3, 4)

[NPR11] Hung Q Ngo, Ely Porat, and Atri Rudra. Efficiently decodable error-correcting list disjunct matrices and applications. In *International Colloquium on Automata, Languages, and Programming*, pages 557–568. Springer, 2011. (cit. on p. 2)

[Res20] Nicolas Resch. *List-decodable codes:(randomized) constructions and applications*. PhD thesis, Carnegie Mellon University, 2020. URL: http://reports-archive.adm.cs.cmu.edu/anon/anon/home/ftp/2020/CMU-CS-20-113.pdf. (cit. on p. 2, 8)

[RV25] Nicolas Resch and S. Venkitesh. List Recoverable Codes: The Good, the Bad, and the Unknown (hopefully not Ugly). (arXiv:2510.07597), October 2025. arXiv:2510.07597, doi:10.48550/arXiv.2510.07597. (cit. on p. 2, 4)

[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*, pages 764–773, 2014. (cit. on p. 2)

[RW18] Atri Rudra and Mary Wootters. Average-radius list-recoverability of random linear codes. In Artur Czumaj, editor, *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2018, New Orleans, LA, USA, January 7-10, 2018*, pages 644–662. SIAM, 2018. doi:10.1137/1.9781611975031.42. (cit. on p. 2, 3, 4)

[Sri25] Shashank Srivastava. Improved list size for folded reed-solomon codes. In *Proceedings of the 2025 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 2040–2050. SIAM, 2025. (cit. on p. 3, 4)

[ST23] Chong Shangguan and Itzhak Tamo. Generalized Singleton Bound and List-Decoding Reed–Solomon Codes Beyond the Johnson Radius. *SIAM Journal on Computing*, 52(3):684–717, June 2023. doi:10.1137/20M138795X. (cit. on p. 2, 5)

[ST25] Shashank Srivastava and Madhur Tulsiani. List decoding expander-based codes up to capacity in near-linear time. *CoRR*, abs/2504.20333, 2025. URL: https://doi.org/10.48550/arXiv.2504.20333, arXiv:2504.20333, doi:10.48550/ARXIV.2504.20333. (cit. on p. 3, 8)

[STV99] Madhu Sudan, Luca Trevisan, and Salil Vadhan. Pseudorandom generators without the xor lemma. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, pages 537–546, 1999. (cit. on p. 1)

[Tam24] Itzhak Tamo. Tighter list-size bounds for list-decoding and recovery of folded reed-solomon and multiplicity codes. *IEEE Trans. Inf. Theory*, 70(12):8659–8668, 2024. doi:10.1109/TIT.2024.3402171. (cit. on p. 2, 3, 4)

[Tre99] Luca Trevisan. Construction of extractors using pseudo-random generators. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, pages 141–148, 1999. (cit. on p. 2)

[TSU12] Amnon Ta-Shma and Christopher Umans. Better condensers and new extractors from parvaresh-vardy codes. In *2012 IEEE 27th Conference on Computational Complexity*, pages 309–315. IEEE, 2012. (cit. on p. 2)

[TSUZ07] Amnon Ta-Shma*, Christopher Umans, and David Zuckerman. Lossless condensers, unbalanced expanders, and extractors. *Combinatorica*, 27(2):213–240, 2007. (cit. on p. 2)

[YH19] Hikmet Yildiz and Babak Hassibi. Optimum Linear Codes With Support-Constrained Generator Matrices Over Small Fields. *IEEE Transactions on Information Theory*, 65(12):7868–7875, December 2019. doi:10.1109/TIT.2019.2932663. (cit. on p. 7, 21)

[ZP81] Victor Vasilievich Zyablov and Mark Semenovich Pinsker. List concatenated decoding. *Problemy Peredachi Informatsii*, 17(4):29–33, 1981. (cit. on p. 2, 3)