Electronic Colloquium on Computational Complexity, Report No. 146 (2025)

From Random to Explicit via Subspace Designs With Applications to Local Properties and Matroids

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

Abstract

In coding theory, a common question is to understand the threshold rates of various local properties of codes, such as their list decodability and list recoverability. A recent work Levi, Mosheiff, and Shagrithaya (FOCS 2025) gave a novel unified framework for calculating the threshold rates of local properties for random linear and random Reed–Solomon codes.

In this paper, we extend their framework to studying the local properties of subspace designable codes, including explicit folded Reed-Solomon and univariate multiplicity codes. Our first main result is a local equivalence between random linear codes and (nearly) optimal subspace design codes up to an arbitrarily small rate decrease. We show any local property of random linear codes applies to all subspace design codes. As such, we give the first explicit construction of folded linear codes that simultaneously attain all local properties of random linear codes. Conversely, we show that any local property which applies to all subspace design codes also applies to random linear codes.

Our second main result is an application to matroid theory. We show that the correctable erasure patterns in a maximally recoverable tensor code can be identified in deterministic polynomial time, assuming a positive answer to a matroid-theoretic question due to Mason (1981). This improves on a result of Jackson and Tanigawa (JCTB 2024) who gave a complexity characterization of $\mathsf{RP} \cap \mathsf{coNP}$ assuming a stronger conjecture. Our result also applies to the generic bipartite rigidity and matrix completion matroids.

As a result of additional interest, we study the existence and limitations of subspace designs. In particular, we tighten the analysis of family of subspace designs constructioned by Guruswami and Kopparty (Combinatorica 2016) and show that better subspace designs do not exist over algebraically closed fields.

*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

ISSN 1433-8092

1 Introduction

One of the biggest success in modern mathematics and theoretical computer science is use randomness to understand discrete and continuous structures. In combinatorics, the probabilistic method [AS16], pioneered by Erdős, has been used to prove existence of various mathematical objects, such as Ramsey graphs, lossless expanders, and many more. In algorithm design and computational complexity theory, the use of randomness has been the key to providing efficient solutions to many computational problems, such as polynomial identity testing (PIT).

However, for both theoretical and practical considerations, it is often desirable to remove the use of randomness through *derandomization*. From this perspective, randomization can be viewed as the first step toward the resolution of a mathematical problem. For example, in combinatorics, we often seek *explicit constructions* of mathematical objects we only know to exist via the probablistic method. Likewise, in algorithm design, often one seeks a *deterministic* algorithm after a randomized algorithm has been identified.

However, in many cases, derandomization proves to be quite formidable, and the existence of a derandomization is often still remain open. To name two examples from combinatorics and algorithm design, respectively, first it is an easy exercise to check that random graphs are lossless two-sided vertex expanders, but explicit constructions were long-standing open problems until two breakthroughts [RVW00] (one-sided expansion) and [HLM+25] (two-sided expansion). Second, randomized PIT algorithm easily follows from Schwarz–Zippel lemma, but a deterministic PIT algorithm remains one of the most significant open problems in theoretical computer science, and perhaps the most key stepping stone toward proving that $\mathsf{P} = \mathsf{BPP}$.

In this paper, we use *subspace designs* introduced by Guruswami and Xing [GX13] in novel ways to achieve derandomizations in two different problems from combinatorial constructions and algorithm design respectively: *Local properties of linear codes* and *Independence testing of birigidity and maximally recoverability matroids*. We now give a brief overview of each of the subfields of mathematics and computer science our work touches upon.

Subspace Designs. The concept of *subspace designs* was first introduced by Guruswami and Xing [GX13] to (randomly) construct the first family of positive-rate rank-metric codes that are list-decodable beyond half their minimum distance, as well as efficiently list-decodable Hamming-metric codes of optimal rate over constant-size alphabets with nearly constant list size. Informally, a subspace design is a family of linear subspaces with the property that any subspace of fixed dimension has only small total overlap with the family (see Definition 1.1 for more details).

While the probabilistic method establishes the existence of subspace designs with both large size and dimension [GX13, GK16], Guruswami and Kopparty [GK16] subsequently provided the first explicit construction attaining the similar parameters over large fields via the idea of folded Reed–Solomon codes and univariate multiplicity codes. As an application, these explicit subspace designs yield a full derandomization of the code constructions from [GX13]. Later, by employing techniques from algebraic function fields, Guruswami, Xing, and Yuan [GXY18] constructed explicit subspace designs with comparable parameters over significantly smaller fields. Besides their use in list-decodable code constructions, subspace designs have also been instrumental in constructing explicit lossless dimension expanders of constant degree [GRX21], which can be viewed as the linear-algebraic analogue of classical expander graphs. For a more fine-grained historical overview, we refer the reader to the recent survey by Santonastaso and Zullo [SZ23].

All the aforementioned list-decodable codes (e.g., [GX13, GK16, GX22]) that make use of the notion of subspace designs are subcodes of classical algebraic codes such as Reed–Solomon, folded Reed–Solomon, algebraic–geometry, univariate multiplicity, and Gabidulin codes. However, a major

recent turning point was achieved by the work of Chen and Zhang [CZ25], who proved that explicit folded Reed–Solomon and univariate multiplicity codes themselves attain optimal list-decodability. In particular, they showed that any code admitting sufficiently good subspace designs enjoys near-optimal list-decodability (see [CZ25, Appendix B] for further details). These codes, known as *subspace designable codes* in [CZ25], will play a central role in our paper.

Local Properties of Linear Codes. List-decodability and list-recoverability are two properties people care the most in the theory of error-correcting codes. Given a code $\mathcal{C} \subseteq \Sigma^n$ over alphabet Σ, a radius ρ, an input list size ℓ, and an output list size L, we say $\mathcal{C}$ is (ρ, ℓ, L) list-recoverable iff for any received table $S_1, \ldots, S_n \in \binom{\Sigma}{\leq \ell}$, there are at most L codewords $c \in \mathcal{C}$ such that at most ρ fraction of coordinates $i \in [n]$ satisfy $c_i \notin S_i$. List-decoding is a special case of list-recovery when $\ell = 1$. Motivated by understanding these two basic combinatorial properties of various families of error-correcting codes, Mosheiff, Resch, Ron-Zewi, Silas, and Wootters [MRR+20] introduced a more generalized framework *local property*. In this broader perspective, One can define the notion *local profile* as the forbidden pattern of codes that can be certified by a small list of codewords. A *local property* $\mathcal{P}$ is defined as a family of local profiles, and a code has the property $\mathcal{P}$ iff it does not contain any certificate for any local profile in $\mathcal{P}$. In this language, both list-decodability and list-recoverability are just special cases of local properties.

The study of local properties mostly starts from analyzing random linear codes, which can be seen the "(nearly) optimal benchmark"[1] in many scenarios. For any local property, people first characterize its *rate threshold* below which random linear codes satisfy the local property with high probability. Then, people make use of this characterization to show that various specific families of linear codes has (almost) the same rate threshold. In particular, [MRR+20] showed that random LDPC codes behaves the same as random linear codes. Guruswami, Li, Mosheiff, Resch, Silas, and Wootters [GLM+22] use this framework to show interesting lower bounds for list-decoding and list-recovery. After that, Guruswami and Mosheiff [GM22] proved randomly punctured low-biased codes locally simulate random linear codes. Most recently, a great work by Levi, Mosheiff and Shagrithaya [LMS25] generalized the previously mentioned characterization of rate thresholds to *large alphabet*, and used this novel characterization to show random Reed–Solomon codes are local equivalence to random linear codes.

However, all of the above results are about *randomness-efficient* families of linear codes. Although compared to uniformly random linear codes, these certain families of linear codes requires fewer random bits to sample from, they are not *explicit constructions*. For some special cases of local properties such as list-decoding, there are explicit constructions with the same quality as random linear codes [ST23, BDG24b, CZ25, JMST25]. However, explicit constructions that match random linear codes in terms of general local properties, or even the special case of list-recoverability, are unknown before. In this paper we provide the first explicit construction that simulate all local properties of random linear codes and address this open problem.

Maximally Recoverability and Rigidity Matroids. The quest for explicit constructions matching random ones has deep connections to *matroid theory*. Informally, matroids are combinatorial objects which generalize the behavior of collections of vectors in a vector space (see Section 5 for a formal definition). We now describe two families of matroids which, while seemingly unrelated, both demand an improved theory of derandomization: maximal recoverability and structural

[1] In some cases non-linear codes can provably outperform linear codes. However, linearity of codes is useful in many applications, and many explicit constructions of specific families of codes are linear. Another work [GMR+22] builds the framework of local properties for random (non-linear) codes.

rigidity.

In the distributed storage community, much effort over the last couple of decades [CHL07,HCL13, BPS13, SAP+13, GHJY14, PD14, HY16, GHK+17, KLR19, MPK19, GGY20, HPYWZ21, CMST21, KMG21, GG22, BGM22, DG23, BDG25] has been put into studying data storage solutions which information-theoretically maximize their resilience from data loss. Error-correcting codes which satisfy such problems are described as *maximum recoverable (MR)*. In a strong sense, the construction of MR codes is a derandomization problem, as a random code can correct any particular error with high probability, but guaranteeing tolerance to all possible errors simultaneously requires an explicit construction.

From a mathematical perspective, a rather fascinating family of MR codes is the MR *tensor* codes introduced by Gopalan et al. [GHK+17], where the error-correcting code is the tensor product of two linear codes. Unlike many other architectures for which MR has been studied, we lack a basic understanding of which failures (i.e., erasure errors) we should even be able to recover from (e.g., [HPYWZ21]), much less explicit constructions of MR tensor codes [BDG24b]. Recently, the construction of maximally recoverable tensor codes has also been linked to optimal list-decodable codes [ST23, BGM23, AGG+25]. A comprehensive understanding of derandomizing the properties of random linear codes could be of much use in answering such questions.

In combinatorics, a long-standing area of study is *structural rigidity theory*.[2] A landmark question open question in rigidity theory is that of *graph rigidity*. Consider an undirected graph $G = (V, E)$ and an ambient space $\mathbb{R}^d$, when does there an embedding[3] $\psi : V \to \mathbb{R}^d$ such that the graph cannot be flexed (i.e., an infinitesimal isometry which is not a translation/rotation)? If such an embedding exists, a random embedding (e.g., random sampled from a multivariate normal distribution) will work probability 1. A simple description for the case $\mathbb{R}^2$ has been known for nearly 100 years [PG27, Lam70]. However, finding deterministic polynomial time description for rigidity in $\mathbb{R}^3$ has been open since the days of James Clerk Maxwell [Max64, GSS93]!

Although MR and structural rigidity are seemingly unrelated, Brakensiek, Dhar, Gao, Gopi, and Larson [BDG+24a] proved a number of equivalence results between maximal recoverability and structural rigidity. For example, understanding the maximal recoverability of a linear code tensored with itself is (roughly speaking) to this classical graph rigidity question. For our purposes, we build on a different equivalence proven by [BDG+24a] that the maximal recoverability of the tensor product of two different linear codes is equivalent to understanding the *bipartite rigidity* (birigidity) of graphs, an adaptation of classical rigidity proposed by Kalai, Nevo, and Novik [KNN15].

We seek to be the first work which takes advantage of this new-found equivalence by using our "random-to-explicit" perspective to make simultaneous progress in the theory of both maximal recoverability and rigidity. We point the interested reader to Section 1.1.2 and Section 5 for a more details. We also recommend the recent survey by Cruickshank, Jackson, Jordán, and Tanigawa for many rich connections between rigidity matroids and other problems [CJJT25].

1.1 Our Results

In order to formulate our main results, we first introduce the notions of subspace designs [GX13, GK16] and subspace designable codes [GK16, CZ25].

Definition 1.1 (Subspace Design, [GK16, Definition 3])**.** A collection $\mathcal{H}$ of $\mathbb{F}$-linear subspaces $H_1, \ldots, H_n \subseteq \mathbb{F}^k$ is called an (ℓ, A) subspace design over $\mathbb{F}$, if for every $\mathbb{F}$-linear space $W \subseteq \mathbb{F}^k$ of

[2] In this paper "rigidity" always refers to *geometric* structural rigidity, there is no known link between these questions and the well-studied *matrix rigidity* problems in TCS (e.g., [Ram20]).

[3] We assume that ψ maps the vertices to "general position," no three points on a line, etc.

dimension ℓ, we have

$$\sum_{i=1}^{n} \dim_{\mathbb{F}} (H_i \cap W) \leq A.$$

.

Definition 1.2 (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.

We call an s-folded $\mathbb{F}$-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.

Since we will establish a negative bound Theorem 1.11 later in this paper, and it indicates that for algebraically closed field, the quality of d-dimensional subspace design cannot be better than $\frac{d(k-d)}{s-d+1} \geq \frac{Rdsn}{s-d+1} - \frac{d^2}{s-d+1} = R(1 + \frac{d-1}{s-d+1})dn - \frac{d^2}{s-d+1}$. For fixed $d \geq 1$ and large enough n, this lower bound is strictly larger than Rdn. Therefore, the d-subspace designable codes actually yield **optimal** subspace designs for subspaces with dimension at most d.

We also need a slacked version for "nearly optimal" subspace designable codes. Namely, for any real $\mu > 0$ and integer $d \geq 1$, we say the code $\mathcal{C} \subseteq (\mathbb{F}^s)^n$ μ-slacked d-subspace designable if for all $1 \leq d' \leq d$, $\mathcal{C}$ is $(d', (R + \mu)d'n)$ subspace designable.

1.1.1 Local Equivalence Between Random Linear Codes and Subspace Designs

Our first main result is to build a local equivalence between random linear codes and nearly optimal subspace designable codes. Since explicit folded Reed–Solomon codes and univariate multiplicity codes yield nearly optimal subspace designs [GK16], our result gives the first explicit construction of folded linear codes that simultaneously preserves all local properties of random linear codes.

We will formally define the concept local profile later. For readers unfamiliar with this notion, a good intuition is to think a local profile as a certain list-decodability or list-recoverability of codes as special cases of our general reduction[4].

Theorem 1.3 (Informal)**.** *Fix $b, q \geq 1, \varepsilon, R \in (0, 1)$ and any b-local profile $\mathcal{V} = (V_1, \ldots, V_n) \in \mathcal{L}(\mathbb{F}_q^b)^n$. The following holds.*

- (Theorem 3.1) *If random $\mathbb{F}_q$-linear codes with rate R does not contain $\mathcal{V}$ with high probability, then all $\mathbb{F}_q$-linear ε-slacked b-subspace designable codes with rate at most $R - \varepsilon$ do not contain $\mathcal{V}$.*
- (Theorem 4.2) *For any $d \geq 1$, if for all large enough block length n, all $\mathbb{F}_q$-linear, d-subspace designable code with rate R does not contain $\mathcal{V}$, then random $\mathbb{F}_q$-linear code with rate $R - o_n(1) - \varepsilon$ does not contain $\mathcal{V}$ with probability at least $1 - q^{-\varepsilon n + b^2}$.*

As a direct corollary of Theorem 1.3, we give a reduction from list-recoverability of optimal subspace designable codes to list-recoverability of random linear codes as stated in Corollary 4.3. In a follow-up work [BCDZ25], the authors use this reduction to prove the nearly-optimal list-recoverability of random linear codes. See Table 1 for a comparison with previous work.

It was known from the pioneer work of Guruswami and Kopparty [GK16] that when $s \geq b(R/\varepsilon + 1)$, the explicit s-folded Reed–Solomon codes and s-univariate multiplicity codes are ε-slacked b-subspace designable codes as discussed later in Remark 1.9.

[4] Actually, list-decoding and list-recovery corresponds to a family of local profiles rather than a single one.

Codes attain thresholds of RLC	List-decoding	List-recovery	All local properties
Random LDPC codes	[MRR+20]	[MRR+20]	[MRR+20]
Randomly punctured low-bias codes	[GM22]	[GM22]	[GM22]
Random RS codes	[ST23, BGM23, GZ23, AGL24]	[LMS25]	[LMS25]
Explicit Constructions	[ST23, BDG24b, CZ25, JMST25]	This work	This work

Table 1: This table compares various randomness-efficient families of linear codes as well as explicit codes that behave like random linear codes in terms of list-decoding, list-recovery, and the most general local properties. See also our discussion on the concurrent work of [JS25].

Therefore, as a corollary, we give the first explicit construction of codes that simultaneously simulate all local properties of random linear codes. Concretely, it follows that

Theorem 1.4. *Fix $b, q \geq 1, \varepsilon, R \in (0,1), s \geq b(R/\varepsilon + 1)$, there are explicit s-folded Reed–Solomon codes and s-order univariate multiplicity codes $\mathcal{C} \subseteq (\mathbb{F}_q^s)^n$, where $q = \Theta(sn)$, with rate $R - \varepsilon$, such that for any b-local profile $\mathcal{V} = (V_1, \ldots, V_n) \in \mathcal{L}(\mathbb{F}_q^b)^n$, if random $\mathbb{F}_q$-linear code with rate R does not contain $\mathcal{V}$ with high probability, then $\mathcal{C}$ does not contain $\mathcal{V}$.*

In particular, for any $\ell, L \geq 1$, if random $\mathbb{F}_q$-linear codes with rate R are (ρ, ℓ, L)-list recoverable, then $\mathcal{C}$ is (ρ, ℓ, L) list-recoverable.

Since it was previously shown by [BGM23, AGL24, LMS25] that random linear codes achieve generalized singleton bound, Theorem 1.4 directly gives an alternative proof of the main theorem of [CZ25] that folded RS codes achieves generalized singleton bound [ST23] as a special case.

Interestingly, since the main theorem of [CZ25] only uses the subspace design property (This generalization is presented in [CZ25, Appendix B]), [CZ25] actually proves that all optimal subspace designable codes achieve generalized singleton bound. Therefore, combined with [CZ25], the second item of Theorem 1.3 actually conversely provides an alternative proof that random linear codes achieve generalized singleton bounds originally by [BGM23, AGL24, LMS25].

Remark 1.5 (List-recoverability)**.** Fix radius $1 - R - \varepsilon$ and input list size $\ell \geq 2$, the best known $(1-R-\varepsilon, \ell, L)$ list-recoverability of random linear codes is $L = (\ell/\varepsilon)^{O(\ell/\varepsilon)}$ by [LS25]. As an algebraic miracle, the bound for explicit folded RS codes is $L = (\ell/\varepsilon)^{O(1+\log(\ell)/\varepsilon)}$ by [KRZSW23, Tam24], which is better! As we have seen before that [CZ25] plus our reduction implies the same bound for random linear codes [BGM23, AGL24, LMS25], it is tempting to use Theorem 1.3 on the bound in [KRZSW23, Tam24] to improve the bound of [LS25]. Regrettably, this cannot work. The reason is that, unlike [CZ25], the proof of [KRZSW23, Tam24] is not "subspace-design-only". Concretely, their proof intrinsically relies on the fact that bad list resides in some low-dimensional affine subspace, which was proved in [GW13] using an interpolation technique that is tailored for algebraic codes, This does not apply to merely optimal subspace designable codes and we cannot apply Theorem 1.3 on their bound.

However, in a follow-up work [BCDZ25], the authors prove a better bound $(\frac{\ell}{R+\varepsilon})^{O(R/\varepsilon)}$ in a "purely subspace-design" way. This directly improves the bound of [KRZSW23, Tam24] for folded RS codes. Moreover, this "subspace design nature" of their proof unlocks the full power of Theorem 1.3 and enables them to use this reduction to transfer the same bound directly to random linear codes, which improves the bound of [LS25].

Concurrent Work. Concurrently and independently, in an exciting work by Jeronimo and Shagrithaya [JS25], the authors use the AEL-type constructions [AEL95] to get explicit constructions of folded linear codes over **constant-sized** alphabet that simulates any fixed "**reasonable** local property". We comment and compare their results with ours as follows.

