

Generic Reed-Solomon codes achieve list-decoding capacity

Joshua Brakensiek*

Sivakanth Gopi†

Visu Makam‡

Abstract

In a recent paper, Brakensiek, Gopi and Makam [BGM21] introduced *higher order MDS codes* as a generalization of MDS codes. An order- ℓ MDS code, denoted by $\text{MDS}(\ell)$, has the property that any ℓ subspaces formed from columns of its generator matrix intersect as minimally as possible. An independent work by Roth [Rot21] defined a different notion of higher order MDS codes as those achieving a generalized singleton bound for list-decoding. In this work, we show that these two notions of higher order MDS codes are (nearly) equivalent.

We also show that generic Reed-Solomon codes are $\text{MDS}(\ell)$ for all ℓ , relying crucially on the GM-MDS theorem which shows that generator matrices of generic Reed-Solomon codes achieve any possible zero pattern. As a corollary, this implies that generic Reed-Solomon codes achieve list decoding capacity. More concretely, we show that, with high probability, a random Reed-Solomon code of rate R over an exponentially large field is list decodable from radius $1 - R - \varepsilon$ with list size at most $\frac{1-R-\varepsilon}{\varepsilon}$, resolving a conjecture of Shanguan and Tamo [ST20].

*Department of Computer Science, Stanford University, Stanford, CA. Email: jbrakens@cs.stanford.edu. Portions of this work were completed at Microsoft Research, Redmond. Research supported in part by an NSF Graduate Research Fellowship and a Microsoft Research PhD Fellowship.

†Microsoft Research, Redmond, WA. Email: sigopi@microsoft.com.

‡Radix Trading Europe B. V. Email: visu@umich.edu. Research supported by NSF Grant No. DMS-1638352, CCF-1412958, and CCF-1900460.

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 3 |
| 1.1 | List-decoding Reed-Solomon codes | 3 |
| 1.1.1 | Previous Work | 5 |
| 1.2 | Higher order MDS codes | 5 |
| 1.3 | Proof overview | 8 |
| 1.4 | Further applications and connections | 10 |
| 1.4.1 | Generic Gabidulin codes achieve list-decoding capacity | 10 |
| 1.4.2 | Field size lower bounds for LD-MDS(L) codes | 11 |
| 1.4.3 | Maximally recoverable tensor codes | 11 |
| 1.4.4 | Connections to invariant theory | 12 |
| 1.5 | Open Questions | 12 |
| 2 | Generic Zero Patterns (GZPs) | 14 |
| 2.1 | Generalized Hall's theorem and maximal GZPs | 15 |
| 2.2 | A characterization of sets in order- ℓ generic zero patterns | 17 |
| 3 | Equivalence of GZP(ℓ) and MDS(ℓ) | 20 |
| 3.1 | GZP(ℓ) implies MDS(ℓ) | 20 |
| 3.2 | MDS(ℓ) implies GZP(ℓ) | 21 |
| 3.3 | Characterizing the null intersection property | 22 |
| 4 | Applications to List Decoding: Proof of Theorem 1.4 | 22 |
| 4.1 | Equivalence of MDS and LD-MDS (up to duality) | 22 |
| 4.2 | Reed-Solomon codes | 24 |
| 4.2.1 | Generic Reed-Solomon codes | 24 |
| 4.2.2 | Random Reed-Solomon codes | 24 |
| 5 | Connections to Invariant Theory | 25 |
| 5.1 | Linear matrices, non-commutative rank and the blow-up regularity lemma | 26 |
| 5.2 | Polynomial time computability of generic intersection ranks | 27 |
| 5.2.1 | A doubling operation | 28 |
| 5.2.2 | Scalability of generic intersection dimension | 29 |
| A | Resolution of Conjecture 5.7 of [ST20] | 33 |
| B | An alternative algorithm for computing generic intersection dimension in polynomial time | 35 |
| B.1 | Proof of Lemma B.1 | 36 |
| B.2 | Proof of Lemma B.2 | 37 |