- For any fixed family of b-local profiles $\mathcal{V}_1, \ldots, \mathcal{V}_m$, if each of them has at most T distinct linear subspaces within it, then [JS25] constructs explicit codes with alphabet $q^{\Theta(T^3)}$ that simulates all these local profiles when $m = q^{o(n)}$. However, for the most general family of local profiles, these parameters could be $m = q^{\Theta(b^2 n)}$ and $T = \min(q^{\Theta(b^2)}, n)$. Although this makes [JS25] inaccessible in the most general setting, it is not an issue when q is a large constant independent of n, which is the primary case of interest in [JS25]. By contrary, our construction uses a single algebraic code to simulate all possible b-local profiles simultaneously.
- As the cost of simultaneous simulation of all local profiles, our explicit construction requires alphabet size $q = \Theta(bn)$, while the construction of [JS25] requires only constant alphabet when the previous conditions are met, which is better in these cases. We further comment that in Theorem 4.1 we prove that there exists nearly optimal subspace designs over constant alphabet. Therefore, future improvement on explicit constructions of subspace designs over smaller fields would reduce the alphabet size required.
- Before our work, local properties are primarily interested for the reasons of list-decoding and list-recovery of linear codes. For these two major applications, the conditions in the first item are met so both [JS25] and our results can handle list-decoding and list-recovery when the input and output list sizes are constants. However, in our second part of results relating to tensor codes, T and q could be enormous so we have to simulate local profiles in the most general setting.

1.1.2 Applications to Tensor Codes and Matroid Theory

As mentioned earlier, two commonly study local properties correspond to the list-decodability and list-recoverability of linear codes. A novel conceptual contribution we make in this paper is that the theory of local properties (with slight modification) can be used to study the *tensoring* of linear codes. Given a column code $C_{\mathsf{col}} \subseteq \mathbb{F}_q^m$ and a row code $C_{\mathsf{row}} \subseteq \mathbb{F}_q^n$, we define their tensor product $C_{\mathsf{col}} \otimes C_{\mathsf{row}} \subseteq \mathbb{F}_q^{m \times n}$ to be the set of all $m \times n$ matrices such that each column is a codeword in C_{col} and each row is a codeword in C_{row}. In particular, $\dim(C_{\mathsf{col}} \otimes C_{\mathsf{row}}) = \dim(C_{\mathsf{col}}) \dim(C_{\mathsf{row}})$.

As a fundamental linear algebraic operation, tensor products are a key operation in many constructions within coding theory as well as more broadly in TCS [GHK+17, PK22, DEL+22, CCS25, KP25, BGI+25]. In this paper, we use the theory of local properties to understand better the *correctability* of tensor products with respect to erasures. That is, given an erasure pattern $E \subseteq [m] \times [n]$, when can we recover a codeword $c \in C_{\mathsf{col}} \otimes C_{\mathsf{row}}$ when only given the symbols $c|_{\bar{E}}$? This is equivalent to asking whether there exists a codeword $c \in C_{\mathsf{col}} \otimes C_{\mathsf{row}}$ supported on E. Of course, the answer depends on the precise structure on the precise structure of C_{col} and C_{row}, but there is much interest in understanding best-case scenario. More formally, Gopalan et al. [GHK+17] asked the following.

Question 1.6. *Given parameters m, n, a, b as well as a pattern $E \subseteq [m] \times [n]$. When does there exist (for sufficiently large q) a $m - a$-dimensional column code $C_{\mathsf{col}} \subseteq \mathbb{F}_q^m$ and a $n - b$-dimensional row code $C_{\mathsf{row}} \subseteq \mathbb{F}_q^n$ such that E is a correctable pattern in $C_{\mathsf{col}} \otimes C_{\mathsf{row}}$?*

In the case $a = 1$, Gopalan et al. [GHK+17] gave a combinatorial description, which was later turned into a deterministic[5] polynomial-time checkable condition by Brakensiek, Gopi, and Makam [BGM22, BGM23]. However, the approach used in those works cannot extend to $a \geq 2$ [HPYWZ21]. Although Question 1.6 may seem like a niche coding theory question on the surface, a recent characterization by Brakensiek et al. [BDG+24a] shows that answering Question 1.6 is

[5] We note that Question 1.6 lies in RP by picking C_{col} and C_{row} to be random linear codes and invoking Schwarz-Zippel [Sch80, Zip79]. The core challenge is to *derandomize* this special case of Polynomial Identity Testing (PIT).

equivalent to resolving some long-standing questions in *matroid* theory, including understanding the structural rigidity of bipartite graphs [KNN15] as well as when partially revealed matrices can be completed to low-rank matrices [SC10]. See Section 5 as well as the recent survey by Cruickshank et al. [CJJT25] for a more thorough discussion of these connections.

We give a novel plan of attack toward resolving Question 1.6 by studying correctability in a tensor code as a a slight variant of a local property in the sense of [LMS25]. By adapting a suitable potential function designed in [LMS25], (see Section 5.2) we give a one-sided test for checking whether E is a correctable pattern in Question 1.6. By "one-sided," we mean than the potential test might report than E is correctable when E is actually uncorrectable, but the opposite can never occur. By suitably adapting Theorem 1.3 (see Section 5.3), we can replace C_{col} and C_{row} with two explicit folded Reed-Solomon codes (with the caveat the folding parameters are $\mathrm{poly}(m,n)$-sized) and use those to deterministically check the correctability conditions.

To understand the accuracy of this algorithm, one needs to know whether there exists patterns E which are uncorrectable in Question 1.6, but are correctable according to the folded Reed-Solomon codes. We connect this question to a long-standing question[6] by Mason [Mas81] on the structure of the tensor products of matroids. Informally, Mason asks whether the linear algebraic tensor product of two random linear codes (over a large field) is the most general matroid which "looks like" a tensor product. See Conjecture 5.5 for the precise assumption we make, which is a modern reformulation oif Mason's question by Cruickshank et al. [CJJT25] which is more convenient for our purposes. With this assumption, we can prove that the potential function we construction is a *zero-error* test for correctability (see Corollary 5.11 and Lemma 5.18). As such, we prove the following result.

Theorem 1.7 (Informal, see Theorem 5.2)**.** *Assuming a positive answer to a question of* Mason [Mas81]*, Question 1.6 can be answered in deterministic polynomial time.*

This result improves over a recent result of Jackson and Tanigawa [JT24] who conditionally showed than Question 1.6 lies in $\mathsf{RP} \cap \mathsf{coNP}$. We note however their conditional assumption was different (and stronger), see Section 5.1 for further discussion. See also Remark 5.6 for a thorough discussion on evidence for and against Conjecture 5.5.

The recent work of Bérczi et al. [BGI+25] also studies products between matroids, although they are interested in constructing products for an arbitrary pair of matroids, whereas we are interested in studying more deeply the tensor products of linear matroids.

1.1.3 Tight Bounds for the Quality of Subspace Designs

Given the aforementioned applications of subspace designable codes, a natural topic to investigate is the optimal parameters of explicit subspace designs. In Section 6, we make new progress toward answering such questions. As a baseline, we first present parameters of the explicit construction of subspace designable codes in [GK16].

Theorem 1.8 ([GK16])**.** *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.*

Remark 1.9. This parameter implies that, for any $b \geq 1, \varepsilon \in (0,1)$ and rate $R = k/(sn)$, when $s \geq b(R/\varepsilon + 1)$, explicit s-folded Reed–Solomon codes and s-order univariate multiplicity codes are ε-slacked b-subspace designable since we can calculate $d(k-1)/(s-d+1) \leq (R+\varepsilon)dn$ for all $d \in [b]$ under this choice of s.

[6] This question on the tensor products of matroids should not be confused with Mason's log-concavity conjectures which were recently resolved [AHK18, HSW21, BH20, Huh22, ALOGV24].

Our first contribution is a more fine-grained analysis of Theorem 1.8 that slightly improves its parameters.

Theorem 1.10 (Informal, see Theorem 6.1)**.** *Assume that $q > ns$, then 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 $(d, \frac{d(k-d)}{s-d+1})$ subspace designable code. In particular, explicit folded RS codes are such constructions.*

The proof of Theorem 1.10 largely follows the proof of Theorem 1.8, except we correct one inefficiency in the root-counting bound of [GK16] which leads to the slightly tighter parameters. More surprisingly, we show that the bound is Theorem 1.10 is *exactly* tight, as long as the base field $\mathbb{F}$ is algebraically closed (e.g., $\mathbb{C}$ or the algebraic closure of $\mathbb{F}_2$).

Theorem 1.11 (Informal, see Theorem 6.2)**.** *Let $\mathbb{F}$ be an algebraically closed field (of any characteristic). Consider any $\mathbb{F}$-linear codes $\mathcal{C} \subseteq (\mathbb{F}^s)^n$ and parameter $d \in \{1, \ldots, s\}$. If $n \leq \frac{d(k-d)}{s-d+1}$ then $\mathcal{C}$ is* not *a $(d, \frac{d(k-d)}{s-d+1} - 1)$ subspace designable code.*

In particular, any improvements over Theorem 1.10 must crucially use the fact that $\mathbb{F}_q$ fails to be algebraically closed. In Section 6.3, we give a simple example over $\mathbb{F}_3$ of a (constant-sized) subspace design utilizing this property to beat Theorem 1.10.

Remark 1.12. A recent work by Santonastaso and Zullo [SZ23] also studies the optimal parameters for subspace designs over finite fields, with the motivation of achieving a better understanding of the parameters sum-rank codes. However, the regime they work in is rather different from ours. In particular, they are primarily interested in the regime for which $d = k - 1$, although they allow the test space U to be a vector space over an extension field. They also allow $\dim(U) + \dim(H_i) > k$, which we do not allow. In the most comparable regime of $s = d = k - 1$, they get that $\mathcal{C}$ is not $(k-1, k-2)$ subspace designable over any field, which matches our bound for algebraically closed fields. Of note, Theorem 1.8 by [GK16] constructs a $(k-1, (k-1)^2)$ design in this regime, which is improved to the tight bound of $(k-1, k-1)$ by our Theorem 1.10.

The proof of Theorem 1.11 makes nontrivial use of algebraic geometry. More precisely, we observe that the space of d-dimensional subspaces $W \subseteq \mathbb{F}^k$ can be viewed as the $d(k-d)$-dimensional *Grassmannian* projective variety (see [LB15]). A subspace design constraint of the form $\dim(H_i \cap W) \geq 1$, carves out a what is known as a *Schubert subvariety* of the Grassmannian. The key property of this Schubert subvariety is that it has codimension $s - d + 1$. A key property of subvarieties over algebraically closed fields is that the codimension of the intersection of subvarieties is a a subadditive function of the codimensions of the respective subvarieties (e.g., [Har77]). Thus, if we seek to rule out all W in the Grassmanian as counterexamples to Definition 1.1, we need to intersect at least $\lfloor \frac{d(k-d)}{s-d+1} \rfloor + 1$ Schubert subvarieties, implying the subspace design parameter shouild be at least $\lfloor \frac{d(k-d)}{s-d+1} \rfloor > \frac{d(k-d)}{s-d+1} - 1$.

Open Questions

Given the many connections between our work and various parts of mathematics and computer science, there are a variety of directions to pursue.

- Theorem 4.1 shows that near-optimal subspace designable codes exist over constant-sized fields. Can such codes be explicitly constructed?

- Conversely, can Theorem 1.11 be extended to the setting of finite fields? Recall we show in Section 6.3 the the lower bound must to degrade to some extent, but is a lower bound of $(1-o(1))\frac{d(k-d)}{s-d+1}$ possible?
- From our connection between local properties and rigidity matroids, a key open question is to prove or disprove Conjecture 5.5. Either outcome has interesting ramifications for both coding theory and rigidity theory, see Remark 5.6 for further discussion.
- We also emphasize the long-standing open question (since the 1800s [Max64, GSS93]) of giving a deterministic polynomial time algorithm for detecting (non-bipartite) rigid graphs in $\mathbb{R}^3$. The methods used in this paper likely are insufficient to resolve this question, but further understanding on derandomizing (not necessarily local) properties of random linear codes could be critical to its resolution.

Organization

In Section 2, we present some basic notation as well as discuss the theory of local properties by Levi, Mosheiff, and Shagrithaya [LMS25]. In Section 3, we show that subspace design codes of slacked rate capture all local properties of random linear codes, establishing the first half of Theorem 1.3. In Section 4, we show that local properties shared by all subspace design codes also apply to random linear codes, proving the second half of Theorem 1.3. In Section 5, we adapt the theory of local properties to the study of quesitons in matroid theory, proving Theorem 1.7. In Section 6, we study the optimal parameters of subspace designs, proving Theorem 1.11 and Theorem 1.10.

2 Preliminaries

Notation. For a matrix $M \in \Sigma^{n\times m}$, we let $M[i,j] \in \Sigma, i \in [n], j \in [m]$ denote the entry at the i-th row and j-th column. We use $M[i:] \in \Sigma^m$ to denote the i-th row of M and $M[:j] \in \Sigma^n$ to denote the j-th column of it. Assume U, V are two linear spaces over field $\mathbb{F}$. We use $\dim(U)$ to denote $\mathbb{F}$-dimension of U. For a set of vectors $f_1, \dots f_m \in U$, we use $\mathrm{Span}(f_1, \dots, f_m)$ to denote the linear subspace of U $\mathbb{F}$-spanned by $f_1, \dots, f_m$. Given a linear map $\psi\colon U \to V$, we let $\ker(\psi)\colon = \{f \in U\colon \psi(f) = 0\}$ denote the kernel of ψ. By the first isomorphism theorem, $\ker(\psi)$ is an $\mathbb{F}$-linear subspace of U.

Definition 2.1 (Folded Wronskian, see [GK16])**.** Let $f_1(X), \dots, f_s(X) \in \mathbb{F}_q[X]$ and $\gamma \in \mathbb{F}_q^\times$. We define their γ-folded Wronskian $W_\gamma(f_1, \dots, f_s)(X) \in (\mathbb{F}_q[X])^{s\times s}$ by

$$W_\gamma(f_1, \dots, f_s)(X) \stackrel{\text{def}}{=} \begin{pmatrix} f_1(X) & \cdots & f_s(X) \\ f_1(\gamma X) & \cdots & f_s(\gamma X) \\ \vdots & \ddots & \vdots \\ f_1\left(\gamma^{s-1}X\right) & \cdots & f_s\left(\gamma^{s-1}X\right) \end{pmatrix}.$$

It is well known that the nonsingularity of the folded Wronskian of a set of vectors characterizes the linear independence of these vectors, as stated below.

Lemma 2.2 (Folded Wronskian criterion for linear independence, see [GK16, GW13])**.** *Let $k < q$ and $\vec{f_1}, \dots, \vec{f_s} \in \mathbb{F}_q^k$. Let γ be a generator of $\mathbb{F}_q^\times$. Then $\vec{f_1}, \dots, \vec{f_s}$ are linearly independent over $\mathbb{F}_q$ if and only if the folded Wronskian determinant $\det W_\gamma(f_1, \dots, f_s)(X) \neq 0$.*

2.1 Local Profiles and Thresholds of Random Linear Codes

In this section, we describe the work Levi, Mosheiff, and Shagrithaya [LMS25] on the theory of local profiles for random linear codes. We closely follow their notation.

Fix a finite field $\mathbb{F}_q$, block length n and configuration parameter $b \geq 1$. Let $\mathcal{L}(\mathbb{F}_q^b)$ denote the set of all linear subspaces of $\mathbb{F}_q^b$. Let $\mathcal{L}_{\mathsf{Dist}}(\mathbb{F}_q^b)$ denote the set of all linear subspaces U of $\mathbb{F}_q^b$ whose basis matrix $B_U \in \mathbb{F}_q^{b\times \dim(U)}$ (This means columns of B_U form a basis of U) does not contain repeated rows. This is equivalent to say that for any $i \neq j \in [b]$, there exists some $f \in U$ such that $f_i \neq f_j$.

We call $\mathcal{V} = (V_1, \ldots, V_n) \in \mathcal{L}(\mathbb{F}_q^b)^n$ a b-local profile. For any b-local profile $\mathcal{V}$ and linear subspace $U \in \mathcal{L}(\mathbb{F}_q^b)$, [LMS25] use $\mathcal{M}_{\mathcal{V},U}$ to denote the set of matrices $M \in \mathbb{F}_q^{n\times b}$ such that

(1) M has pairwise distinct columns.

(2) for any $i \in [n]$, the i-th row M_i of M satisfies $M_i \in V_i \cap U$.

(3) The row span of M is U.

They use $\mathcal{M}^*_{\mathcal{V},U}$ to denote the set of matrices that satisfy condition (2). For any $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$, we say $\mathcal{C}$ contains $(\mathcal{V}, U)$ if there is some $M \in \mathcal{M}_{\mathcal{V},U}$ such that each column of M is in $\mathcal{C}$. We say $\mathcal{C}$ contains $\mathcal{V}$ if there is some $U \in \mathcal{L}(\mathbb{F}_q^b)$ such that $\mathcal{C}$ contains $(\mathcal{V}, U)$. [LMS25] defines the potential function of $(\mathcal{V}, U)$ as

$$\Phi(\mathcal{V}, U, R) = -n\dim(U) + \sum_{i=1}^{n} \dim(V_i \cap U) + Rn\dim(U). \tag{1}$$

Moreover, [LMS25] defines $R_{\mathcal{V}}$ of a b-local profile $\mathcal{V}$ as follows.

$$R_{\mathcal{V}} = \max\{R \in [0,1] \colon \forall U \in \mathcal{L}_{\mathsf{Dist}}(\mathbb{F}_q^b), \exists W \subsetneq U, \text{ s.t. } \Phi(\mathcal{V}, U, R) - \Phi(\mathcal{V}, W, R) \leq 0\}.$$

We observe the following simple fact about $R_{\mathcal{V}}$.

Fact 2.3. *For any b-local profile $\mathcal{V}$, rate $R \in [0,1]$, and subspace $U \in \mathcal{L}_{\mathsf{Dist}}(\mathbb{F}_q^b)$, if $R \leq R_{\mathcal{V}}$, there exists a proper subspace $W \subsetneq U$ such that $\Phi(\mathcal{V}, U, R) - \Phi(\mathcal{V}, W, R) \leq 0$.*

Proof. It follows from the definition of $R_{\mathcal{V}}$ and the fact that for any $W \subsetneq U$, $\frac{\mathsf{d}(\Phi(\mathcal{V},U,R) - \Phi(\mathcal{V},W,R))}{\mathsf{d}R} = n(\dim(U) - \dim(W)) \geq 0$. □

One of the main contributions of [LMS25] is that they show $R_{\mathcal{V}}$ is exactly the rate threshold for random $\mathbb{F}_q$-linear code to contain $\mathcal{V}$, which we quote as follows.

Theorem 2.4 ([LMS25, Theorem 4.4])**.** *Let $\mathcal{V} = (V_1, \ldots, V_n) \in \mathcal{L}(\mathbb{F}_q^b)^n$ be a b-local profile. Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a random $\mathbb{F}_q$-linear code of rate R. The following holds.*

(1) If $R \geq R_{\mathcal{V}} + \varepsilon$, then $\Pr[\mathcal{C}$ contains $\mathcal{V}] \geq 1 - q^{-\varepsilon n + b^2}$.

(2) If $R \leq R_{\mathcal{V}} - \varepsilon$, then $\Pr[\mathcal{C}$ contains $\mathcal{V}] \leq q^{-\varepsilon n + b^2}$.

3 All Subspace Designable Codes Locally Simulate RLCs

Fix $s, b, n \geq 1$ and finite field $\mathbb{F}_q$. For any s-folded $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq (\mathbb{F}_q^s)^n$ and b-local profile $\mathcal{V} = (V_1, \ldots, V_n) \in \mathcal{L}(\mathbb{F}_q^b)^n$, let $\mathcal{C}' \subseteq \mathbb{F}_q^{sn}$ denote the "unfolded" $\mathbb{F}_q$-linear code $\mathcal{C}$ with block length sn and define the s-duplicated b-local profile $\mathcal{V}^{(s)} := (V_1, \ldots, V_1, V_2, \ldots, V_2, \ldots, V_n, \ldots, V_n) \in \mathcal{L}(\mathbb{F}_q^b)^{sn}$ to be the b-local profile with length sn derived from $\mathcal{V}$ such that each V_i is repeated s times. We say $\mathcal{C}$ contains $\mathcal{V}$ iff $\mathcal{C}'$ contains $\mathcal{V}^{(s)}$.

The main result of this section is that nearly-optimal subspace designable codes simultaneously avoid all local profiles that a random linear code could avoid with high probability, with a cost of an arbitrarily small rate decrease. This establishes the harder direction of the local equivalence between subspace desgins and random linear codes.

For any b-local profile $\mathcal{V} = (V_1, \ldots, V_n) \in \mathcal{L}(\mathbb{F}_q^b)^n$, from Theorem 2.4 we know that random $\mathbb{F}_q$-linear code with rate arbitrarily close to $R_{\mathcal{V}}$ could avoid $\mathcal{V}$ with high probability. Therefore, our target is the following.

Theorem 3.1. *Let $s, b \geq 1, \mu > 0$ and $\mathcal{C} \subseteq (\mathbb{F}_q^s)^n$ be a μ-slacked b-subspace designable code with rate $R = k/(sn)$. For any b-local profile $\mathcal{V} = (V_1, \ldots, V_n) \in \mathcal{L}(\mathbb{F}_q^b)^n$, if $R \leq R_{\mathcal{V}} - \mu - 1/n$, then $\mathcal{C}$ does not contain $\mathcal{V}$.*

Technical Overview. Our proof is initially inspired by the similarity between the definition of potential function (1) and the defining inequaliltes of subspace designs. When the rate $R < R_{\mathcal{V}}$ is smaller than the threshold, we know that for any "coordinate configuration" linear subspace $U \subseteq \mathbb{F}_q^b$, it must have a proper linear sbuspace W such that $\Phi(U, \mathcal{V}, R) < \Phi(W, \mathcal{V}, R)$. In previous work on local properties [LMS25], the main proof strategy was to exclude the possibility that the "bad list of codewords" could span U using their "vectors on coordinates" simultaneously for all U. They use the critical subspace $W \subsetneq U$ to project the original local profile $\mathcal{V}$ onto $W^\perp$ to get a new local profile $\mathcal{V}'$, and then reduce the original problem to the smaller linear subspace $W^\perp$ with respect to $\mathcal{V}'$, and calculate the potentials for this case and complete the proof.

However, if we wish to establish the result from subspace designs, we have to find a linear space $N \subseteq \mathbb{F}_q^k$ in the **message space**, which resides in $\mathbb{F}_q^k$, to trigger the defining inequality of subspace designs. As discussed above, [LMS25] primarily works over the **coordinate configuration** linear subspace $U \subseteq \mathbb{F}_q^b$, which resides in $\mathbb{F}_q^b$. Therefore, it was not clear how to find the "working linear subspace" in the message space, so we need a different proof strategy. Unlike [LMS25] that simultaneously[7] avoids all "coordinate subspace" $U \subseteq \mathbb{F}_q^b$, we would only work on a specific $U \subseteq \mathbb{F}_q^b$ depending on any potential "bad list of messages" that we would like to exclude. Concretely, suppose for the sake of contradiction there exists some "bad list of messages" that certifies $\mathcal{V}$, we will define an "associated coordinate subspace" $U \subseteq \mathbb{F}_q^b$ generated from the bad list. Guaranteed by the definition of the threshold rate $R_{\mathcal{V}}$, there exists a proper linear subspace $W \subsetneq U \subseteq \mathbb{F}_q^b$ with larger potential. Then, from U and W, we can construct some linear subspace $N \subseteq \mathbb{F}_q^k$ in the message space. Finally, if we calculate the defining inequality of subspace designs on N, it will lead to a contradiction and concludes that the bad list of messages does not exist. Our main technical novelty is the way to find the specific $U \subseteq \mathbb{F}_q^b$ and $N \subseteq \mathbb{F}_q^k$ such that the potential functions $\Phi(U, \mathcal{V}, R) - \Phi(W, \mathcal{V}, R)$ can be perfectly transformed to "subspace intersections" between $N \subseteq \mathbb{F}_q^k$ and the subspace design.

Proof of Theorem 3.1. Let $\pi_1, \ldots, \pi_n \colon \mathbb{F}_q^k \to \mathbb{F}_q^s$ be linear maps corresponding to $\mathcal{C}$ such that for

[7] In the random RS code setting, [LMS25] starts from the single "whole coordinate space" $\mathbb{F}^b$, but it is still not in the message space.

any $i \in [n], f \in \mathbb{F}_q^k$, there is $\pi_i(f) = \mathcal{C}(f)[i] \in \mathbb{F}_q^s$. Since $\mathcal{C}$ is a μ-slacked b-subspace designable code, we know that for any $1 \le d' \le d$, $\ker(\pi_1), \ldots, \ker(\pi_n) \subseteq \mathbb{F}_q^k$ form a $(d', (R+\mu)d'n)$ subspace design.

Suppose by contrapositive $\mathcal{C}$ contains $\mathcal{V}$, we have distinct $f_1, \ldots, f_b \in \mathbb{F}_q^k$ such that for any $i \in [n]$ and $j \in [s]$, there is $(\pi_i(f_1)[j], \ldots, \pi_i(f_b)[j]) \in V_i$. At least one of $f_1, \ldots, f_b$ is non-zero. Let $F = \mathrm{Span}(f_1, \ldots, f_b)$ and $\dim F = t \ge 1$. Let $g_1, \ldots, g_t \in \mathbb{F}_q^k$ be an arbitrary basis of F, we define a matrix $K \in \mathbb{F}_q^{t \times k}$ such that the i-th row of K is g_i for each $i \in [t]$. Let $\varphi_F \colon \mathbb{F}_q^t \to F$ denote the linear map defined as $\varphi_F(v) = K^T v, \forall v \in \mathbb{F}_q^t$. Since $\mathrm{rank}(K) = t$, φ_F is actually an isomorphism from $\mathbb{F}_q^t$ to F. For each $f_i, i \in [b]$, there is a unique way to write $f_i = \sum_{j=1}^t m_{ij} g_j$ as a $\mathbb{F}_q$-linear combination of the basis $g_1, \ldots, g_t$.

Let $M = (m_{ij}) \in \mathbb{F}_q^{b \times t}$ be the matrix corresponding these coefficients. Since $g_1, \ldots, g_t$ form a basis, so the linear subspace spanned by rows of M is exactly F, which implies $\mathrm{rank}(M) = t$. Also, since $\vec{g}_1, \ldots, \vec{g}_t$ are linear independent and $\vec{f}_1, \ldots, \vec{f}_b$ are distinct, it is clear that M has distinct rows. Therefore, let $U \subseteq \mathbb{F}_q^b$ denote the linear subspace spanned by columns of M. Namely, let $d_1, \ldots, d_t \in \mathbb{F}_q^b$ the columns of M such that $d_i = M[:i], i \in [t]$, we know that $U = \mathrm{Span}(d_1, \ldots, d_t)$. We claim that $U \in \mathcal{L}_{\mathsf{Dist}}(\mathbb{F}_q^b)$. To show this, for any $u \ne v \in [b]$, since M has distinct rows, $M[u:] \ne M[v:]$. This means for some $w \in [t]$ there is $M[u, w] \ne M[v, w]$, so the w-th column $M[: w] = d_w \in U$ satisfies that $d_{w,u} \ne d_{w,v}$. Therefore, we know $U \in \mathcal{L}_{\mathsf{Dist}}(\mathbb{F}_q^b)$. Since $\mathrm{rank}(M) = \dim(U) = t$, we know $d_1, \ldots, d_t$ form a basis of U. We define the linear map $\varphi \colon \mathbb{F}_q^b \to \mathbb{F}_q^t$ as $\varphi(v) = M^\top v$ for all $v \in \mathbb{F}_q^b$. Since $\mathrm{rank}(M) = t$, φ is surjective (epimorphism).

Then, let $R' = R + \mu + 1/n$, from Fact 2.3 we know there is some proper linear subspace $W \subsetneq U$ such that

$$\Phi(\mathcal{V}, U, R') - \Phi(\mathcal{V}, W, R') \le 0.$$

Let $m = \dim(W) \ge 0$. Note that $m < t$ since W is a proper linear subspace of U. There must be some surjective linear map (epimorphism) $\psi \colon \mathbb{F}_q^\top \to \mathbb{F}_q^m$ such that $\ker(\psi \circ \varphi) \subseteq \mathbb{F}_q^b$ is exactly $W^\perp$. To show the existence of ψ, there are two cases. If $m = 0$, then ψ must be trivial and we are done. Otherwise, let $w_1, \ldots, w_m \in W \subsetneq U \subseteq \mathbb{F}_q^b$ denote a basis of W. There is a unique way to write $w_i = \sum_{j=1}^t h_{ij} d_j$ as an $\mathbb{F}_q$-linear combination for each $i \in [m]$. Let $H = (h_{ij}) \in \mathbb{F}_q^{m \times t}$, the linear map $\psi \colon \mathbb{F}_q^t \to \mathbb{F}_q^m$ defined as $\psi(v) = Hv, \forall v \in \mathbb{F}_q^t$ satisfies the requirement since $(HM^\top)[i] = w_i, \forall i \in [m]$, which means $\ker(\psi \circ \varphi) = \mathrm{Span}(w_1, \ldots, w_m)^\perp = W^\perp$. ψ is surjective since the rows of H are $w_1, \ldots, w_m$, which are linearly independent.

Let $N = \ker(\psi) \subseteq \mathbb{F}_q^t$, we know $\dim(N) = t - m \ge 1$ since ψ is surjective. we consider the linear space $N' = \varphi_F(N) \subseteq F \subseteq \mathbb{F}_q^k$. Since φ_F is injective, it follows that $\dim(N') = t - m \le b$.

Recall that $\mathcal{V} = (V_1, \ldots, V_n) \in \mathcal{L}(\mathbb{F}_q^b)^n$ is the interested b-local profile, we have the following claim

Claim 3.2. *For any $i \in [n]$, there is $\varphi_F(\varphi(V_i^\perp) \cap N) \subseteq N' \cap \ker(\pi_i)$.*

Proof. Fix any $i \in [n]$, our proof is splitted into two pieces.

(1) $\varphi_F(\varphi(V_i^\perp) \cap N) \subseteq N'$: Since $N' = \varphi_F(N)$, this part is trivial.

(2) $\varphi_F(\varphi(V_i^\perp) \cap N) \subseteq \ker(\pi_i)$: For any $v \in V_i^\perp$, it suffices to prove $(\pi_i \circ \varphi_F \circ \varphi)(v) = 0$. By the definition of π_i, let $H_i \in \mathbb{F}_q^{s \times k}$ denote the matrix such that $\pi_i(f) = H_i f, \forall f \in \mathbb{F}_q^k$. Therefore, the target is equivalent to $H_i K^\top M^\top v = 0$. It suffices to show that for any $j \in [s]$, the j-th row $z_j \in \mathbb{F}_q^b$ of $H_i K^\top M^\top \in V_i$. Actually, since j-th row of $H_i K^\top$ is $(\pi_i(g_1)[j], \ldots, \pi_i(g_t)[j]) \in \mathbb{F}_q^t$

by definition, and $f_u = \sum_{v=1}^{t} M[u,v]g_v, \forall u \in [b]$, by $\mathbb{F}_q$-linearity of $\mathcal{C}$, we know that

$$\begin{aligned} z_j &= (\sum_{v=1}^{t} \pi_i(g_v)[j]M^\top[v,1], \ldots, \sum_{v=1}^{t}]\pi_i(g_v)[j]M[v,b]) \\ &= \left(\pi_i\left(\sum_{v=1}^{t} g_v M[1,v]\right)[j], \ldots, (\pi_i\left(\sum_{v=1}^{t} g_v M[b,v]\right)[j]\right) \\ &= (\pi_i(f_1)[j], \ldots, \pi_i(f_b)[j]) \in V_i. \end{aligned}$$

This completes the proof of the claim.

□

Since φ_F is injective. $\dim(\varphi_F(\varphi(V_i^\perp) \cap N)) = \dim(\varphi(V_i^\perp) \cap N)$. By Claim 3.2, it follows that $\dim(N' \cap \ker(\pi_i)) \geq \dim(\varphi(V_i^\perp) \cap N)$. Since $\dim(N') \leq b$ and $\pi_1, \ldots, \pi_n$ are $(\dim(N'), (R+\mu)\dim(N')n)$-subspace designable, it follows that

$$(R+\mu)\dim(N')n \geq \sum_{i=1}^{n} \dim(N' \cap \ker(\pi_i)) \geq \sum_{i=1}^{n} \dim(\varphi(V_i^\perp) \cap N) \tag{2}$$

Let us calculate $\dim(\varphi(V_i^\perp) \cap N)$. Since $N = \ker(\psi)$, we have,

$$\dim(\psi(\varphi(V_i^\perp))) = \dim(\varphi(V_i^\perp)) - \dim(N \cap \varphi(V_i^\perp))$$

This implies

$$c_i = \dim(\varphi(V_i^\perp) \cap N) = \dim(\varphi(V_i^\perp)) - \dim(\psi(\varphi(V_i^\perp)))$$

For each $i \in [n]$ let $D_i \in \mathbb{F}_q^{b \times (b - \dim(V_i))}$ denote the matrix such that the linear subspace spanned by its columns is exactly $V_i^\perp$ and define the linear map $\phi_i : \mathbb{F}_q^b \to \mathbb{F}_q^{b-\dim(V_i)}$ such that $\phi_i(v) = D_i^\top v, \forall v \in \mathbb{F}_q^b$, then $\ker(\phi_i) = V_i$. We compute c_i by definition as follows:

$$\begin{aligned} \dim(\varphi(V_i^\perp)) - \dim(\psi(\varphi(V_i^\perp))) &= \operatorname{rank}(M^\top D_i) - \operatorname{rank}(HM^\top D_i) \\ &= \operatorname{rank}(D_i^\top M) - \operatorname{rank}(D_i^\top M H^\top) \\ &= \dim(\phi_i(U)) - \dim(\phi_i(W)) \\ &= (\dim(U) - \dim(U \cap \ker(\phi_i))) - (\dim(W) - \dim(W \cap \ker(\phi_i))) \\ &= (\dim(U) - \dim(U \cap V_i)) - (\dim(W) - \dim(W \cap V_i)) \end{aligned}$$

Note that the third line above relies on the facts that the linear subspace spanned by columns of M is U and the linear subspace spanned by columns of $MH^\top$, which is the subspace spanned by rows of $HM^\top$, is exactly W, as discussed in previous paragraphs. It follows that

$$\begin{aligned} \sum_{i=1}^{n} c_i &\geq \sum_{i=1}^{n} (\dim(U) - \dim(U \cap V_i)) - (\dim(W) - \dim(W \cap V_i)) \\ &= \Phi(\mathcal{V}, W, R') - \Phi(\mathcal{V}, U, R') - R'n(\dim(W) - \dim(U)) \\ &\geq R'n(\dim(U) - \dim(W)) \\ &= (R + \mu + 1/n)n\dim(N') > (R+\mu)\dim(N')n. \end{aligned}$$

This contradicts to (2), so the assumed pairwise distinct $f_1, \ldots, f_b$ do not exist. We conclude that $\mathcal{C}$ does not contain $\mathcal{V}$. □

4 RLCs Simulate Local Properties Shared by all Optimal Subspace Designable Codes

In this section, we show the easier direction of the local equivalence between subspace designs and random linear codes. Namely, our target is to prove that for any local profile $\mathcal{V}$, if it can be guaranteed to be avoided by all optimal subspace designs, then it can be avoided by random linear code with high probability. As a direct corollary, we show in Corollary 4.3 that list-recoverability guaranteed by optimal subspace designs also holds for random linear codes. In a follow-up work [BCDZ25], the authors use this reduction to prove the nearly-optimal list-recoverability of random linear codes, as well as random RS codes by a further reduction established in [LMS25].

Technical Overview. The proof framework is as follows. In Theorem 4.1, we prove random folded linear codes yield nearly-optimal subspace designs with high probability, so all local properties guaranteed by optimal subspace designs also hold for random folded linear codes with high probability. Then, for any folding parameter s and local profile $\mathcal{V}$, we observe that the values of potential functions (1) satisfy $s\Phi(U, \mathcal{V}, R) = \Phi(U, \mathcal{V}^{(s)}, R)$, where $\mathcal{V}^{(s)}$ is the s-duplicated version of $\mathcal{V}$ which matches the s-folded codes. Therefore, the rate thresholds satisfy $R_{\mathcal{V}} = R_{\mathcal{V}^{(s)}}$ so local properties of random folded linear codes also hold for the plain random linear codes, which completes the reduction from subspace designs to random linear codes.

Theorem 4.1. *Fix positive integers k, n, s, q, d where $k \le sn, d < s$, $\varepsilon \in (0, 1)$ and let rate $R = k/(sn)$. A random $\mathbb{F}_q$-linear $C \subseteq (\mathbb{F}_q^s)^n$ is a $(d, (R+\varepsilon)dn)$ subspace designable code with probability at least $1 - q^{-\varepsilon sdn+3d^2n+3n}$.*

Proof. The generator matrix of the random $\mathbb{F}_q$-linear code C can be seen as a random matrix of shape $k \times sn$ whose entries are uniformly and independently sampled from $\mathbb{F}_q$. Let $M_i \in \mathbb{F}_q^{k\times s}, i \in [n]$ denote the sub-matrix of this random matrix consisting of its $((i-1)s+1)$-th to (is)-th column. We need to show that, with probability at least $1 - q^{-\varepsilon sdn+3d^2n+3n}$, for any d-dimensional linear subspace of $\mathbb{F}_q^k$ encoded as a matrix $W \in \mathbb{F}_q^{k\times d}$ with rank d, there is

$$f(W) := \sum_{i=1}^{n} \operatorname{rank}(M_i^\top W) \ge (1 - R - \varepsilon)dn.$$

We fix an arbitrary matrix $W \in \mathbb{F}_q^{k\times d}$ with rank d. By union bound, since the number of different W is at most $q^{kd} = q^{Rdsn}$, it suffices to prove that with probability at most $q^{-(\varepsilon+R)dsn+3d^2n+3n}$, there is $f(W) < (1 - R - \varepsilon)dn$.

For any sequence $A = (a_1, \ldots, a_n) \in \{0, 1, \ldots, d\}^n$, we call A a valid sequence if the sum $S(A) := \sum_{i=1}^n a_i < (1 - R - \varepsilon)dn$. Let E_A denote the event that $\operatorname{rank}(M_i^\top W) = a_i$ for all $i \in [n]$. We only need to bound the probability that E_A happens for some valid sequence A. The number of valid sequences is at most $\binom{(2-R-\varepsilon)n}{n} \le (e(2 - R - \varepsilon))^n \le (2e)^n \le q^{3n}$. If we fix some arbitrary valid sequence A, by union bound, we only need to show that E_A happens with probability at most $q^{-(\varepsilon+R)dsn+3d^2n}$.