1 Introduction

The singleton bound states that a (n, k) -code can have distance at most $n - k + 1$. Codes achieving this bound are called *MDS codes*. Reed-Solomon codes [RS60] are an explicit construction of such codes over fields of size $O(n)$. In particular, they allow us to decode uniquely from up to half the minimum distance. List decoding was introduced independently by [Woz58, Eli57] to decode from beyond half the minimum distance. Naturally, we are not guaranteed to decode uniquely. But we can hopefully return a small list of codewords which are close to a corrupted codeword. We now define this formally.

Definition 1.1. *We say that a (n, k) -code C is (ρ, L) -list decodable if there are at most L codewords in any Hamming ball of radius ρn .*

We call ρ the list-decoding radius and L the list size. A code with rate R cannot be list decoded beyond radius $1 - R$ with polynomial list size (see [GRS12]). Therefore we must have $\rho \leq 1 - R$, this is called *list-decoding capacity*. A code with rate R which is $(1 - R - \varepsilon, L)$ -list decodable for $L = L(\varepsilon)$ is said to achieve list-decoding capacity. Here ε is called the *gap to capacity*. It is known that random non-linear codes can achieve list decoding capacity with list size $O(1/\varepsilon)$ and alphabet size $\exp(1/\varepsilon)$ (see [GRS12]). It is also known that random *linear* codes over large enough alphabet achieve list-decoding capacity [ZP81]. There is also a stronger form of list decoding called *average-radius list-decoding*.

Definition 1.2. *We say that a (n, k) -code C is (ρ, L) -average-radius list-decodable¹ if there doesn't exist $L + 1$ distinct codewords $c_0, c_1, \dots, c_L \in C$ and $y \in \mathbb{F}^n$, such that²*

$$\frac{1}{L+1} \sum_{i=0}^L \text{wt}(c_i - y) \leq \rho n.$$

Note that if a code is (ρ, L) -average-radius list-decodable then it is also (ρ, L) -list decodable. The capacity for average case list-decoding is also $1 - R$ and random linear codes achieve it [ZP81].

A long line of work exists on constructing explicit codes which achieve list-decoding capacity. Following an initial breakthrough by [PV05], Folded Reed-Solomon codes of [GR08] were the first explicit codes to achieve list-decoding capacity, but with list size and alphabet size polynomial in code length. Further works have reduced the list size to $\exp(\tilde{O}(1/\varepsilon))$ where ε is the gap to capacity [DL12, GX12, GX13, KRZSW18]. Some classes of structured random codes can also be shown to achieve list decoding capacity. [MRRZ⁺20] show that LDPC codes achieve list decoding capacity. [GM21] show that puncturings of low-bias codes have good list-decodability.

1.1 List-decoding Reed-Solomon codes

Reed-Solomon codes are one of the most popular codes with several applications both in theory and practice [WB99]. We say that C is a Reed-Solomon code if it has a generator matrix which is

¹In some previous works, such as [Rot21] this is referred to as *strongly list-decodable*.

²Here $\text{wt}(x)$ is the Hamming weight of x , i.e., the number of non-zero coordinates of x .

a *Vandermonde* matrix. That is, there exists distinct $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ such that

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix} \quad (1)$$

is a generator matrix of C . Reed-Solomon codes are MDS (maximum distance separable) codes, i.e., they achieve the maximum distance possible for a code with given rate. So naturally, there is a lot of interest in understanding the list-decodability of Reed-Solomon codes.