We can directly compute $\Pr[E_A]$ as follows

$$\Pr[E_A] = \prod_{i=1}^{n} \Pr[\operatorname{rank}(M_i^\top W) = a_i].$$

Fix any $i \in [n]$, our target is to compute $\Pr[\operatorname{rank}(M_i^\top W) = a_i]$. since M_i is a uniformly random matrix and W has full column rank. $\Pr[\operatorname{rank}(M_i^\top W) = a_i]$ is the same as the probability that

a uniformly random matrix $P \in \mathbb{F}_q^{s\times d}$ has rank a_i. It suffices to bound the number of matrices $P \in \mathbb{F}_q^{s\times d}$ with rank a_i. If P has rank a_i, then there exists a subset $S \subseteq [d]$ of columns of size $|S| = a_i$ such that columns in S are linearly independent, and all the other columns are linear combinations of columns in S. Fix such an S, the number of matrices P satisfying above conditions is at most $q^{sa_i+a_i(d-a_i)}$. Since there are $\binom{d}{a_i}$ choices of S, it follows that

$$\Pr[\mathrm{rank}(M_i^\top W) = a_i] = \Pr[\mathrm{rank}(P) = a_i] \le \binom{d}{a_i} q^{-sd} q^{sa_i+a_i(d-a_i)} \le q^{d\log_q d-(s-a_i)(d-a_i)}$$

Since $\sum_{i=1}^n (d-a_i) \ge (R+\varepsilon)dn$, there is

$$\Pr[E_A] = \prod_{i=1}^n \Pr[\mathrm{rank}(M_i^\top W) = a_i] \le q^{nd\log_q d-(s-d)(\varepsilon+R)dn} \le q^{d^2n-(\varepsilon+R)sdn+2d^2n} \le q^{-(\varepsilon+R)sdn+3d^2n}$$

□

Then we show that if all optimal subspace designable codes does not contain a local profile $\mathcal{V}$, then random linear codes also do not contain $\mathcal{V}$.

Theorem 4.2. *Fix $n, b, q, d \ge 1, R \in (0,1)$ and any b-local profile $\mathcal{V} = (V_1, \ldots, V_n) \in \mathcal{L}(\mathbb{F}_q^b)^n$. If for all large enough s, we have that all d-**subspace designable** s-folded $\mathbb{F}_q$-linear codes $\mathcal{C} \subseteq (\mathbb{F}_q^s)^n$ with rate R does not contain $\mathcal{V}$, then it follows that $R_{\mathcal{V}} \ge R - (b^2+1)/n$.*

Proof. We can choose a large enough $s \ge \Omega(d^3 n)$ such that a random $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq (\mathbb{F}_q^s)^n$ is a $(d', Rd'n+1)$ subspace designable code for all $1 \le d' \le d$ with probability at least $2/3$ by Theorem 4.1.

let $\mathcal{C}' \subseteq \mathbb{F}_q^{sn}$ denote the "unfolded" random $\mathbb{F}_q$-linear code $\mathcal{C}$ with block length sn and define the s-duplicated b-local profile $\mathcal{V}^{(s)} := (V_1, \ldots, V_1, V_2, \ldots, V_2, \ldots, V_n, \ldots, V_n) \in \mathcal{L}(\mathbb{F}_q^b)^{sn}$ to be the b-local profile with length sn derived from $\mathcal{V}$ such that each V_i is repeated s times. From the statement, we know that $\mathcal{C}'$ does not contain $\mathcal{V}^{(s)}$ with probability at least $2/3$.

Then we observe that the threshold rate $R_{\mathcal{V}^{(s)}} = R_{\mathcal{V}}$. The reason is that for any $U \in \mathcal{L}(\mathbb{F}_q^b)$, by the definition of the potential function there is $\Phi(\mathcal{V}^{(s)}, U, R) = s\Phi(\mathcal{V}, U, R)$, and the rate threshold $R_{\mathcal{V}^{(s)}}$ only depends on signs of $\Phi(\mathcal{V}^{(s)}, U, R) - \Phi(\mathcal{V}^{(s)}, W, R)$ where $W \subsetneq U, U \in \mathcal{L}(\mathbb{F}_q^b)$. These signs do not change by replacing $\mathcal{V}^{(s)}$ with $\mathcal{V}$.

However, suppose by contrapositive that $R_{\mathcal{V}^{(s)}} = R_{\mathcal{V}} < R-(b^2+1)/n$, we know that the random $\mathbb{F}_q$-linear code $\mathcal{C}'$ with length sn contains $\mathcal{V}^{(s)}$ with probability at least $1 - q^{-1} \ge 1/2$ by the first item of Theorem 2.4, which contradicts the fact that $\mathcal{C}'$ does not contain $\mathcal{V}^{(s)}$ with probability at least $2/3$. □

The second item of Theorem 1.3 is proved by combining Theorem 4.2 and the second item of Theorem 2.4.

As a corollary, we conclude that list-recoverability guaranteed by optimal subspace designable codes can also be attained by random linear codes if the alphabet size q is large enough.

Corollary 4.3. *Fix constants $\ell, L, d \ge 1, \varepsilon, \rho, R \in (0,1), q \ge (3\ell)^{2(L+1)/\varepsilon}$. 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 $1 - o_n(1)$.*

Proof. By [LMS25, Proposition 2.2], we can construct a series of $(L+1)$-local profiles $\mathcal{V}_1, \dots, \mathcal{V}_m$, where $m = \binom{n}{\rho n}^{L+1} \ell^{(L+1)n} \le \binom{n}{n/2}^{L+1} \ell^{(L+1)n} \le (2e)^{(L+1)n/2} \ell^{(L+1)n} \le (3\ell)^{(L+1)n}$, such that $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq (\mathbb{F}_q)^n$ is (ρ, ℓ, L) list-recoverable iff $\mathcal{C}$ does not contain all these $(L+1)$-local profiles. Note that for any s-folded $\mathbb{F}_q$-linear code $\mathcal{C}' \subseteq (\mathbb{F}_q^s)^n$, we also know that $\mathcal{C}'$ is (ρ, ℓ, L) list-recoverable iff $\mathcal{C}'$ does not contain $\mathcal{V}_1, \dots, \mathcal{V}_m$. (Recall that $\mathcal{C}'$ does not contain some $\mathcal{V}_i$ means the unfolded version of $\mathcal{C}'$ does not contain $\mathcal{V}_i^{(s)}$). Then, by Theorem 4.2, we know that for any $\mathcal{V}_i, i \in [m]$, it follows that $R_{\mathcal{V}_i} \ge R - (L^2 + 2L + 2)/n$. Therefore, from Theorem 2.4, for a random $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq (\mathbb{F}_q)^n$, we know that

$$\forall i \in [m], \quad \Pr[\mathcal{C} \text{ contains } \mathcal{V}_i] \le q^{-\varepsilon n + (L+1)^2} \le (3\ell)^{-2(L+1)n + 2(L+1)^3/\varepsilon}$$

By a union bound over all these local profiles, it implies that

$$\begin{aligned}
\Pr[\mathcal{C} \text{ is not } (\rho, \ell, L) \text{ list-recoverable}] &\le \sum_{i=1}^{m} \Pr[\mathcal{C} \text{ contains } \mathcal{V}_i] \\
&\le (3\ell)^{(L+1)n} (3\ell)^{-2(L+1)n + 2(L+1)^3/\varepsilon} \\
&= (3\ell)^{-(L+1)n + 2(L+1)^3/\varepsilon} \le o_n(1).
\end{aligned}$$

□

5 Applications to Matroid Theory

A primary application of our random-to-explicit reduction is contribute new algorithms in matroid theory. We now present a few standard definitions in matroid theory (e.g., [Oxl06]).

A matroid is a pair $\mathcal{M} = (X, \mathcal{I})$, where X is a *ground set* and $\mathcal{I}$ is a set of subsets of X known as *independent sets* subject to the conditions (1) that $\varnothing \in I$, (2) if $A \in \mathcal{I}$ and $B \subseteq A$ then $B \in \mathcal{I}$, and (3) if $A, B \in \mathcal{I}$, with $|B| > |A|$, then there is $x \in B \setminus A$ with $A \cup \{x\} \in \mathcal{I}$. Maximal independent sets are called *bases*. Any set $A \subseteq X$ with $A \notin \mathcal{I}$ is *dependent*. In particular, a dependent set A is a *circuit* if every proper subset of A is independent (that is A is a minimal dependent set). We say that any $A \subseteq X$ containing a basis is *spanning*.

Every matroid $\mathcal{M}$ has an associated *rank function* $r_{\mathcal{M}}$, where for any $A \subseteq X$, $r_{\mathcal{M}}(A)$ is the size of the largest independent set $B \in \mathcal{I}$ which is a subset of A. In particular, $A \subseteq X$ is independent if and only if $r_{\mathcal{M}}(A) = |A|$. We define $r_{\mathcal{M}}(X)$ (i.e., the size of every basis) to be the *rank* of $\mathcal{M}$. Given two matroids $\mathcal{M}_1 := (X, \mathcal{I}_1)$ and $\mathcal{M}_2 = (X, \mathcal{I}_2)$ on the same ground set, we say that $\mathcal{M}_1 \preceq \mathcal{M}_2$ if $\mathcal{I}_1 \subseteq \mathcal{I}_2$. In other words, $r_{\mathcal{M}_1}(A) \le r_{\mathcal{M}_2}(A)$ for all $A \subseteq X$. Given matroids $\mathfrak{M}$ on the same ground set, we say that $\mathcal{M} \in \mathfrak{M}$ is *maximal* if $\mathcal{N} \not\succ \mathcal{M}$ for all $\mathcal{N} \in \mathfrak{M}$.

By interpreting certain matroid properties as local profiles, we apply our random-to-explicit reduction to obtain novel *conditional* deterministic algorithms for computing the rank functions of various matroids. In this paper, we focus on the following three families of matroids.

Maximally Recoverable (MR) Tensor Code Matroid. Given a field $\mathbb{F}$, an $[n, k]$-code is a k-dimensional subspace C of $\mathbb{F}^n$. Motivated by applications in distributed storage, Gopalan et al. [GHK+17] studied the following code architecture. Pick parameters, $m, n, a, b \in \mathbb{N}$ and consider a $[m, m-a]$-column code C_{col} and a $[n, n-b]$ row code C_{row}. The tensor product of these codes $C_{\mathsf{col}} \otimes C_{\mathsf{row}} := \operatorname{span}\{c_{\mathsf{col}} \otimes c_{\mathsf{row}} \mid c_{\mathsf{col}} \in C_{\mathsf{col}}, c_{\mathsf{row}} \in C_{\mathsf{row}}\} \subseteq \mathbb{F}^{m \times n}$ is the set of all $m \times n$ matrices with entries from $\mathbb{F}$ where every row is a codeword in C_{row} and every column is a codeword in C_{col}.

The tensor code $C_{\mathsf{col}} \otimes C_{\mathsf{row}}$ has an associated correctability matroid on the ground set $[m] \times [n]$, where a *pattern* $E \subseteq [m] \times [n]$ is independent in the matroid if and only if one can recover from erasing the symbols associated with E. In other words, the punctured[8] code $(C_{\mathsf{col}} \otimes C_{\mathsf{row}})|_{\overline{E}}$ has dimension $(m-a)(n-b)$. We call this matroid $\mathcal{M}(C_{\mathsf{col}}, C_{\mathsf{row}})$.

For a fixed choice of m, n, a, b, there are many possible matroids $\mathcal{M}(C_{\mathsf{col}}, C_{\mathsf{row}})$. However, there is a provably unique maximal matroid of this form, which corresponds to the setting in which $\mathbb{F}$ is a characteristic zero field (e.g., $\mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$) and C_{col} and C_{row} are chosen uniformly from a continuous distribution, which we call *generic*[9] codes. In this paper, we denote this unique maximal matroid by $\mathsf{MR}(m, n, a, b)$. Since $C_{\mathsf{col}} \otimes C_{\mathsf{row}}$ has dimension $(m-a)(n-b)$, the rank of this matroid is $mn - (m-a)(n-b) = bm + an - ab$.

Bipartitie Rigidity (Birigidity) Matroid. Kalai et al. [KNN15] posed the following geometric question, which is a variant of the classical graph rigidity problem studied since the 19th century [Max64]. Consider a bipartite graph $G = (V, E)$ where V is the disjoint union of $[m]$ and $[n]$ and $E \subseteq [m] \times [n]$. Consider two embedding maps $\alpha : [m] \to \mathbb{R}^b \times \{0^a\}$ and $\beta : [n] \to \{0^b\} \times \mathbb{R}^a$. Kalai et al. [KNN15] say this embedding is *rigid* if no infinitesimal change to α and β can preserve the (ℓ_2) length of every edge E. It turns out such rigid graphs correspond to the spanning sets of a bipartite rigidity matroid with parameters (m, n, a, b). Like in the case of MR, if α and β are chosen generically, there is a unique maximal *generic birigidity matroid*, which we denote by $\mathsf{BR}(m, n, a, b)$ in this paper. See [KNN15, JT24, BDG+24a, CJJT25] for a more precise description of this matroid.

Recently Brakensiek et. al. [BDG+24a] proved all the MR and BR matroids are equal, so any properties of one such matroid apply to the other.

Theorem 5.1 (Theorem 1.1(3) of [BDG+24a], restated)**.** *For all $m, n, a, b \in \mathbb{N}$ with $m \geq a$ and $n \geq b$, we have that $\mathsf{MR}(m, n, a, b) = \mathsf{BR}(m, n, a, b)$.*

Matrix Completion. In the case where $a = b$, $\mathsf{BR}(m, n, a, a)$ has an alternative interpretation as the *matrix completion problem* (see [SC10, CJJT25]). In particular, for $E \subseteq [m] \times [n]$, imagine that the entries indexed by E are revealed in a (say, complex-valued) $m \times n$ matrix. For a generic (aka random) choice of these revealed entries, does there exist a rank a matrix $M \in \mathbb{C}^{m \times n}$ which corresponds to the revealed entries? Such questions are closely related to the *Netflix problem* in machine learning (e.g., [NKS19, DGN+25]).

For all three of these families of matroids, it is a substantial open question to give a *deterministic* polynomial time algorithm for detecting whether a pattern $E \subseteq [m] \times [n]$ is independent in these matroids (e.g., [GHK+17, HPYWZ21, BGM22, JT24, BDG+24a, CJJT25]). Such an algorithm is only known when $a = 1$ [Whi89, KNN15, GHK+17, BGM22, BGM23] or $m - a \leq 3$ [BDG+24a]. We emphasize that all three of these matroids have efficient *randomized* algorithms by invoking the Schwarz-Zippel lemma. In particular, the case $a = b = 2$ (aka rank 2 matrix completion) is unresolved [Ber17, BDG+24a, CJJT25]. However, barring the resolution of $\mathsf{RP} = \mathsf{P}$, this approach will not yield an efficient deterministic algorithm.

In an alternative direction, Jackson and Tanigawa [JT24] recently proved that the computational complexity of these rank functions lies in coNP if one makes a *conditional* assumption on the structure of these rigidity matroids (see [JT24, Conjecture 6.4]). Improving on this result, we conditionally show (under a weaker assumption) that detecting independence lies in P. More precisely,

[8] Given a code $C \subseteq \mathbb{F}^n$ and a set $A \subseteq [n]$, we let $C|_A := \{c|_A : c \in C\} \subseteq \mathbb{F}^A$ denote a puncturing of C.

[9] More precisely, "generic" refers to properties which are Zariski dense (in the sense of algebraic geometry). For our purposes, a "generic" code is a random linear code for which the relevant matroid properties hold with probability 1.

our matroid-theoretic assumption is a positive answer to a open question of Mason [Mas81], which is formalized in Conjecture 5.5.

Theorem 5.2. *Assuming Conjecture 5.5, Algorithm 1 computes whether $E \subseteq [m] \times [n]$ is independent in $\mathsf{MR}(m, n, a, b) = \mathsf{BR}(m, n, a, b)$ in deterministic $\mathrm{poly}(m, n)$ time.*

By a standard oracle reduction (e.g., [Oxl06]), this also implies a deterministic $\mathrm{poly}(m, n)$-time algorithm for the rank function of $\mathsf{MR}(m, n, a, b)$.

Proof Overview

The proof of Theorem 5.2 has a number of components which we outline as follows. Building on Section 3, our high-level goal is to show that the tensor product of two explicit folded Reed-Solomon codes "simulates" the $\mathsf{MR}(m, n, a, b)$ matroid. However, the accuracy of this simulation is contingent on the validity of Conjecture 5.5.

Section 5.1. First, we build up the necessary background needed to formally discuss Conjecture 5.5. In particular, we define the notion of an *abstract birigidity matroid* [JT24, CJJT25] which captures matroids which "look like" birigidity matroids. Conjecture 5.5 formalizes the intuition of matroid theorists that $\mathsf{MR}(m, n, a, b)$ is the (unique) maximal abstract birigidity matroid. We remark that Conjecture 5.5 is equivalent to a positive answer to a much older question due to Mason [Mas81].

Section 5.2. Inspired by the potential functions of [LMS25], we define a potential function that is (unconditionally) at least the rank function of $\mathsf{MR}(m, n, a, b)$. We show this potential function satisfies the axioms of a matroid and that this matroid is an (m, n, a, b) abstract birigidity matroid. As such, by Conjecture 5.5, we have that this potential function *is* the rank function of $\mathsf{MR}(m, n, a, b)$.

Section 5.3. Even with these facts in hand, directly computing this potential function is still difficult, as it corresponds to the behavior of the tensor product of two random linear codes. By adapting the framework of Section 3, we show that this potential function can be approximated by the tensor product of two explicit folded[10] Reed-Solomon codes. To do this, we actually need a two-phase approach. First, we show that the tensor product of two random linear codes is closely approximated by the tensor product of one random linear code with a folded Reed-Solomon code. Then, we swap the roles of the two codes being tensored and construct a new potential function which allows us to replace the remaining random linear code with another folded Reed Solomon code. Unlike most applications of folded Reed Solomon codes, the folding parameters need to be of size $\mathrm{poly}(m, n)$ so that the folded Reed-Solomon sufficiently approximate the worst-case rank loss by the FRS codes.

Section 5.4. Finally, we present Algorithm 1, which constructs two folded Reed-Solomon codes, takes their tensor product, and performs a (linear algebra) rank computation to obtain the rank function of $\mathsf{MR}(m, n, a, b)$. The analysis is a straightforward combination of the tools built in the previous sections.

[10] Although we are using the theory of folded Reed–Solomon codes, in the actual analysis we "unfold" the Reed–Solomon codes and adjust the erasure patterns accordingly through what we call *scaling*.

5.1 Abstract Bipartite Rigidity Matroids

For the remainder of this section, we assume $\mathbb{F}$ is a field with characteristic 0 (e.g., $\mathbb{Q}, \mathbb{R}, \mathbb{C}$). To properly discuss Conjecture 5.5, we need to introduce the notion of an *abstract birigidity matroid* (see [JT24, CJJT25]). There are a few equivalent definitions (see Theorem 5.29 of [CJJT25]), but the following is the most convenient for our use case.

Definition 5.3 (e.g., [JT24, CJJT25])**.** For parameters (m, n, a, b), we say that a matroid $\mathcal{M}$ on round set $[m] \times [n]$ is an (m, n, a, b)-abstract birigidity matroid if it meets the following conditions.

- The rank of $\mathcal{M}$ is $bm + an - ab$.
- For every $A \subseteq [m]$ of size $a + 1$ and every $B \subseteq [n]$ of size $b + 1$, we have $A \times B$ is a circuit.

To gain some intuition, we first prove that ordinary tensor codes are an example of abstract birigidity matroids if we make the assumption that C_{col} and C_{row} are *MDS* codes. In particular, an $[n, k]$-code $C \subseteq \mathbb{F}^n$ is MDS it attains the Singleton bound: every nonzero codeword has Hamming weight at least $n - k + 1$. In matroid theory, such MDS codes correspond to *uniform* matroids, where every subset of $[n]$ of size $n - k$ is a basis.

Proposition 5.4. *For any $[m, m - a]$-MDS code C_{col} and $[n, n - b]$-MDS code C_{row}, we have that the correctability matroid for $C_{\mathsf{col}} \otimes C_{\mathsf{row}}$ is an (m, n, a, b) abstract birigidity matroid. Thus, $\mathsf{MR}(m, n, a, b)$ is an (m, n, a, b) abstract birigidity matroid.*

Proof. As previously discussed, the rank of the correctability matroid is $mn - (m - a)(n - b) = bm + an - ab$, as desired. It suffices to check for every $A \subseteq [m]$ of size $a + 1$ and $B \subseteq [n]$ of size $b + 1$ that $A \times B$ is a circuit.

First, too see that $A \times B$ is dependent in $C_{\mathsf{col}} \otimes C_{\mathsf{row}}$, note that since C_{col} is $m - a$-dimensional, there exists at least one nonzero $u \in C_{\mathsf{col}}$ supported on A. Likewise, there is at least one $v \in C_{\mathsf{row}}$ supported on B. The codeword $u \otimes v$ is supported entirely on $A \times B$. Thus, erasing $A \times B$ makes $u \otimes v$ unrecoverable. Therefore, $A \times B$ is dependent.

However, consider any $(a, b) \in A \times B$, we claim that $A \times B \setminus \{(a, b)\}$ is independent. The bth column has exactly a erasures. Thus, by using the column parity checks of C_{col}, we can recover the entire column $[m] \times \{b\}$. This leaves our erasure pattern as $A \times (B \setminus \{b\})$. Every row of this pattern has at most b erasures, so we can use the parity checks of C_{row} to recover the rest of the codeword. Thus, $A \times B \setminus \{(a, b)\}$ is independent. □

Conjecture 5.5 (Conjecture 5.30 [CJJT25], restated)**.** $\mathsf{BR}(m, n, a, b) = \mathsf{MR}(m, n, a, b)$ *is the maximal (m, n, a, b) abstract birigidity matroid.*

This conjecture is equivalent to an affirmative answer to an open question raised by Mason [Mas81] over 40 years ago on the most general possible tensor product of two uniform matroids. We also note that the conditional assumption made by Jackson and Tanigawa [JT24] is a stronger assumption than Conjecture 5.5 that particular rank estimation techniques in the generic bipartite rigidity matroid are perfectly accurate [Lar25].

Remark 5.6. We now discuss the current evidence in the literature for and against Conjecture 5.5. Much of this evidence is presented in Section 5 of the recent rigidity survey [CJJT25].

Currently, the strongest evidence for Conjecture 5.5 being true is that it has been proved in the special cases when $a = 1$ [Whi89, KNN15, GHK+17] or $m - a \leq 3$ [BDG+24a] (with other parameters arbitrary). Of note, the truth of Conjecture 5.5 when $a = 1$ led [BGM23] to connect the structure of higher order MDS codes to the recent algorithms for computing non-commutative ranks

[GGOW20]. We note that the resolution of these cases $a = 1$ and $m - a \leq 3$ imply Algorithm 1 is unconditionally correct in these settings, although efficient deterministic algorithms were already known in such cases [BGM22, BDG+24a].

Conversely, the strongest evidence against Conjecture 5.5 is that the natural analogue of the conjecture for (traditional) non-bipartite rigidity (where the entire graph is embedded into the same space) is false when the ambient dimension is 4 or greater. In fact, such counterexamples have been known for over 30 years–see the discussion surrounding Conjecture 5.7.1 in [GSS93] as well as the discussion in Section 5.3.2 of [CJJT25]. However, no analogue of these constructions has been found in the non-bipartite setting which disproves Conjecture 5.5.

To mitigate such concerns, we do not need the full power of Conjecture 5.5 to prove Theorem 5.2. In particular, the maximality of $\mathsf{MR}(m, n, a, b)$ is not strictly required; rather, we merely need that $\mathsf{MR}(m, n, a, b)$ is equal to the corresponding "potential matroid" which we construct in Section 5.2. Thus, if one is pessimistic about the validity of Conjecture 5.5, one could use the novel matroid construction in Section 5.2 as a new plan of attack toward generating counterexamples toward Conjecture 5.5 and negatively answering the question of Mason [Mas81].

We also briefly touch on the coding theory implication if the fragment of Conjecture 5.5 we use is false. In short, it would imply that the tensor product of two (random) folded linear codes has *strictly* better[11] maximally recoverability guarantees than the tensor product of two (random) linear codes. In other words, for practical applications (see discussion in [GHK+17]), it may be preferable to consider a folded linear architecture when designing tensor codes. For example, in [CCS25, Section 6], the authors use the tensor product of two explicit folded linear codes to construct graph codes.

5.2 The Potential Matroid

Fix parameters $m, n, a, b \in \mathbb{N}$. Fix an $[m, m-a]$ code $C_{\mathsf{col}} \in \mathbb{F}^m$. Given a set $A \subseteq [m]$, we let $\mathbb{F}^A \subseteq \mathbb{F}^m$ denote the vector space spanned by the indicator vectors indexed by A. Inspired by [LMS25], we now define the following potential function Φ on subsets $E \subseteq [m] \times [n]$ as follows.

$$\Phi(E) := \max_{U \subseteq C_{\mathsf{col}}} \left[-b \dim(U) + \sum_{j=1}^{n} \dim(U \cap \mathbb{F}^{E_j}) \right], \tag{3}$$

where for all $j \in [n]$, $E_j := \{i \in [m] \mid (i, j) \in E\}$. Further define

$$r(E) := |E| - \Phi(E). \tag{4}$$

Our first goal is to prove that r is the rank function of a matroid. Toward this, we need the following subspace inequality.

Claim 5.7. *For any subspaces $X_1, X_2, Y_1, Y_2 \subseteq \mathbb{F}_q^m$, we have that*

$$\dim(X_1 \cap Y_1) + \dim(X_2 \cap Y_2) \leq \dim((X_1 \cap X_2) \cap (Y_1 \cap Y_2)) + \dim((X_1 + X_2) \cap (Y_1 + Y_2)).$$

Proof. Observe that

$$\begin{aligned} \dim(X_1 \cap Y_1) + \dim(X_2 \cap Y_2) - \dim((X_1 \cap X_2) \cap (Y_1 \cap Y_2)) &= \dim((X_1 \cap Y_1) + (X_2 \cap Y_2)) \\ &\leq \dim((X_1 + X_2) \cap (Y_1 + Y_2)), \end{aligned}$$

[11] In fact, the folded RS codes will have a slightly smaller rate. However, it is a general phenomenon in coding theory that explicitly simulating random linear codes requires a slack from the threshold, so an arbitrarily small rate decrease as in our case should be in expectation. See Section III of [BDGZ25] for a theory of *approximate* MR tensor codes with a rate slack.

where the last inequality follows from the fact that $X_1 \cap Y_1 \subseteq (X_1 + X_2) \cap (Y_1 + Y_2)$ and $X_2 \cap Y_2 \subseteq (X_1 + X_2) \cap (Y_1 + Y_2)$. □

We now prove that r is the rank function of a matroid.

Lemma 5.8. *There exists a matroid $\mathcal{M}(C_{\mathsf{col}}, n, b)$ over $[m] \times [n]$ with rank function r.*

Proof. To show that r is the rank function of a matroid, we have to prove the following properties (see Corollary 1.3.4 from [Oxl06])

1. $r(E) \leq |E|$ for all $E \subseteq [m] \times [n]$.
2. $r(E) \geq 0$ for all $E \subseteq [m] \times [n]$.
3. For all $E \subseteq F$, we have that $r(E) \leq r(F)$.
4. r is submodular: for all $E, F \subseteq [m] \times [n]$, we have that $r(E \cap F) + r(E \cup F) \leq r(E) + r(F)$.

Item 1. First, by picking $U = 0$, we can see that $\Phi(E) \geq 0$. Thus, Item 1 immediately holds.

Item 2. Further, for any $U \subseteq C_{\mathsf{col}}$, we have that

$$-b \dim(U) + \sum_{j=1}^{n} \dim(U \cap \mathbb{F}^{E_j}) \leq \sum_{j=1}^{n} |E_j| = |E|.$$

So, $\Phi(E) \leq |E|$, or $r(E) \geq 0$, proving Item 2.

Item 3. For $E \subseteq F$, to show that $r(E) \leq r(F)$, note that for any $U \subseteq C_{\mathsf{col}}$, we have that

$$\begin{aligned} -b \dim(U) + \sum_{j=1}^{n} \dim(U \cap \mathbb{F}^{E_j}) &\geq -b \dim(U) + \sum_{j=1}^{n} \left[\dim(U \cap \mathbb{F}^{F_j}) - |F_j \setminus E_j|\right] \\ &= -|F \setminus E| - b \dim(U) + \sum_{j=1}^{n} \dim(U \cap \mathbb{F}^{F_j}). \end{aligned}$$

This implies that $\Phi(E) \geq \Phi(F) - |F \setminus E|$, which implies that $r(E) \leq r(F)$, proving Item 3.

Item 4. Pick $U_E, U_F \subseteq C_{\mathsf{col}}$ such that

$$\Phi(E) = -b \dim(U_E) + \sum_{j=1}^{n} \dim(U_E \cap \mathbb{F}^{E_j})$$

$$\Phi(F) = -b \dim(U_F) + \sum_{j=1}^{n} \dim(U_F \cap \mathbb{F}^{F_j})$$

Further observe that

$$\Phi(E \cap F) \geq -b \dim(U_E \cap U_F) + \sum_{j=1}^{n} \dim((U_E \cap U_F) \cap \mathbb{F}^{E_j \cap F_j})$$

$$\Phi(E \cup F) \geq -b \dim(U_E + U_F) + \sum_{j=1}^{n} \dim((U_E + U_F) \cap \mathbb{F}^{E_j \cup F_j}).$$

Note that $\mathbb{F}^{E_j \cap F_j} = \mathbb{F}^{E_j} \cap \mathbb{F}^{F_j}$ and $\mathbb{F}^{E_j \cup F_j} = \mathbb{F}^{E_j} + \mathbb{F}^{F_j}$. Using Claim 5.7, we have that

$$\begin{aligned}
\Phi(E \cap F) + \Phi(E \cup F) &\geq -b \dim(U_E \cap U_F) + \sum_{j=1}^{n} \dim((U_E \cap U_F) \cap (\mathbb{F}^{E_j} \cap \mathbb{F}^{F_j})) \\
&\quad - b \dim(U_E + U_F) + \sum_{j=1}^{n} \dim((U_E + U_F) \cap (\mathbb{F}^{E_j} + \mathbb{F}^{F_j})) \\
&\geq -b \dim(U_E) - b \dim(U_F) + \sum_{j=1}^{n} \left[\dim(U_E \cap \mathbb{F}^{E_j}) + \dim(U_F \cap \mathbb{F}^{F_j})\right] \\
&= \Phi(E) + \Phi(F).
\end{aligned}$$

Since $|E| + |F| = |E \cap F| + |E \cup F|$, we have that $r(E \cap F) + r(E \cup F) \leq r(E) + r(F)$, proving Item 4.

Thus, r is indeed the rank function of a matroid. □

We remark that $\Phi(E) = |E| - r(E)$ is called the *corank* function of $\mathcal{M}(C_{\mathsf{col}}, n, b)$. We next show that $\mathcal{M}(C_{\mathsf{col}}, n, b)$ has more independent sets than $\mathcal{M}(C_{\mathsf{col}}, C_{\mathsf{row}})$.

Lemma 5.9. *Let $C_{\mathsf{row}} \subseteq \mathbb{F}^n$ be an arbitrary $[n, n-b]$ code. If E is a correctable erasure pattern for $C_{\mathsf{col}} \otimes C_{\mathsf{row}}$, then E is an independent set of $\mathcal{M}(C_{\mathsf{col}}, n, b)$.*

Proof. We prove the contrapositive: assume that E is a dependent set of $\mathcal{M}(C_{\mathsf{col}}, n, b)$, we seek to show that the erasure pattern E is not correctable in $C_{\mathsf{col}} \otimes C_{\mathsf{row}}$. Thus, $\Phi(E) \geq 1$. This means there exists $U \subseteq C_{\mathsf{col}}$ such that

$$-b \dim(U) + \sum_{j=1}^{n} \dim(U \cap \mathbb{F}^{E_j}) \geq 1.$$

We now invoke the a dimension-counting argument. Let $\mathbb{F}^m \otimes C_{\mathsf{row}}$ be the set of $m \times n$ matrices each of whose m rows lies in C_{row}. Let $\bigoplus_{j=1}^{n}(U \cap \mathbb{F}^{E_j})$ be the set of $m \times n$ matrices, such that for all $j \in [n]$, the jth row lies in U and is supported on E_j. We see that

$$\begin{aligned}
&\dim\left[\mathbb{F}^m \otimes C_{\mathsf{row}} \cap \bigoplus_{j=1}^{n}(U \cap \mathbb{F}^{E_j})\right] \\
&= \dim\left[U \otimes C_{\mathsf{row}} \cap \bigoplus_{j=1}^{n}(U \cap \mathbb{F}^{E_j})\right] \\
&= \dim(U \otimes C_{\mathsf{row}}) + \sum_{j=1}^{n} \dim(U \cap \mathbb{F}^{E_j}) - \dim\left[U \otimes C_{\mathsf{row}} + \bigoplus_{j=1}^{n}(U \cap \mathbb{F}^{E_j})\right] \\
&\geq (n-b)\dim(U) + (b\dim(U) + 1) - \dim(U \otimes \mathbb{F}^n) \\
&= 1,
\end{aligned}$$

Thus, there exists a nonzero codeword $c \in \mathbb{F}^m \otimes C_{\mathsf{row}} \cap \bigoplus_{j=1}^{n}(U \cap \mathbb{F}^{E_j}) \subseteq C_{\mathsf{col}} \otimes C_{\mathsf{row}}$. In other words, $C_{\mathsf{col}} \otimes C_{\mathsf{row}}$ has a nonzero codeword supported on E. Therefore, E is not a correctable erasure pattern in $C_{\mathsf{col}} \otimes C_{\mathsf{row}}$, as desired. □

Next, we prove that $\mathcal{M}(C_{\mathsf{col}}, n, b)$ is an abstract rigidity matroid when C_{col} is MDS.

Lemma 5.10. *If C_{col} is an MDS $[m, m-b]$ code, then $\mathcal{M}(C_{\mathsf{col}}, n, b)$ is an (m, n, a, b) abstract rigidity matroid.*

Proof. First, we need to show that the rank of $\mathcal{M}(C_{\mathsf{col}}, n, b)$ is $bm + an - ab$. To see why, observe that for all $U \subseteq C_{\mathsf{col}}$, we have that

$$-b \dim(U) + \sum_{j=1}^{n} \dim(U \cap \mathbb{F}^{[m]}) = (n-b) \dim(U).$$

Thus, $\Phi([m] \times [n]) = (n-b) \dim(C_{\mathsf{col}}) = (n-b)(m-a)$. Thus, $r([m] \times [n]) = mn - (m-a)(n-b) = bm + an - ab$, as desired.

Second, we seek to show that for any $A \subseteq [m]$ of size $a+1$ and $B \subseteq [n]$ of size $b+1$ that $A \times B$ is a circuit of $\mathcal{M}(C_{\mathsf{col}}, n, b)$. First, to see why $A \times B$ is dependent, let $U_A \subseteq C_{\mathsf{col}}$ be the set of codewords supported on A. Since C_{col} is an $[m, m-a]$ MDS code and $|A| = a+1$, we have that $\dim(U_A) = 1$. Thus,

$$\Phi(A \times B) \geq -b \dim(U_A) + \sum_{j \in B} \dim(U_A \cap \mathbb{F}^A) = -b + (b+1) = 1.$$

Thus, $r(A \times B) < |A \times B|$, so $A \times B$ is dependent.

Pick any $a \in A$ and $b \in B$. By Proposition 5.4, we have that $A \times B \setminus \{(a, b)\}$ is an independent set of $C_{\mathsf{col}} \times C_{\mathsf{row}}$ for any $[n, n-b]$ MDS code $C_{\mathsf{row}} \subseteq \mathbb{F}^n$. Thus, by Lemma 5.9, we have that $A \times B \setminus \{(a, b)\}$ is an independent set of $\mathcal{M}(C_{\mathsf{col}}, n, b)$. □

We conclude this section with the following observation. If $C_{\mathsf{col}} \subseteq \mathbb{F}^m$ is a generic $[m, m-a]$ code and $C_{\mathsf{row}} \subseteq \mathbb{F}^n$ is a generic $[n, n-b]$ code, then both codes are MDS (e.g., [BGM22]). Further, we have by Lemma 5.9 that $\mathcal{M}(C_{\mathsf{col}}, n, b) \succeq \mathcal{M}(C_{\mathsf{col}}, C_{\mathsf{row}}) = \mathsf{MR}(m, n, a, b)$. Since $\mathcal{M}(C_{\mathsf{col}}, n, b)$ is an (m, n, a, b) abstract tensor matroid by Lemma 5.10, we have the following corollary of Conjecture 5.5.

Corollary 5.11. *Assume Conjecture 5.5. Let $C_{\mathsf{col}} \subseteq \mathbb{F}^m$ be a generic $[m, m-a]$ code, then $\mathcal{M}(C_{\mathsf{col}}, n, b) = \mathsf{MR}(m, n, a, b)$.*

This corollary will be of use in the next section, where we seek to replace C_{row} (and later C_{col}) with a folded Reed-Solomon code.

5.3 Replacing Generic Codes with FRS

Building on the techniques of Section 3, we show how to replace the generic codes C_{col} and C_{row} with suitable (folded) Reed-Solomon codes. More precisely, fix parameters $m, n, a, b \in \mathbb{N}$. Fix parameters $t := 2m^2 n$ and $d := mn$ and construct the following datum:

- Let $b' := bt + d$.
- Pick $\beta_1, \ldots, \beta_n \in \mathbb{F}$ and $\gamma \in \mathbb{F}$ such that the set $Z := \{\alpha_i \gamma^j \mid i \in [n], j \in \{0, 1, \ldots, t-1\}\}$ has exactly tn elements.
- Let $C_{\mathsf{row}}^{\mathsf{RS}} \subseteq \mathbb{F}^{tn}$ be the $[tn, tn-b']$ Reed-Solomon code with evaluation points from Z. That is, $C_{\mathsf{row}}^{\mathsf{RS}} = \mathsf{RS}^{\mathbb{F}}_{tn, tn-b'}(\beta_1, \gamma\beta_1, \ldots, \gamma^{t-1}\beta_1, \ldots, \beta_n, \gamma\beta_n, \ldots, \gamma^{t-1}\beta_n)$.

One acceptable choice of parameters (as done in Line 1) is to set $\gamma = 2$ and let $\beta_1, \ldots, \beta_n$ be consecutive odd integers.

We seek to compare the matroid $\mathcal{M}(C_{\mathsf{col}}, C_{\mathsf{row}})$ with $\mathcal{M}(C_{\mathsf{col}}, C_{\mathsf{row}}^{\mathsf{RS}})$. However, the matroids are on different ground sets. To correct for this, we need to "scale" an erasure pattern $E \subseteq [m] \times [n]$ as follows.

Definition 5.12 (Pattern scaling)**.** Given $E \subseteq [m] \times [n]$ and parameter $s, t \in \mathbb{N}$, we define the (s,t)-scaling of E to be the pattern $E^{s,t} \subseteq [sm] \times [tn]$ such that

- if $(i,j) \in E$ then $(s(i-1)+x, t(j-1)+y) \in E^{s,t}$ for all $(x,y) \in [s] \times [t]$, and
- if $(i,j) \notin E$ then $(s(i-1)+x, t(j-1)+y) \notin E^{s,t}$ for all $(x,y) \in [s] \times [t]$.

The main goal of this section is to prove the following key "scaling" lemma.

Lemma 5.13. *For all $E \subseteq [m] \times [n]$ we have that E is an independent set of $\mathcal{M}(C_{\mathsf{col}}, n, b)$ if and only $E^{1,t}$ is an independent set of $\mathcal{M}(C_{\mathsf{col}}, C_{\mathsf{row}}^{\mathsf{RS}})$.*

The proof of Lemma 5.13 requires a careful adaptation of the techniques of Section 3. In some sense, the adapted argument in this section is simpler, as we do not require the distinctness condition needed in Section 3.