Question 1.3. *Can Reed-Solomon codes achieve list-decoding capacity?*

Guruswami and Sudan [Sud97, GS98] showed that rate R Reed-Solomon codes can be list-decoded from radius $1 - \sqrt{R}$, which is also coincidentally the Johnson bound for list-decoding [Joh62]. Whether Reed-Solomon codes can be list-decoded beyond the Johnson bound has been a topic of intense research. [RW14] are the first to show that random Reed-Solomon codes (i.e., when α_i are chosen randomly from a large enough field in (1)) can be list-decoded beyond the Johnson bound in some parameter ranges. On the other hand, full length Reed-Solomon codes where $\alpha_1, \alpha_2, \dots, \alpha_n$ are all the field elements (with $n = |\mathbb{F}|$) are not list-decodable with constant list size with list-decoding radius $1 - \alpha\sqrt{R}$ for sufficiently small constant $\alpha, R < 1$, in fact the list size has to be at least $n^{2 \log(1/\alpha)}$ [BSKR09]. Therefore it is clear that the evaluation points α_i have to be chosen carefully from a large enough finite field to even beat the Johnson bound. In this paper, we are interested in understanding the list-decoding behavior of *generic*³ Reed-Solomon codes. That is, the limiting behavior of a random choice of $\alpha_1, \dots, \alpha_n$ as \mathbb{F} tends to infinity. In [ST20], Shangguan and Tamo made a startling conjecture that generic Reed-Solomon codes don't just beat the Johnson bound, but in fact achieve list-decoding capacity! They also conjectured a precise bound on the list size. In Section 4, we fully resolve their conjecture.

Theorem 1.4. *Generic Reed-Solomon codes achieve list decoding capacity. If C is a generic (n, k) -Reed-Solomon code with rate $R = k/n$, then C is (ρ, L) -list decodable for*

$$\rho = 1 - R - \frac{1 - R}{L + 1}. \quad (2)$$

Moreover, C is also (ρ, L) -average-radius list-decodable for the same ρ .

Equivalently, Theorem 1.4 shows that a generic Reed-Solomon code of rate R is $(1 - R - \varepsilon, L)$ -list decodable with $L = \frac{1 - R - \varepsilon}{\varepsilon}$. The bound (2) is the best possible even for non-linear codes [GST21a, Rot21].

In Section 4, we also show how to turn Theorem 1.4 into a quantitative bound on the field size required for random Reed-Solomon codes to achieve list-decoding capacity.

Theorem 1.5. *Let n, k, L be positive integers and let $c(n, k, L) = 2Ln^2 \binom{n}{\leq n-k}^{L+1}$. A random (n, k) -Reed-Solomon code of rate $R = k/n$ over \mathbb{F} is $(1 - R - \frac{1-R}{L+1}, L)$ -average-radius list decodable with probability at least $1 - c/|\mathbb{F}|$.*

Remark 1.6. *Combining the construction from this paper with a different one in [BGM21], one can get $c(n, k, L) = n^{O(\min(k, n-k)L)}$ in Theorem 1.5 (see Remark 4.6).*

³**Genericity** (from [BGM21]): “A generic point X can be thought of either as a symbolic vector, or one can think of it as a point with entries in an infinite field \mathbb{F} which avoids any fixed low-dimensional algebraic variety. If $\mathbb{F} = \mathbb{R}$ or \mathbb{C} , then one can think of a generic point as something which escapes any measure zero set. In particular, low-dimensional varieties are measure zero sets.”

1.1.1 Previous Work

[ST20] conjectured Theorem 1.4 and Theorem 1.5 and proved them in the case of $L = 2, 3$.⁴ Note that it is also true for $L = 1$ trivially, since Reed-Solomon codes are MDS. They also made an algebraic conjecture in their paper (see Conjecture 5.7 from [ST20]) about the non-singularity of certain symbolic matrices, which would imply Theorem 1.4. We prove this conjecture in Appendix A, the proof follows from some of the results in our paper which we use to prove Theorem 1.4. Table 1.1.1 shows prior results on list-decoding of random Reed-Solomon codes over fields of size q .