5.3.1 Dependent Sets Are Preserved

As a first step toward proving Lemma 5.13, we show that if E is a dependent set of $\mathcal{M}(C_{\mathsf{col}}, n, b)$, then $E^{1,t}$ is a dependent set of $\mathcal{M}(C_{\mathsf{col}}, C_{\mathsf{row}}^{\mathsf{RS}})$. The proof is an application of Lemma 5.9.

Proposition 5.14. *If E is a dependent set of $\mathcal{M}(C_{\mathsf{col}}, n, b)$ then $E^{1,t}$ is a dependent set of $\mathcal{M}(C_{\mathsf{col}}, nt, b')$ and thus a dependent set of $\mathcal{M}(C_{\mathsf{col}}, C_{\mathsf{row}}^{\mathsf{RS}})$.*

Proof. Since E is a dependent set of $\mathcal{M}(C_{\mathsf{col}}, n, b)$, we have that $\Phi(E) \geq 1$. In other words, for all $U \subseteq C_{\mathsf{col}}$, we have that

$$\sum_{j=1}^{n} \dim(U \cap \mathbb{F}^{E_j}) \geq b \dim(U) + 1 \geq \left(b + \frac{1}{m}\right) \dim(U).$$

Let Φ' be the corresponding corank function of the matroid $\mathcal{M}(C_{\mathsf{col}}, tn, b')$. Note then that

$$\begin{aligned}
\Phi'(E^{1,t}) &= \max_{U \subseteq C_{\mathsf{col}}} \left[-b' \dim(U) + \sum_{j=1}^{tn} \dim(U \cap \mathbb{F}^{E_j^{1,t}}) \right] \\
&= t \max_{U \subseteq C_{\mathsf{col}}} \left[-\frac{b'}{t} \dim(U) + \sum_{j=1}^{n} \dim(U \cap \mathbb{F}^{E_j}) \right] \\
&\geq t \max_{U \subseteq C_{\mathsf{col}}} \left[-\frac{b'}{t} \dim(U) + \left(b + \frac{1}{m}\right) \dim(U) \right] \\
&= tm \left(b + \frac{1}{m} - \frac{b'}{t}\right) > 0,
\end{aligned}$$

where we use the fact that $b' = bt + d < bt + \frac{t}{m}$. Thus, $E^{1,t}$ is dependent in $\mathcal{M}(C_{\mathsf{col}}, nt, b')$. By Lemma 5.9, we have that $E^{1,t}$ is dependent in $\mathcal{M}(C_{\mathsf{col}}, C_{\mathsf{row}}^{\mathsf{RS}})$, as desired. □

5.3.2 Independent Sets Are Preserved

Next, we show the converse of Proposition 5.14, which is sufficient to prove Lemma 5.13.

Proposition 5.15. *If $E^{1,t}$ is a dependent set of $\mathcal{M}(C_{\mathsf{col}}, C_{\mathsf{row}}^{\mathsf{RS}})$ then E is a dependent set of $\mathcal{M}(C_{\mathsf{col}}, n, b)$.*

Similar to argument in Section 3, the proof of Proposition 5.15 crucially uses the subspace design properties underlying $C^{\mathsf{RS}}_{\mathsf{row}}$. We use the following variant of the subspace design conditions proved in Section 6.

Proposition 5.16. *For $j \in [n]$, let $I_j := \{(j-1)t+1, (j-1)t+2, \ldots, jt\}$. For any linear subcode $V \subseteq C^{\mathsf{RS}}_{\mathsf{row}}$ for which $\dim(V) \le t$, we have that*

$$\sum_{j=1}^{n} \dim(V|_{I_j}) \ge n \dim(V) - \frac{\dim(V)(tn - b' - \dim(V))}{t - \dim(V) + 1}.$$

We defer the proof of Proposition 5.16 to Section 6.1.4.

Proof of Proposition 5.15. Assume that $E^{1,t}$ is a dependent set of $\mathcal{M}(C_{\mathsf{col}}, C^{\mathsf{RS}}_{\mathsf{row}})$. Thus, there is a nonzero matrix $M \in C_{\mathsf{col}} \times C^{\mathsf{RS}}_{\mathsf{row}}$ which is supported on $E^{1,t}$. Let $U_M := \mathrm{colspan}(M) \subseteq C_{\mathsf{col}}$. We seek to show that

$$-b \dim(U_M) + \sum_{j=1}^{n} \dim(U_M \cap \mathbb{F}^{E_j}) > 0, \tag{5}$$

as this would prove that E is a dependent set of $\mathcal{M}(C_{\mathsf{col}}, n, b)$. Let $V_M := \mathrm{rowspan}(M) \subseteq C^{\mathsf{RS}}_{\mathsf{row}}$, and note that $\dim(U_M) = \dim(V_M) = \mathrm{rank}\, M \le m < t$. By Proposition 5.16, we have that

$$\sum_{j=1}^{n} \dim(V_M|_{I_j}) \ge n \dim(U_M) - \frac{\dim(U_M)(tn - b' - \dim(U_M))}{t - \dim(U_M) + 1}.$$

For all $j \in [n]$, let $M|_{I_j}$ be the restriction of M to the columns indexed by I_j. Since $V_M|_{I_j}$ is precisely the rowspan of $M|_{I_j}$ we have that $\dim(V_M|_{I_j}) \le \dim \mathrm{colspan}(M|_{I_j}) \le \dim(U_M \cap \mathbb{F}^{E_j})$. Therefore, we have that

$$\begin{aligned}
&-b \dim(U_M) + \sum_{j=1}^{n} \dim(U_M \cap \mathbb{F}^{E_j}) \\
&\qquad \ge (n-b)\dim(U_M) - \frac{\dim(U_M)(tn - b' - \dim(U_M))}{t - \dim(U_M) + 1} \\
&\qquad \ge \dim(U_M)\left[n - b - \frac{tn - b' - \dim(U_M)}{t - \dim(U_M) + 1}\right] \\
&\qquad \ge n - b - \frac{tn - b' - 1}{t - m + 1} && \text{(since } U_M \neq 0\text{)} \\
&\qquad = \frac{(n-b)(t-m+1) - tn + tb + d + 1}{t - m + 1} \\
&\qquad = \frac{d + 1 - (m-1)(n-b)}{t - m + 1} > 0,
\end{aligned}$$

since $d = mn > (m-1)(n-b)$, as desired. This proves (5), completing the proof. □

5.3.3 Tensoring Two Reed-Solomon Codes

As a near-immediate corollary of Lemma 5.13, we show that both C_{col} and C_{row} can be replaced by suitable RS codes. To do this, let $s = 8m^5n^4$ and $d' = 2m^3n^2$.

- Let $a' := sa + d'$.
- Pick $\alpha_1, \ldots, \alpha_m \in \mathbb{F}$ and $\gamma \in \mathbb{F}$ such that the set $Y := \{\alpha_i \gamma^j \mid i \in [n], j \in \{0, 1, \ldots, s-1\}\}$ has exactly sm elements.
- Let $C^{\mathsf{RS}}_{\mathsf{col}} \subseteq \mathbb{F}^{sm}$ be the $[sm, sm - a']$ Reed-Solomon code with evaluation points from Z.

Again, we may set $\gamma = 2$ and $\alpha_1, \ldots, \alpha_m$ to be consecutive odd integers. Since $s = 2(2m^2n^2)^2 n$ and $d' = (2m^2n^2)m$, by Lemma 5.13, we have the following corollary.

Corollary 5.17. *Let C'_{row} be any $[tn, tn - b']$ code. For all $E \subseteq [2m^2n^2] \times [m]$ we have that E is an independent set of $\mathcal{M}(C'_{\mathsf{row}}, m, a)$ if and only $E^{1,s}$ is an independent set of $\mathcal{M}(C'_{\mathsf{row}}, C^{\mathsf{RS}}_{\mathsf{col}})$.*

By the theory of Section 5.2, we have our key structural result.

Lemma 5.18. *Assuming Conjecture 5.5, $E \subseteq [m] \times [n]$ is an independent set of $\mathsf{MR}(m, n, a, b)$ if and only if $E^{s,t}$ is an independent set of $\mathcal{M}(C^{\mathsf{RS}}_{\mathsf{col}}, C^{\mathsf{RS}}_{\mathsf{row}})$.*

Proof. Pick (generic) $[m, m-a]$ code C_{col} and $[n, n-b]$ code C_{row} such that $\mathcal{M}(C_{\mathsf{col}}, C_{\mathsf{row}}) = \mathsf{MR}(m, n, a, b)$. By Lemma 5.9, any independent set E of $\mathsf{MR}(m, n, a, b)$ is an independent set of $\mathcal{M}(C_{\mathsf{col}}, n, b)$. By Lemma 5.13, we have that $E^{1,t}$ is an independent set of $\mathcal{M}(C_{\mathsf{col}}, C^{\mathsf{RS}}_{\mathsf{row}})$. Let $F \subseteq [n] \times [m]$ be the "transpose" of E. Then, $F^{t,1}$ is an independent set of $\mathcal{M}(C^{\mathsf{RS}}_{\mathsf{row}}, C_{\mathsf{col}})$. Thus, by Lemma 5.9, we have that $F^{t,1}$ is an independent set of $\mathcal{M}(C^{\mathsf{RS}}_{\mathsf{row}}, m, a)$. By Corollary 5.17 with $C'_{\mathsf{row}} = C^{\mathsf{RS}}_{\mathsf{row}}$, we have that $F^{t,s}$ is an independent set of $\mathcal{M}(C^{\mathsf{RS}}_{\mathsf{row}}, C^{\mathsf{RS}}_{\mathsf{col}})$, so $E^{s,t}$ is an independent set of $\mathcal{M}(C^{\mathsf{RS}}_{\mathsf{row}}, C^{\mathsf{RS}}_{\mathsf{col}})$.

For the other direction, assume E is dependent in $\mathcal{M}(C_{\mathsf{col}}, C_{\mathsf{row}})$. By Corollary 5.11, assuming Conjecture 5.5, we have that E is dependent in $\mathcal{M}(C_{\mathsf{col}}, n, b)$. Pick a generic $[tn, tn - b']$ code C'_{row} such that we have $\mathcal{M}(C_{\mathsf{col}}, C'_{\mathsf{row}}) = \mathsf{MR}(m, tn, a, b')$. By Proposition 5.14, we have that $E^{1,t}$ is a dependent set of $\mathcal{M}(C_{\mathsf{col}}, tn, b') \succeq \mathsf{MR}(m, tn, a, b') = \mathcal{M}(C_{\mathsf{col}}, C'_{\mathsf{row}})$. Thus, $F^{t,1}$ is a dependent set of $\mathcal{M}(C'_{\mathsf{row}}, C_{\mathsf{col}}) = \mathsf{MR}(tn, m, b', a) = \mathcal{M}(C'_{\mathsf{row}}, m, a)$, where the latter equality holds by Corollary 5.11 assuming Conjecture 5.5. By Proposition 5.14, we have that $F^{t,s}$ is a dependent set of $\mathcal{M}(C'_{\mathsf{row}}, C^{\mathsf{RS}}_{\mathsf{col}})$. Thus, $E^{s,t}$ is a dependent set of $\mathcal{M}(C^{\mathsf{RS}}_{\mathsf{col}}, C_{\mathsf{row}})$ and thus is a dependent set of $\mathcal{M}(C^{\mathsf{RS}}_{\mathsf{col}}, C^{\mathsf{RS}}_{\mathsf{row}})$. □

5.4 Proof of Theorem 5.2

We next present Algorithm 1 which attempts to compute the rank function $\mathsf{MR}(m, n, a, b)$. In the algorithm, we assume that $\mathbb{F} = \mathbb{Q}$. The correctness of this algorithm is conditional on Conjecture 5.5.

To complete the proof of Theorem 5.2, we need to prove that Algorithm 1 is correct (assuming Conjecture 5.5) and that Algorithm 1 it indeed runs in deterministic polynomial time.

Correctness. The correctness follows immediately by Lemma 5.18.

Runtime Analysis. We note that this algorithm runs in polynomial time unconditionally, as checking whether $E^{s,t}$ is independent in $C^{\mathsf{RS}}_{\mathsf{col}} \otimes C^{\mathsf{RS}}_{\mathsf{row}}$ is equivalent to checking that the dimension of $(C^{\mathsf{RS}}_{\mathsf{col}} \otimes C^{\mathsf{RS}}_{\mathsf{row}})|_{\overline{E^{s,t}}}$ is $(sm - a')(tn - b')$. This is equivalent to computing the rank of a matrix with $\mathrm{poly}(m, n)$ entries each of which is an integer representable in $\mathrm{poly}(m, n)$ bits. The rank of this matrix can be computed in polynomial time as Gaussian elimination can be done in strongly polynomial time over $\mathbb{Q}$ [Sch86].

Algorithm 1: (Conditional) Independence Oracle

Input: Parameters $m, n, a, b \in \mathbb{N}$. Pattern $E \subseteq [m] \times [n]$.

Output: Whether E is independent in $\mathsf{MR}(m, n, a, b)$

$s := 8m^5n^4$;

$t := 2m^2n$;

$a' := sa + 2m^3n^2$;

$b' := sb + mn$;

$\alpha_1, \ldots, \alpha_m := 1, 3, \ldots, 2m-1$;

$\beta_1, \ldots, \beta_n := 1, 3, \ldots, 2n-1$;

$\gamma := 2$;

$C^{\mathsf{RS}}_{\mathsf{col}} := \mathsf{RS}^{\mathbb{Q}}_{sm,sm-a'}(\alpha_1, \gamma\alpha_1, \ldots, \gamma^{s-1}\alpha_1, \ldots, \alpha_n, \gamma\alpha_n, \ldots, \gamma^{s-1}\alpha_m)$;

$C^{\mathsf{RS}}_{\mathsf{row}} := \mathsf{RS}^{\mathbb{Q}}_{tn,tn-b'}(\beta_1, \gamma\beta_1, \ldots, \gamma^{t-1}\beta_1, \ldots, \beta_n, \gamma\beta_n, \ldots, \gamma^{t-1}\beta_n)$;

if *$E^{s,t}$ is independent in $C^{\mathsf{RS}}_{\mathsf{col}} \otimes C^{\mathsf{RS}}_{\mathsf{row}}$* **then**

  return *INDEPENDENT;*

end

return *DEPENDENT*;

6 Improvements and Limitations for Subspace Designs

We now return to $\mathbb{F}$ representing an arbitrary field (possibly finite). Recall that a collection of vector spaces $H_1, \ldots, H_n \subseteq \mathbb{F}^k$ each of codimension s form an (ℓ, A)-strong subspace design for some $\ell \leq s$ if for all ℓ-dimensional $U \subseteq \mathbb{F}^k$, we have that

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

Likewise, we say that these spaces form an (ℓ, A)-weak subspace design if for all ℓ-dimensional $U \subseteq \mathbb{F}^k$, we have that

$$\sum_{i=1}^{n} \mathbf{1}[H_i \cap U \neq 0] \leq A.$$

As shown by this paper, and many prior works (e.g., [GK16, GXY18, Tam24, CZ25]), strong and weak subspace designs have proved important in near-optimal explicit constructions for various coding theory problems. Thus, we seek to better understand what is the optimal choice of A for various choices of $\mathbb{F}, n, k, \ell$. Toward this problem, we present two results, the first improves on the well-known bound of Guruswmai and Kopparty [GK16].

Theorem 6.1. *Assume that $|\mathbb{F}| > ns$, then there exists an explicit choice of $H_1, \ldots, H_n \subseteq \mathbb{F}^k$ of codimension s which forms an $(\ell, \lfloor \frac{\ell(k-\ell)}{s-\ell+1} \rfloor)$ strong subspace design.*

This improves on Guruswami and Kopparty's bound of $\lfloor \frac{\ell(k-1)}{s-\ell+1} \rfloor$ by using a near-identical construction and a slightly more refined analysis.

Our second result, more surprisingly, shows that Theorem 6.1 is tight when $\mathbb{F}$ is an algebraically closed field and n is sufficiently large.

Theorem 6.2. *Let $\mathbb{F}$ be an algebraically closed field (of any characteristic), then for any $H_1, \ldots, H_n \subseteq \mathbb{F}^k$ of codimension s (possibly with repetition), if $n \leq \frac{\ell(k-\ell)}{s-\ell+1}$, then there exists an ℓ-dimensional sub-*

space $U \subseteq \mathbb{F}^k$ which has nontrivial intersection with each H_i. In other words, if $n \geq \lfloor \frac{\ell(k-\ell)}{s-\ell+1} \rfloor$ then a $(\ell, \lfloor \frac{\ell(k-\ell)}{s-\ell+1} \rfloor - 1)$ weak subspace design does not exist.

The main technique toward proving Theorem 6.2 is to use Schubert calculus to analyze how the conditions $U \cap H_i$ affect the structure of the projective variety induced by all ℓ-dimensional subspaces of $\mathbb{F}^k$ (a.k.a., the Grassmannian). We prove Theorem 6.1 and Theorem 6.2 in Section 6.1 and Section 6.2, respectively. However, Theorem 6.2 does not apply over non-algebraically closed fields. See Section 6.3 for a counterexample.

6.1 An Improved Analysis of Guruswami–Kopparty

Toward proving Theorem 6.1, we begin by discussing the subspace design construction of Guruswami–Kopparty [GK16] and then explaining how to improve upon their analysis. First, observe that $\mathbb{F}^k$ is in bijection with the vector space of polynomials $f \in \mathbb{F}[x]_{<k}$ of degree less than k. Pick a nonzero element $\gamma \in \mathbb{F}$ of order at least k, as well as nonzero $\alpha_1, \ldots, \alpha_n$, we call this choice of $\gamma, \alpha_1, \ldots, \alpha_n$ *appropriate* if all of

$$\{\gamma^{j-1}\alpha_i : (i,j) \in [n] \times [s]\}$$

are distinct. Given an appropriate choice, Guruswami–Kopparty construction $H_1, \ldots, H_n \subseteq \mathbb{F}^k$ as follows. For each $i \in [n]$, let H_i be the set of all polynomials $f \in \mathbb{F}[x]_{<k}$ with $\alpha_1, \gamma\alpha_1, \ldots, \gamma^{s-1}\alpha_1$ as roots. By the appropriate condition, each H_i has codimension s.

We now seek to show that $(H_1, \ldots, H_n)$ form a strong subspace design with the parameters of Theorem 6.1. Fix an ℓ-dimensional $U \subseteq \mathbb{F}[x]_{<k}$ as well as a polynomial basis $f_1, \ldots, f_\ell$ of U. Recall from Definition 2.1, the *Wronskian* of this basis is as follows

$$W_\gamma(f_1, \ldots, f_\ell)(X) \stackrel{\text{def}}{=} \begin{pmatrix} f_1(X) & \cdots & f_\ell(X) \\ f_1(\gamma X) & \cdots & f_\ell(\gamma X) \\ \vdots & \ddots & \vdots \\ f_1\left(\gamma^{\ell-1}X\right) & \cdots & f_\ell\left(\gamma^{\ell-1}X\right) \end{pmatrix},$$

where X is a symbolic variable (i.e., the entries of the matrix lie in $\mathbb{F}[X]$). Note our application is a bit more general than Definition 2.1, as we no longer assume γ is a multiplicative generator. The following lemma is key.

Lemma 6.3. *Let $p(X) = \det W_\gamma(f_1, \ldots, f_\ell)(X)$. Then, p has the following properties.*

(a) If the multiplicative order of γ is at least k, then $p(X) \neq 0$.

(b) The degree of $p(X)$ is at most $\ell k - \binom{\ell+1}{2}$.

(c) $X^{\binom{\ell}{2}}$ is a factor of $p(X)$.

(d) If $\dim(H_i \cap U) = d_i$, then $(X - \alpha_1)^{d_i}, \ldots, (X - \gamma^{s-\ell}\alpha_1)^{d_i}$ are factors $p(X)$.

Note that (a), (b), (c) improve upon Guruswami–Kopparty in various ways, while (d) is identical. more precisely, for (a), Guruswami–Kopparty assume that γ is a multiplicative generator of $\mathbb{F}$, although we relax that to just needing a lower bound on the order of γ. For (b), we improve over their bound of $\ell(k-1)$, and no observation like (c) appears in [GK16]. Assuming Lemma 6.3, Theorem 6.1 follows easily.

Proof of Theorem 6.1. Construct $H_1, \dots, H_n \subseteq \mathbb{F}^k$ as indicated above. Consider any ℓ-dimensional $W \subseteq \mathbb{F}^k$ as well as a corresponding nonzero polynomial $p(X)$ of Lemma 6.3. By Lemma 6.3(b), we know that $\deg p \le \ell k - \binom{\ell+1}{2}$. By Lemma 6.3(c) 0 is a root of $p(X)$ $\binom{\ell}{2}$ times. By Lemma 6.3(d) we know that each of $\alpha_i, \dots, \gamma^{s-\ell}\alpha_i$ is are roots of p with multiplicity at least $\dim(H_i \cap U)$ each. Thus, since $\alpha_1, \dots, \alpha_n, \gamma$ are appropriate, we have that

$$\ell k - \binom{\ell+1}{2} \ge \deg p \ge \binom{\ell}{2} + \sum_{i=1}^{n} (s - \ell + 1) \dim(H_i \cap U).$$

Thus,

$$\frac{\ell(k-\ell)}{s-\ell+1} \ge \sum_{i=1}^{n} \dim(H_i \cap U),$$

as desired. □

We now proceed to prove the various parts of Lemma 6.3.

6.1.1 Proof of Lemma 6.3(a) and (b)

This proof technique appears in [Gur11], but we give the argument for completeness.[12] Recall that $W_\gamma(f_1, \dots, f_\ell)(X)$ depends on the choice of basis $f_1, \dots, f_\ell$ of U. However, any two bases $f_1, \dots, f_\ell$ and $g_1, \dots, g_\ell$ of U are related by an invertible matrix $Q \in \mathbb{F}^{\ell \times \ell}$ where $g_i = \sum_{j=1}^{\ell} Q_{i,j} f_j$. As such, it is not hard to see then that

$$W_\gamma(g_1, \dots, g_\ell)(X) = W_\gamma(f_1, \dots, f_\ell)(X) Q^\top,$$

In particular,

$$\det W_\gamma(g_1, \dots, g_\ell)(X) = \det W_\gamma(f_1, \dots, f_\ell)(X) \det Q,$$

where $\det Q$ is a nonzero element of $\mathbb{F}$. Thus, for any of (a)-(d) in Lemma 6.3, we may freely pick a basis of U which is most convenient for that part. For parts (a) and (b), we consider a basis $f_1, \dots, f_\ell$ of U for which $\deg f_1 < \deg f_2 < \cdots < \deg f_\ell < k$. For each $i \in [\ell]$, let $d_i = \deg f_i$. Furthermore, let $c_1, \dots, c_\ell \in \mathbb{F}^\times$ be the leading coefficients of $f_1, \dots, f_\ell$.

It is clear that if $p(X) = \det W_\gamma(f_1, \dots, f_\ell)(X)$ is nonzero, then $\deg p \le d_1 + \cdots + d_\ell \le (k-\ell) + (k-(\ell-1)) + \cdots + (k-1) = \ell k - \binom{\ell+1}{2}$. Thus, (a) implies (b). To show (a), we prove that the coefficient $X^{d_1 + \cdots + d_\ell}$ of $p(X)$ is nonzero. To see why, note that the coefficient of $X^{d_1+\cdots+d_\ell}$ in the expansion of $\det W_\gamma(f_1, \dots, f_\ell)(X)$ is

$$\sum_{\sigma \in S_\ell} (-1)^\sigma \prod_{i=1}^{\ell} c_i (\gamma^{\sigma(i)-1} X)^{d_i} = \gamma^{-\ell} \prod_{i=1}^{\ell} c_i X^{d_i} \cdot \left[\sum_{\sigma \in S_s} (-1)^\sigma \gamma^{d_1 \sigma(1) + \cdots + d_\ell \sigma(\ell)} \right],$$

where S_ℓ is the set of permutations of $[\ell]$ and $(-1)^\sigma$ is the sign of a particular permutation $\sigma \in S_\ell$. Now observe that

$$\sum_{\sigma \in S_\ell} (-1)^\sigma \gamma^{d_1 \sigma(1) + \cdots + d_\ell \sigma(\ell)} = \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \gamma^{d_1} & \gamma^{d_2} & \dots & \gamma^{d_\ell} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma^{(\ell-1)d_1} & \gamma^{(\ell-1)d_2} & \dots & \gamma^{(\ell-1)d_\ell} \end{pmatrix}.$$

This is nonzero only if $\gamma^{d_i} = \gamma^{d_j}$ for some i and j. But, since the order of γ is at least k, this cannot happen. Thus, we have proved (a) and also (b).

[12] See also https://www.cnblogs.com/Elegia/p/18738181/wronskian

6.1.2 Proof of Lemma 6.3(c)

As mentioned in Section 6.1.1, we may pick a most convenient basis to prove this part. By computing a suitable row-echelon form of U, we may assume that our basis $f_1, \ldots, f_s$ of U has the property that f_i is divisible by X^{i-1} for all $i \in [\ell]$. Thus, $p(X)$ must be divisible by $\prod_{i=1}^{\ell} X^{i-1} = X^{\binom{\ell}{2}}$, as desired.

6.1.3 Proof of Lemma 6.3(d)

Assume that $\dim(H_i \cap U) = d_i$. Thus, there exists a basis $f_1, \ldots, f_\ell$ of W for which $f_1, \ldots, f_{d_i} \in H_i$. Now for any $\beta \in \{\alpha_i, \ldots, \gamma^{s-\ell}\alpha_i\}$, observe that the first d_i columns of $W_\gamma(f_1, \ldots, f_\ell)(\beta)$ are identically zero. That is, each of the first d_i columns of $W_\gamma(f_1, \ldots, f_\ell)(X)$ are divisible by $X - \beta$. Thus, $p(X)$ must be divisible by $(X-\beta)^{d_i}$ for all $\beta \in \{\alpha_i, \ldots, \gamma^{s-\ell}\alpha_i\}$, as desired.

Remark 6.4. If $\dim(H_i \cap U) \geq 2$, then we can identify additional roots of $p(X)$ (e.g., $\gamma^{-1}\alpha_i$). This allow for a tighter analysis in various applications, although we defer such arguments to future work.

6.1.4 Proof of Proposition 5.16

We now prove Proposition 5.16, which we state in more generality as follows.

Proposition 6.5. *Let $C^{\mathsf{RS}} \subseteq \mathbb{F}^{sn}$ be an $[sn, k]$ Reed-Solomon code with evaluation points*

$$(\alpha_1, \gamma\alpha_1, \ldots, \gamma^{s-1}\alpha_1, \ldots, \alpha_n, \gamma\alpha_n, \ldots, \gamma^{s-1}\alpha_n).$$

For $i \in [n]$, let $I_i := \{s(i-1)+1, s(i-1)+2, \ldots, si\}$. For any subcode $V \subseteq C^{\mathsf{RS}}$ for which $\dim(V) \leq s$, we have that

$$\sum_{i=1}^{n} \dim(V|_{I_i}) \geq n \dim(V) - \frac{\dim(V)(k - \dim(V))}{s - \dim(V) + 1}. \tag{6}$$

Proof. Let $\psi : \mathbb{F}_{<k}[x] \to C^{\mathsf{RS}}$ be the canonical encoding map of $\mathbb{C}^{RS}$. That is,

$$\psi(f) = (f(\alpha_1), f(\gamma\alpha_1), \ldots, f(\gamma^{s-1}\alpha_1), \ldots, f(\alpha_n), f(\gamma\alpha_n), \ldots, f(\gamma^{s-1}\alpha_n)).$$

Since $V \subseteq C^{\mathsf{RS}}$ is a subcode, there exists a unique $U \subseteq \mathbb{F}_{<k}[x]$ with $\dim(U) = \dim(V)$ for which $\psi(U) = V$.

Let $H_1, \ldots, H_n \subseteq \mathbb{F}_{<k}[x]$ be spaces of codimension s such that H_i corresponds to polynomials of degree less than k with $\{\alpha_i, \gamma\alpha_i, \ldots, \gamma^{s-1}\alpha_i\}$ as roots. By Theorem 6.1, we have that

$$\sum_{i=1}^{n} \dim(H_i \cap U) \leq \frac{\dim(U)(k - \dim(U))}{s - \dim(U) + 1} = \frac{\dim(V)(k - \dim(V))}{s - \dim(V) + 1}.$$

Thus, to prove (6), it suffices to prove that $\dim(V|_{I_i}) = \dim(U) - \dim(U \cap H_i)$ for all $j \in [n]$. Given $u \in U$, we have that $\psi(u)|_{I_i} = 0^s$ if and only if $u \in H_i$. In other words, $\dim V|_{I_i} = \dim \psi(U)|_{I_i} = \dim(U) - \dim(H_i \cap U)$, as desired. □

6.2 Lower Bounds over Algebraically Closed Fields

We now turn toward proving limitations on subspace designs. To prove Theorem 6.2, we first need some machinery from algebraic geometry.

6.2.1 Grassmaniann and Plücker Coordinates

Note that a subspace design is a list of algebraic conditions for all ℓ-dimensional $W \subseteq \mathbb{F}^k$. The set of all such subspaces is known as the *Grassmannian* $\mathrm{Gr}(\ell, \mathbb{F}^k)$ (see [LB15] for a comprehensive reference). To study $\mathrm{Gr}(\ell, \mathbb{F}^k)$ algebraically, we use what are known as *Plücker coordinates*. More precisely, we can identify any ℓ-dimensional $U \subseteq \mathbb{F}^k$ with a matrix $M_U \in \mathbb{F}^{\ell \times k}$ whose ℓ rows form a basis of U. For each $S \in \binom{[k]}{\ell}$, we define the Sth Plücker coordainte to be $p_S(U) := \det(M_U|_S)$, where $|_S$ is the restriction to the columns indexed by S. Now, observe that different bases M_U of U may produce different Plücker coordinates. However, one can show that any two sets of Plücker coordiantes of W have the same up to a global nonzero scalar (i.e., $p_S(U) = \lambda q_S(U)$ for some $\lambda \in \mathbb{F}^\times$ for all $S \in \binom{[k]}{\ell}$). In other words, we think of $\mathrm{Gr}(\ell, \mathbb{F}^k)$ as a *projective* variety. A crucial fact we shall use is that the dimension of $\mathrm{Gr}(\ell, \mathbb{F}^k)$ is $\ell(k-\ell)$ [Har92, LB15].

6.2.2 Schubert Variety

Recall that a weak subspace design consists of a number of constraints of the form $\dim(H \cap U) \geq 1$, where H is a fixed subspace and U is selected from the Grassmannian $\mathrm{Gr}(\ell, \mathbb{F}^k)$. The set $V_H \subseteq \mathrm{Gr}(\ell, \mathbb{F}^k)$ of U which satisfy this condition is a special case of a *Schubert (sub)variety*.

Definition 6.6 (Schubert Variety, (e.g., [LB15]))**.** Given a vector space $\mathbb{F}^k = \langle e_1, \ldots, e_k \rangle$ and an integer $\ell \in \{0, 1, \ldots, k\}$, consider a sequence $\vec{a} = (a_1, \ldots, a_\ell)$ be a sequence of integers $1 \leq a_1 < a_2 < \cdots < a_\ell \leq k$. We then define

$$\mathrm{Sch}_{\vec{a}}(\ell, e_1, \ldots, e_k) := \{U \in \mathrm{Gr}(\ell, \mathbb{F}^k) : \forall i \in [\ell], \dim(W \cap \langle e_j : j \in [a_i] \rangle) \geq i\}.$$

In particular, if $\vec{a} = (k-\ell+1, k-\ell+2, \ldots, k)$, then $\mathrm{Sch}_{\vec{a}}(\ell, e_1, \ldots, e_k) = \mathrm{Gr}(\ell, \mathbb{F}^k)$ because every $U \in \mathrm{Gr}(\ell, \mathbb{F}^k)$ satisfies

$$\begin{aligned} \dim(U \cap \langle e_j : j \in [k-\ell+i] \rangle) &\geq \dim(U) + \dim(\langle e_j : j \in [k-\ell+i] \rangle) - k \\ &= \ell + k - \ell + i - k \geq i. \end{aligned} \tag{7}$$

Besides the fact that each $\mathrm{Sch}_{\vec{a}}$ is a projective variety, we also need the following formula for the (Krull) dimension (see [Har77] for a precise definition) of each variety.

Theorem 6.7 (e.g., Theorem 5.3.7 [LB15])**.** *For all $\vec{a} = (a_1, \ldots, a_\ell)$ with $1 \leq a_1 < a_2 < \cdots < a_\ell \leq k$, we have that*

$$\dim \mathrm{Sch}_{\vec{a}}(\ell, e_1, \ldots, e_k) = \sum_{i=1}^{\ell} (a_i - i).$$

In particular, the choice $\vec{a} = (k-\ell+1, k-\ell+2, \ldots, k)$ implies that $\dim \mathrm{Gr}(\ell, \mathbb{F}^k) = \ell(k-\ell)$ (Corollary 5.3.8 [LB15]). As an immediate corollary of Theorem 6.7, we can compute the dimension of each $V_H := \{U \in \mathrm{Gr}(\ell, \mathbb{F}^k) : V_H \cap U \neq 0\}$ we need for analyzing subspace varieties.

Corollary 6.8. *For any $H \subseteq \mathbb{F}^k$ of dimension $k-s$ with $s \geq \ell$, we have that $V_H = \{U \in \mathrm{Gr}(\ell, \mathbb{F}^k) : V_H \cap U \neq 0\}$ is projective variety of dimension $\ell(k-\ell) - (s-\ell+1)$.*

Proof. Let $b_1, \ldots, b_k$ be a basis of $\mathbb{F}^k$ such that $b_1, \ldots, b_{k-s}$ is a basis of H. Let $\vec{a} = (k-s, k-\ell+2, \cdots, k)$. We claim that $\mathrm{Sch}_{\vec{a}}(\ell, b_1, \ldots, b_k) = V_H$. To see why, note that for $i \geq 2$, the condition that $\dim(U \cap \langle b_j : j \in [a_i] \rangle) \geq i$ in $\mathrm{Sch}_{\vec{a}}$ is immediate from (7). Furthermore, by the choice of basis, the condition $\dim(U \cap \langle b_j : j \in [k-s] \rangle) \geq 1$ is exactly $\dim(U \cap H) \geq 1$, i.e., $U \cap H \neq 0$. Thus, V_H is a projective subvariety of $\mathrm{Gr}(\ell, \mathbb{F}^k)$.

To finish, we apply Theorem 6.7 to get that

$$\dim(V_H) = a_1 - 1 + \sum_{i=2}^{\ell}(a_i - i) = (k - s - 1) + (\ell - 1)(k - \ell) = \ell(k - \ell) - (s - \ell + 1),$$

as desired. □

6.2.3 Proof of Theorem 6.2

To prove Theorem 6.2, we use a standard fact of algebraic geometry that dimensions of intersections of projective varieties behave analogously to that of vector spaces.

Proposition 6.9 (Lemma 43.13.14 [Aut] and Theorem I.7.2 [Har77], adapted)**.** *Let X, Y, Z be projective varieties over an algebraically closed field with $X, Y \subseteq Z$. If $\dim(X) + \dim(Y) \geq \dim(Z)$, then $X \cap Y$ is nonempty and has dimension*[13] *at least $\dim(X) + \dim(Y) - \dim(Z)$.*

Theorem 6.10 (Theorem 6.2 restated)**.** *Let $\mathbb{F}$ be an algebraically closed field (of any characteristic), then for any $H_1, \ldots, H_n \subseteq \mathbb{F}^k$ of codimension s (possibly with repetition), if $n \leq \frac{\ell(k-\ell)}{s-\ell+1}$, then there exists an ℓ-dimensional subspace $U \subseteq \mathbb{F}^k$ which has nontrivial intersection with each H_i. In other words, if $n \geq \lfloor \frac{\ell(k-\ell)}{s-\ell+1} \rfloor$ then a $(\ell, \lfloor \frac{\ell(k-\ell)}{s-\ell+1} \rfloor - 1)$ weak subspace design does not exist.*

Proof of Theorem 6.2. Let V_{H_i} be the subvariety of $\mathrm{Gr}(\ell, \mathbb{F}^k)$ corresponding to the U for which $H_i \cap U \neq 0$. It suffices to prove that if $n \leq \frac{\ell(k-\ell)}{s-\ell+1}$ then $\bigcap_{i=1}^n V_{H_i} \neq \varnothing$. By Corollary 6.8, we have that $\dim(V_{H_i}) = \ell(k-\ell) - (s-\ell+1)$ for all $i \in [n]$. We claim by induction for all $m \in [n]$ that $\bigcap_{i=1}^m V_{H_i}$ is nonempty with each irreducible component having dimension at least $\ell(k-\ell) - m(s-\ell+1)$. The base case of $m = 1$ is precisely Corollary 6.8. For $m \geq 2$, assume the inductive hypothesis for $m-1$ and apply Proposition 6.9 with $X = \bigcap_{i=1}^{m-1} V_{H_i}$, $Y = V_{H_m}$ and $Z = \mathrm{Gr}(\ell, \mathbb{F}^k)$. Then, observe that

$$\dim(X)+\dim(Y)-\dim(Z) \geq \ell(k-\ell)-(m-1)(s-\ell+1)+\ell(k-\ell)-(s-\ell+1)-\ell(k-\ell) = \ell(k-\ell)-m(s-\ell+1).$$

Therefore, since $m \leq n \leq \frac{\ell(k-\ell)}{s-\ell+1}$, we have that $\dim(X) + \dim(Y) - \dim(Z) \geq 0$, so $\bigcap_{i=1}^m V_{H_i}$ is nonempty with dimension at least $\ell(k-\ell) - m(s-\ell+1)$. In particular, when $m = n$, we have that $\bigcap_{i=1}^n V_{H_i}$ is nonempty, so $(H_1, \ldots, H_n)$ cannot be an $(\ell, n-1)$ weak subspace design. □

6.3 Theorem 6.2 does not apply to $\mathbb{F}_3$

We now show that Theorem 6.2 does not apply when $\mathbb{F}$ is not algebraically closed. Let $e_1, \ldots, e_4$ be a basis of $\mathbb{F}_3^4$ and let

$$\begin{aligned} H_1 &= \langle e_1, e_2 \rangle \\ H_2 &= \langle e_3, e_4 \rangle \\ H_3 &= \langle e_1 + e_3, e_2 + e_4 \rangle \\ H_4 &= \langle e_1 + e_4, e_2 - e_3 \rangle. \end{aligned}$$

Proposition 6.11. *$H_1, \ldots, H_4$ form a $(2, 3)$-weak subspace design.*

Thus, Theorem 6.2 cannot be extended to $\mathbb{F}_3$

[13] Technically, the result applies to the each irreducible component of the respective varieties, but here we define the dimension of a variety to be the maximum dimension of its irreducible components.