| | ρ | L | Rate R | Field size q |
|-----------------------|---------------------------|---------------------------------------|--|----------------------------------|
| Johnson bound | $1 - \varepsilon$ | qn^2 | ε^2 | n |
| [RW14] | $1 - \varepsilon$ | $O(1/\varepsilon)$ | $\Omega\left(\frac{\varepsilon}{\log(q) \log^5(1/\varepsilon)}\right)$ | $\tilde{\Omega}(n/\varepsilon)$ |
| [ST20] | $1 - R - \frac{1-R}{L+1}$ | $L = 2, 3$ | R | $\exp(n)$ |
| [GLS ⁺ 22] | $1 - \varepsilon$ | $O(1/\varepsilon)$ | $\Omega\left(\frac{\varepsilon}{\log(1/\varepsilon)}\right)$ | $(1/\varepsilon)^n$ |
| [FKS22] | $1 - \varepsilon$ | $\lceil 3/\varepsilon \rceil$ | $\frac{\varepsilon}{3(1+\zeta)}$ | $n^{1+1/\zeta}$ |
| [GST21a] | $1 - \varepsilon$ | $O(1/\zeta)$ | $\frac{\varepsilon-\zeta}{2-\varepsilon+\zeta}$ | $\text{poly}(n)$ |
| Our work | $1 - R - \varepsilon$ | $\frac{1-R-\varepsilon}{\varepsilon}$ | R | $\exp(\tilde{O}(n/\varepsilon))$ |

Table 1: Adapted from [GST21a]. Prior works on list-decoding of random Reed-Solomon codes over fields of size q .

1.2 Higher order MDS codes

Our results on list-decodability of generic Reed-Solomon codes follow from studying generalizations of MDS codes called *higher order MDS codes*. We will show that generic Reed-Solomon codes are not just MDS, they are in fact higher order MDS codes. As we will see shortly, this implies that generic Reed-Solomon codes have optimal list-decodability. We will now dive into the rich theory of higher order MDS codes.

A (n, k) -code C is MDS if it has the property that every non-zero codeword has hamming weight at least $n - k + 1$. MDS codes have a number of equivalent characterizations. As has recently been explored in the literature [BGM21, Rot21], for many of the characterizations one can define a suitable generalization of MDS codes, deriving various notions of *higher-order MDS codes*. Each of these has an order parameter $\ell \geq 1$, indicating the degree of generality over MDS codes.

► **MDS(ℓ).** Suppose $G_{k \times n}$ is the generator matrix of an (n, k) -code C over \mathbb{F} . For $A \subset [n]$, let G_A denote the linear subspace of \mathbb{F}^k spanned by the columns of G indexed by A . C is MDS iff every k columns of G are linearly independent, equivalently $\dim(G_A) = \min\{|A|, k\}$ for all $A \subset [n]$. Equivalently, we can write this as $\dim(G_A) = \dim(W_A)$ where $W_{k \times n}$ is a generic matrix.

⁴They did not conjecture average-radius list-decodability and also didn't conjecture an explicit bound on $c(n, k, L)$.

If $A, B \subset [n]$ are any two subsets, then

$$\begin{aligned}\dim(G_A \cap G_B) &= \dim(G_A) + \dim(G_B) - \dim(G_A + G_B) \\ &= \dim(G_A) + \dim(G_B) - \dim(G_{A \cup B}) \\ &= \dim(W_A) + \dim(W_B) - \dim(W_{A \cup B}) \\ &= \dim(W_A \cap W_B).\end{aligned}$$

Unfortunately, it may not be true that $\dim(G_{A_1} \cap G_{A_2} \cap G_{A_3}) = \dim(W_{A_1} \cap W_{A_2} \cap W_{A_3})$ for all subsets $A_1, A_2, A_3 \subset [n]$ if C is MDS. This is because, the usual inclusion-exclusion principle fails for 3 or more subspaces. [BGM21] considered the following generalization of MDS codes which they called *higher order MDS codes*.