Proof. We seek to show that there is no 2-dimensional $U \subseteq \mathbb{F}_3^4$ which intersects every H_i. Assume for sake of contradiction that there exists a U for which $H_i \cap W \neq 0$. Since H_1 and H_2 are disjoint and U is 2-dimensional, there exist $\lambda_1, \ldots, \lambda_4 \in \mathbb{F}_3$ with $(\lambda_1, \lambda_2), (\lambda_3, \lambda_4) \neq (0,0)$ such that

$$U = \langle \lambda_1 e_1 + \lambda_2 e_2, \lambda_3 e_3 + \lambda_4 e_4 \rangle.$$

Now, in order for $U \cap H_3 \neq 0$, we must have that (λ_1, λ_2) is a scalar multiple of (λ_3, λ_4). Since U is invariant to the scaling of its basis, we may assume without loss of generality that $\lambda_3 = \lambda_1$ and $\lambda_4 = \lambda_2$. Now, since $U \cap H_4 \neq 0$, there exists $a, b, c, d \in \mathbb{F}_3$ with $(a, b) \neq (0,0)$ and $(c, d) \neq (0,0)$ such that

$$a(\lambda_1 e_1 + \lambda_2 e_2) + b(\lambda_1 e_3 + \lambda_2 e_4) = c(e_1 + e_4) + d(e_2 - e_3).$$

As such, we get the following system of equations

$$\begin{aligned} a\lambda_1 &= c \\ a\lambda_2 &= d \\ b\lambda_1 &= -d \\ b\lambda_2 &= c. \end{aligned}$$

Thus, $a\lambda_1 = b\lambda_2$ and $a\lambda_2 = -b\lambda_1$. Since $(\lambda_1, \lambda_2) \neq (0,0)$. We break into cases.

First, if $\lambda_1 \neq 0$, we have that $a = b\lambda_2/\lambda_1$, so we get that $b\lambda_2^2 = -b\lambda_1^2$. If $b = 0$, then $a = 0$ which contradicts that $(a, b) \neq (0,0)$. Thus, $b \neq 0$ so $\lambda_1^2 + \lambda_2^2 = 0$, but the only solution to this equation over $\mathbb{F}_3$ is $(\lambda_1, \lambda_2) = (0,0)$, a contradiction.

Likewise, if $\lambda_2 \neq 0$, we get $a = -b\lambda_1/\lambda_2$ so $-b\lambda_1^2 = b\lambda_2^2$. We then proceed by identical logic to the previous case. Thus, $(H_1, \ldots, H_4)$ is a $(2,3)$ weak subspace design. □

Remark 6.12. If we look at a quadratic extension of $\mathbb{F}_3$, then the equation $\lambda_1^2 + \lambda_2^2 = 0$ has nonzero solutions, from which we can then construct a subspace U intersecting all four spaces.

Acknowledgments

We thank Sivakanth Gopi for numerous discussions on the relationship between [LMS25] and MR tensor codes, which greatly inspired Section 5. We thank Matt Larson for helpful clarifications on the relationship between Theorem 5.2 and the matroid/rigidity literature. We thank Mahdi Cheraghchi, Venkatesan Guruswami and Madhur Tulsiani for many helpful discussions and much 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 the Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 512–519. IEEE, 1995. (cit. on p. 6)

[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. 4)

[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. 6)

[AHK18] Karim Adiprasito, June Huh, and Eric Katz. Hodge theory for combinatorial geometries. *Annals of Mathematics*, 188(2):381–452, 2018. (cit. on p. 8)

[ALOGV24] Nima Anari, Kuikui Liu, Shayan Oveis Gharan, and Cynthia Vinzant. Log-concave polynomials iii: Mason's ultra-log-concavity conjecture for independent sets of matroids. *Proceedings of the American Mathematical Society*, 152(05):1969–1981, 2024. (cit. on p. 8)

[AS16] Noga Alon and Joel H. Spencer. *The Probabilistic Method*. Wiley Publishing, 4th edition, 2016. (cit. on p. 2)

[Aut] The Stacks Project Authors. Stacks project. URL: https://stacks.math.columbia.edu/. (cit. on p. 33)

[BCDZ25] Joshua Brakensiek, Yeyuan Chen, Manik Dhar, and Zihan Zhang. Combinatorial bounds for list recovery via discrete brascamp–lieb inequalities. 2025. (cit. on p. 5, 6, 15)

[BDG+24a] Joshua Brakensiek, Manik Dhar, Jiyang Gao, Sivakanth Gopi, and Matt Larson. Rigidity matroids and linear algebraic matroids with applications to matrix completion and tensor codes. (arXiv:2405.00778), May 2024. arXiv:2405.00778, doi:10.48550/arXiv.2405.00778. (cit. on p. 4, 7, 18, 20, 21)

[BDG24b] Joshua Brakensiek, Manik Dhar, and Sivakanth Gopi. Improved field size bounds for higher order MDS codes. *IEEE Trans. Inf. Theory*, 70(10):6950–6960, 2024. doi:10.1109/TIT.2024.3449030. (cit. on p. 3, 4, 6)

[BDG25] Joshua Brakensiek, Manik Dhar, and Sivakanth Gopi. Improved constructions and lower bounds for maximally recoverable grid codes. *arXiv preprint arXiv:2509.15013*, 2025. (cit. on p. 4)

[BDGZ25] Joshua Brakensiek, Manik Dhar, Sivakanth Gopi, and Zihan Zhang. Ag codes achieve list-decoding capacity over constant-sized fields. *IEEE Transactions on Information Theory*, 2025. (cit. on p. 21)

[Ber17] Daniel Irving Bernstein. Completion of tree metrics and rank 2 matrices. *Linear Algebra Appl.*, 533:1–13, 2017. doi:10.1016/j.laa.2017.07.016. (cit. on p. 18)

[BGI+25] Kristóf Bérczi, Boglárka Gehér, András Imolay, László Lovász, Balázs Maga, and Tamás Schwarcz. Matroid products via submodular coupling. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, pages 2074–2085, 2025. (cit. on p. 7, 8)

[BGM22] Joshua Brakensiek, Sivakanth Gopi, and Visu Makam. Lower Bounds for Maximally Recoverable Tensor Codes and Higher Order MDS Codes. *IEEE Transactions on Information Theory*, 68(11):7125–7140, November 2022. doi:10.1109/TIT.2022.3187366. (cit. on p. 4, 7, 18, 21, 24)

[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. 4, 6, 7, 18, 20)

[BH20] Petter Brändén and June Huh. Lorentzian polynomials. *Annals of Mathematics*, 192(3):821–891, 2020. (cit. on p. 8)

[BPS13] Mario Blaum, James S. Plank, and Moshe Schwartz. Partial-MDS codes and their application to RAID-type of architectures. *IEEE Transactions on Information Theory*, 59(7):4510–4519, 2013. doi:10.1109/TIT.2013.2258343. (cit. on p. 4)

[CCS25] Yeyuan Chen, Mahdi Cheraghchi, and Nikhil Shagrithaya. Optimal erasure codes and codes on graphs. *arXiv preprint arXiv:2504.03090*, 2025. (cit. on p. 7, 21)

[CHL07] Minghua Chen, Cheng Huang, and Jin Li. On the Maximally Recoverable Property for Multi-Protection Group Codes. In *2007 IEEE International Symposium on Information Theory*, pages 486–490, June 2007. doi:10.1109/ISIT.2007.4557272. (cit. on p. 4)

[CJJT25] James Cruickshank, Bill Jackson, Tibor Jordán, and Shin-ichi Tanigawa. Rigidity of graphs and frameworks: A matroid theoretic approach. *arXiv preprint arXiv:2508.11636*, 2025. (cit. on p. 4, 8, 18, 19, 20, 21)

[CMST21] Han Cai, Ying Miao, Moshe Schwartz, and Xiaohu Tang. A construction of maximally recoverable codes with order-optimal field size. *IEEE Transactions on Information Theory*, 68(1):204–212, 2021. (cit. on p. 4)

[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. 3, 4, 5, 6, 28)

[DEL+22] Irit Dinur, Shai Evra, Ron Livne, Alexander Lubotzky, and Shahar Mozes. Locally testable codes with constant rate, distance, and locality. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 357–374, 2022. (cit. on p. 7)

[DG23] Manik Dhar and Sivakanth Gopi. A construction of maximally recoverable lrcs for small number of local groups. In *2023 IEEE International Symposium on Information Theory (ISIT)*, pages 1753–1757. IEEE, 2023. (cit. on p. 4)

[DGN+25] S Dzhenzher, T Garaev, O Nikitenko, A Petukhov, A Skopenkov, and A Voropaev. Low rank matrix completion and realization of graphs: results and problems. *arXiv preprint arXiv:2501.13935*, 2025. (cit. on p. 18)

[GG22] Sivakanth Gopi and Venkatesan Guruswami. Improved maximally recoverable LRCs using skew polynomials. *IEEE Transactions on Information Theory*, 68(11):7198–7214, 2022. (cit. on p. 4)

[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. 21)

[GGY20] Sivakanth Gopi, Venkatesan Guruswami, and Sergey Yekhanin. Maximally recoverable LRCs: A field size lower bound and constructions for few heavy parities. *IEEE Transactions on Information Theory*, 66(10):6066–6083, 2020. (cit. on p. 4)

[GHJY14] Parikshit Gopalan, Cheng Huang, Bob Jenkins, and Sergey Yekhanin. Explicit maximally recoverable codes with locality. *IEEE Transactions on Information Theory*, 60(9):5245–5256, 2014. (cit. on p. 4)

[GHK+17] Parikshit Gopalan, Guangda Hu, Swastik Kopparty, Shubhangi Saraf, Carol Wang, and Sergey Yekhanin. Maximally Recoverable Codes for Grid-like Topologies. In *Proceedings of the 2017 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, Proceedings, pages 2092–2108. Society for Industrial and Applied Mathematics, January 2017. doi:10.1137/1.9781611974782.136. (cit. on p. 4, 7, 17, 18, 20, 21)

[GK16] Venkatesan Guruswami and Swastik Kopparty. Explicit subspace designs. *Combinatorica*, 36(2):161–185, 2016. (cit. on p. 2, 4, 5, 8, 9, 10, 28, 29)

[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)

[GM22] Venkatesan Guruswami and Jonathan Mosheiff. Punctured low-bias codes behave like random linear codes. In *63rd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2022, Denver, CO, USA, October 31 - November 3, 2022*, pages 36–45. IEEE, 2022. doi:10.1109/FOCS54457.2022.00011. (cit. on p. 3, 6)

[GMR+22] Venkatesan Guruswami, Jonathan Moshieff, Nicolas Resch, Shashwat Silas, and Mary Wootters. Threshold rates for properties of random codes. *IEEE Trans. Inf. Theor.*, 68(2):905–922, February 2022. doi:10.1109/TIT.2021.3123497. (cit. on p. 3)

[GRX21] Venkatesan Guruswami, Nicolas Resch, and Chaoping Xing. Lossless dimension expanders via linearized polynomials and subspace designs. *Combinatorica*, 41(4):545–579, 2021. (cit. on p. 2)

[GSS93] Jack E Graver, Brigitte Servatius, and Herman Servatius. *Combinatorial rigidity*. Number 2. American Mathematical Soc., 1993. (cit. on p. 4, 10, 21)

[Gur11] Venkatesan Guruswami. Linear-Algebraic List Decoding of Folded Reed-Solomon Codes. In *2011 IEEE 26th Annual Conference on Computational Complexity*, pages 77–85, June 2011. doi:10.1109/CCC.2011.22. (cit. on p. 30)

[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. 6, 10)

[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. 2, 4)

[GX22] Venkatesan Guruswami and Chaoping Xing. Optimal rate list decoding over bounded alphabets using algebraic-geometric codes. *ACM Journal of the ACM (JACM)*, 69(2):1–48, 2022. (cit. on p. 2)

[GXY18] Venkatesan Guruswami, Chaoping Xing, and Chen Yuan. Subspace designs based on algebraic function fields. *Transactions of the American Mathematical Society*, 370(12):8757–8775, 2018. (cit. on p. 2, 28)

[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. 6)

[Har77] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer New York, New York, NY, 1977. doi:10.1007/978-1-4757-3849-0. (cit. on p. 9, 32, 33)

[Har92] Joe Harris. *Algebraic Geometry*, volume 133 of *Graduate Texts in Mathematics*. Springer New York, New York, NY, 1992. doi:10.1007/978-1-4757-2189-8. (cit. on p. 32)

[HCL13] Cheng Huang, Minghua Chen, and Jin Li. Pyramid codes: Flexible schemes to trade space for access efficiency in reliable data storage systems. *ACM Transactions on Storage (TOS)*, 9(1):1–28, 2013. (cit. on p. 4)

[HLM+25] Jun-Ting Hsieh, Alexander Lubotzky, Sidhanth Mohanty, Assaf Reiner, and Rachel Yun Zhang. Explicit lossless vertex expanders. *arXiv preprint arXiv:2504.15087*, 2025. (cit. on p. 2)

[HPYWZ21] Lukas Holzbaur, Sven Puchinger, Eitan Yaakobi, and Antonia Wachter-Zeh. Correctable erasure patterns in product topologies. In *2021 IEEE Int. Symp. Inform. Theory (ISIT)*, pages 2054–2059. IEEE, 2021. (cit. on p. 4, 7, 18)

[HSW21] June Huh, Benjamin Schröter, and Botong Wang. Correlation bounds for fields and matroids. *Journal of the European Mathematical Society*, 24(4):1335–1351, 2021. (cit. on p. 8)

[Huh22] June Huh. Combinatorics and hodge theory. In *Proceedings of the international congress of mathematicians*, volume 1, pages 212–239, 2022. (cit. on p. 8)

[HY16] Guangda Hu and Sergey Yekhanin. New constructions of sd and mr codes over small finite fields. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 1591–1595. IEEE, 2016. (cit. on p. 4)

[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, *Proceedings of the 57th Annual ACM Symposium on Theory of Computing, STOC 2025, Prague, Czechia, June 23-27, 2025*, pages 843–854. ACM, 2025. doi:10.1145/3717823.3718302. (cit. on p. 3, 6)

[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. 6, 7)

[JT24] Bill Jackson and Shin-ichi Tanigawa. Maximal matroids in weak order posets. *Journal of Combinatorial Theory, Series B*, 165:20–46, 2024. (cit. on p. 8, 18, 19, 20)

[KLR19] Daniel Kane, Shachar Lovett, and Sankeerth Rao. The independence number of the birkhoff polytope graph, and applications to maximally recoverable codes. *SIAM Journal on Computing*, 48(4):1425–1435, 2019. (cit. on p. 4)

[KMG21] Xiangliang Kong, Jingxue Ma, and Gennian Ge. New bounds on the field size for maximally recoverable codes instantiating grid-like topologies. *Journal of Algebraic Combinatorics*, pages 1–29, 2021. (cit. on p. 4)

[KNN15] Gil Kalai, Eran Nevo, and Isabella Novik. Bipartite rigidity. *Transactions of the American Mathematical Society*, 368(8):5515–5545, November 2015. doi:10.1090/tran/6512. (cit. on p. 4, 8, 18, 20)

[KP25] Gleb Kalachev and Pavel Panteleev. Maximally Extendable Product Codes are Good Coboundary Expanders. (arXiv:2501.01411), January 2025. arXiv:2501.01411, doi:10.48550/arXiv.2501.01411. (cit. on p. 7)

[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. 6)

[Lam70] G. Laman. On graphs and rigidity of plane skeletal structures. *J. Engrg. Math.*, 4:331–340, 1970. doi:10.1007/BF01534980. (cit. on p. 4)

[Lar25] Matt Larson. personal communication, 2025. (cit. on p. 20)

[LB15] V. Lakshmibai and Justin Brown. *The Grassmannian Variety: Geometric and Representation-Theoretic Aspects*, volume 42 of *Developments in Mathematics*. Springer New York, New York, NY, 2015. doi:10.1007/978-1-4939-3082-1. (cit. on p. 9, 32)

[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. 3, 6, 8, 10, 11, 12, 15, 17, 19, 21, 34)

[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. 6)

[Mas81] John H Mason. Glueing matroids together: a study of dilworth truncations and matroid analogues of exterior and symmetric powers. *Algebraic methods in graph theory*, 1:519–561, 1981. (cit. on p. 8, 19, 20, 21)

[Max64] James Clerk Maxwell. On the calculation of the equilibrium and stiffness of frames. *Philos. Mag.*, 27:294—299, 1864. (cit. on p. 4, 10, 18)

[MPK19] Umberto Martínez-Peñas and Frank R Kschischang. Universal and dynamic locally repairable codes with maximal recoverability via sum-rank codes. *IEEE Transactions on Information Theory*, 65(12):7790–7805, 2019. (cit. on p. 4)

[MRR+20] Jonathan Mosheiff, Nicolas Resch, Noga Ron-Zewi, Shashwat Silas, and Mary Wootters. LDPC codes achieve list decoding capacity. In Sandy Irani, editor, *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020*, pages 458–469. IEEE, 2020. doi:10.1109/FOCS46700.2020.00050. (cit. on p. 3, 6)

[NKS19] Luong Trung Nguyen, Junhan Kim, and Byonghyo Shim. Low-rank matrix completion: A contemporary survey. *IEEE Access*, 7:94215–94237, 2019. (cit. on p. 18)

[Oxl06] James G Oxley. *Matroid theory*, volume 3. Oxford University Press, USA, 2006. (cit. on p. 17, 19, 22)

[PD14] Dimitris S Papailiopoulos and Alexandros G Dimakis. Locally repairable codes. *IEEE Transactions on Information Theory*, 60(10):5843–5855, 2014. (cit. on p. 4)

[PG27] Hilda Pollaczek-Geiringer. Über die gliederung ebener fachwerke. *Z.Angew. Math. Mech.*, 7:58–72, 1927. (cit. on p. 4)

[PK22] Pavel Panteleev and Gleb Kalachev. Asymptotically good quantum and locally testable classical ldpc codes. In *Proceedings of the 54th annual ACM SIGACT symposium on theory of computing*, pages 375–388, 2022. (cit. on p. 7)

[Ram20] Chandrasekaran Ramya. Recent progress on matrix rigidity–a survey. *arXiv preprint arXiv:2009.09460*, 2020. (cit. on p. 4)

[RVW00] Omer Reingold, Salil P. Vadhan, and Avi Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors. In *41st Annual Symposium on Foundations of Computer Science, FOCS 2000, Redondo Beach, California, USA, November 12-14, 2000*, pages 3–13. IEEE Computer Society, 2000. doi:10.1109/SFCS.2000.892006. (cit. on p. 2)

[SAP+13] Maheswaran Sathiamoorthy, Megasthenis Asteris, Dimitris Papailiopoulos, Alexandros G Dimakis, Ramkumar Vadali, Scott Chen, and Dhruba Borthakur. Xoring elephants: Novel erasure codes for big data. *arXiv preprint arXiv:1301.3791*, 2013. (cit. on p. 4)

[SC10] Amit Singer and Mihai Cucuringu. Uniqueness of low-rank matrix completion by rigidity theory. *SIAM Journal on Matrix Analysis and Applications*, 31(4):1621–1641, 2010. (cit. on p. 8, 18)

[Sch80] Jacob T Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM (JACM)*, 27(4):701–717, 1980. (cit. on p. 7)

[Sch86] Alexander Schrijver. *Theory of linear and integer programming*. Wiley-Interscience Series in Discrete Mathematics. John Wiley & Sons, Ltd., Chichester, 1986. A Wiley-Interscience Publication. (cit. on p. 27)

[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. 3, 4, 6)

[SZ23] Paolo Santonastaso and Ferdinando Zullo. On subspace designs. *EMS Surveys in Mathematical Sciences*, 11(1):1–62, 2023. (cit. on p. 2, 9)

[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. 6, 28)

[Whi89] Walter Whiteley. A matroid on hypergraphs, with applications in scene analysis and geometry. *Discrete Comput. Geom.*, 4(1):75–95, 1989. doi:10.1007/BF02187716. (cit. on p. 18, 20)

[Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *International symposium on symbolic and algebraic manipulation*, pages 216–226. Springer, 1979. (cit. on p. 7)

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il