Definition 1.7 (MDS(ℓ) [BGM21]). *Let C be an (n, k) -code with generator matrix G . Let ℓ be a positive integer. We say that C is MDS(ℓ) if for any ℓ subsets $A_1, \dots, A_\ell \subseteq [n]$ of size of at most k , we have that*

$$\dim(G_{A_1} \cap \dots \cap G_{A_\ell}) = \dim(W_{A_1} \cap \dots \cap W_{A_\ell}), \quad (3)$$

where $W_{k \times n}$ is a generic matrix over the same field characteristic.⁵

Since $\dim(W_{A_1} \cap \dots \cap W_{A_\ell})$ is minimized when W is a generic matrix, another intuitive way to think of an MDS(ℓ) code is that $G_{A_1}, G_{A_2}, \dots, G_{A_\ell}$ intersect as minimally as possible for any ℓ subsets A_1, A_2, \dots, A_ℓ . The usual MDS codes are MDS(ℓ) for $\ell = 1, 2$ by the above discussion. This definition arose out of attempting to understand the properties of *maximally recoverable tensor codes*, which are explained in more detail in Section 1.4.3. Briefly, the tensor product of C and a parity check code is a maximally recoverable tensor code iff C is a higher order MDS code of appropriate order (Proposition 1.19). Unlike MDS property, MDS(ℓ) is not preserved under duality. The dual of an MDS(ℓ) code is MDS(ℓ) for $\ell \leq 3$, but this fails for $\ell \geq 4$ [BGM21].

To get some intuition for MDS(ℓ), let's understand a $(n, 3)$ -code C which is MDS(3). Let $v_1, v_2, \dots, v_n \in \mathbb{F}^3$ be the columns of a generator matrix of C . Since scaling the columns doesn't affect MDS(3), we can think of them as points in the projective plane $\mathbb{P}\mathbb{F}^2$. It is easy to see that C is MDS iff the points $v_1, v_2, \dots, v_n \in \mathbb{P}\mathbb{F}^2$ are in general position, that is no three points are collinear. C is MDS(3) iff in addition, any 3 lines formed by joining disjoint pairs of points in v_1, v_2, \dots, v_n are not concurrent.

► **LD-MDS(ℓ).** A generalization of the singleton bound was recently proved for list-decoding in [ST20, Rot21, GST21b]. Roth [Rot21] defined a higher order generalization of MDS codes as codes achieving this generalized singleton bound for list-decoding.⁶

Definition 1.8 (LD-MDS(L) [Rot21]). *Let C be a (n, k) -code. We say that C is list decodable-MDS(L), denoted by LD-MDS(L), if C is (ρ, L) -average-radius list-decodable for $\rho = \frac{L}{L+1} \left(1 - \frac{k}{n}\right)$. In other words, for any $y \in \mathbb{F}^n$, there doesn't exist $L+1$ distinct codewords $c_0, c_1, \dots, c_L \in C$ such that*

$$\sum_{i=0}^L \text{wt}(c_i - y) \leq L(n - k). \quad (4)$$

We say⁷ that C is LD-MDS($\leq L$) if it is LD-MDS(ℓ) for all $1 \leq \ell \leq L$.

⁵Note that MDS(ℓ) is a property of the code C and not a particular generator matrix G used to generate C . This is because if G satisfies (3) then MG also satisfies (3) for any $k \times k$ invertible matrix M .

⁶[Rot21] also called these *higher order MDS codes* independently of the prior work [BGM21], leading to some confusion. Fortunately, as we will see shortly, these two notions are nearly equivalent.

⁷In general, the notion of LD-MDS(ℓ) is not monotone in ℓ .

The list-decoding guarantees of LD-MDS(L) are very strong. In particular, LD-MDS(L) codes of rate R get ε -close to list-decoding capacity when $L \geq \frac{1-R-\varepsilon}{\varepsilon}$. Note that the usual MDS codes are LD-MDS(1). [Rot21] showed that LD-MDS(L) property is preserved under duality only for $L = 1, 2$, and also gave some explicit constructions of LD-MDS(2) codes.

► **GZP(ℓ).** In many coding theory applications, it is useful to have MDS codes with generator matrices having constrained supports, see [DSY14, HHYD14, YS13, DSDY13] for some such applications to multiple access networks and secure data exchange. Dau et al. [DSY14] have made a remarkable conjecture that Reed-Solomon codes over fields of size $q \geq n + k - 1$ can have generator matrices with arbitrary patterns of zeros, as long as the pattern of zeros do not obviously preclude MDS property by having a large block of zeros. This came to be called the *GM-MDS conjecture*. It was eventually proved independently by Lovett [Lov18] and Yildiz and Hassibi [YH19b]. Before we state the GM-MDS theorem, we will make some crucial definitions.

Let $\mathcal{S} = (S_1, S_2, \dots, S_k)$ where $S_1, \dots, S_k \subset [n]$, we call such an \mathcal{S} a *zero pattern* for $k \times n$ matrices. We say that \mathcal{S} has *order* ℓ if there are ℓ distinct non-empty sets among S_1, S_2, \dots, S_k . We say that a matrix $G_{k \times n}$ *attains* the zero pattern \mathcal{S} if there exists an invertible matrix $M_{k \times k}$ such that $\tilde{G} := MG$ has zeros in $\bigcup_{i=1}^k \{i\} \times S_i$. Note that \tilde{G} and G generate the same code. We now define the crucial notion of a *generic zero pattern*.

Definition 1.9 (Generic zero pattern). *Suppose $\mathcal{S} = (S_1, S_2, \dots, S_k)$ is a zero pattern for $k \times n$ matrices. We say \mathcal{S} is a generic zero pattern if for all $I \subset [k]$,*

$$\left| \bigcap_{i \in I} S_i \right| \leq k - |I|. \quad (5)$$

It is not hard to see that, by Hall's matching theorem, (5) is equivalent to the condition that a generic $k \times n$ matrix W which has zeros in $\bigcup_{i=1}^k \{i\} \times S_i$ (and the rest of the entries of W are generic), has all $k \times k$ minors non-zero. This is because the condition (5) ensures that any $k \times k$ submatrix of W has a matching of non-zero entries, and thus ensures non-zero determinant for this $k \times k$ submatrix. (5) appeared in [DSY14], where it is called the MDS condition because it is a necessary condition for a $k \times n$ matrix with zeros in \mathcal{S} to be MDS. We will now define a new generalization of MDS codes, which we call GZP(ℓ).

Definition 1.10 (GZP(ℓ)). *We say that a (n, k) -code C is GZP(ℓ) if C is MDS⁸ and its generator matrix $G_{k \times n}$ attains all $k \times n$ generic zero patterns of order at most ℓ .⁹*

Thus, a code C is GZP(ℓ) if we can choose a generator matrix of C to have any order ℓ generic zero pattern. One can prove that GZP(1) and GZP(2) are equivalent to MDS property, therefore this is indeed a generalization of the MDS property. Given how we defined GZP(ℓ), it is not obvious to see why generic matrices should be GZP(ℓ). In Proposition 2.1, we give an elementary proof of the fact that generic matrices are indeed GZP(ℓ), i.e., a fixed generic matrix can attain any generic zero pattern.

We will now state the GM-MDS theorem in terms of GZP(ℓ) property.

Theorem 1.11 (GM-MDS [DSY14, Lov18, YH19b]). *A generic Reed-Solomon code is GZP(ℓ) for all ℓ , i.e., a generic Reed-Solomon code can attain any generic zero pattern.*

⁸We explicitly add the MDS condition to avoid degenerate cases like zero matrix being GZP(ℓ).

⁹Note that GZP(ℓ) is a property of the code C , and not a particular generator matrix G used to generate C . This is because if G attains a generic zero pattern, then MG also attains it for any invertible $k \times k$ matrix M .

The actual GM-MDS theorem says that for any particular generic zero pattern \mathcal{S} , there exists a Reed-Solomon code over any field of size $q \geq n + k - 1$ which can attain \mathcal{S} . This is a simple consequence of Theorem 1.11, but we are more interested in GZP(ℓ) codes which simultaneously attain *all* order ℓ generic zero patterns.

Equivalence of higher-order MDS codes. We are now ready to present the most important theorem of our paper. We show that, surprisingly, all these notions of higher-order MDS codes are equivalent (up to duality).

Theorem 1.12. *The following are equivalent for a linear code C for all $\ell \geq 1$.*

- (a) C is MDS($\ell + 1$).
- (b) C^\perp is LD-MDS($\leq \ell$).
- (c) C is GZP($\ell + 1$).

Proof. (a) iff (b) is proved in Section 4 and (a) iff (c) is proved in Section 3. \square

Remark 1.13. *One can show that MDS(1), MDS(2), LD-MDS(1), GZP(1), GZP(2) are all equivalent to MDS (see [BGM21, Rot21]).*

As we will see, the core of the proof of Theorem 1.12 is combinatorial, with some simple linear algebra on top. Since by GM-MDS theorem, generic Reed-Solomon codes are GZP(ℓ) for all ℓ , we have the following corollary.

Corollary 1.14. *Generic Reed-Solomon codes are GZP(ℓ), MDS(ℓ) and LD-MDS(ℓ) for all ℓ .*

Proof. The dual of a generic Reed-Solomon code is also a generic Reed-Solomon code (Proposition 4.4). Therefore, Theorem 1.12 together with the GM-MDS theorem (Theorem 1.11), immediately implies that generic Reed-Solomon codes are MDS(ℓ) and LD-MDS(ℓ) for all ℓ . \square

This immediately implies our main result that generic Reed-Solomon codes achieve list-decoding capacity (Theorem 1.4).

1.3 Proof overview

The proof of Theorem 1.12 has a few key steps, including proving some novel properties of generic zero patterns as well as solving a *generic intersection problem*.

Dimension of generic intersections The core of the proof of Theorem 1.12 is a combinatorial characterization of the RHS of (3).

Theorem 1.15 (Dimension of Generic Intersection). *Given $A_1, \dots, A_\ell \subseteq [n]$ of size at most k , for a generic matrix $W_{k \times n}$, we have that*

$$\dim(W_{A_1} \cap \dots \cap W_{A_\ell}) = \max_{P_1 \sqcup P_2 \sqcup \dots \sqcup P_s = [\ell]} \left(\sum_{i \in [s]} \left| \bigcap_{j \in P_i} A_j \right| - (s-1)k \right) \quad (6)$$

where the maximum is over all partitions of $[\ell]$. Note that the result is independent of the characteristic of the underlying field.

The proof of Theorem 1.15 appears in Section 3.1. Since the RHS of (6) has a maximum over exponentially many terms in ℓ , it gives an $(\exp(\tilde{O}(\ell))k)$ -time algorithm for computing the generic intersection dimension. In Section 5, we give a $\text{poly}(k, \ell)$ -time algorithm to compute the RHS of (6) by reducing it non-commutative rank computation (see Theorem 1.21). We give an alternative algorithm in Appendix B.

In literature, one can find many problems that are similar or related to Theorem 1.15 in a range of subjects like Schubert calculus, intersection theory, matroid theory, representation stability and homological algebra to name a few. For example, it seems conceivable that there is a matroid-theoretic description or that there is a formula for the intersection dimension coming from Schubert calculus and intersection theory. Despite that, it seems very difficult to adapt the techniques from any of those subjects to say anything meaningful about the problem above, but a more in-depth analysis from the view-point of any of those subjects could lead to new insights in broader contexts (see Section 1.5).

A novel characterization of sets in order- ℓ generic zero patterns We also show a novel structural result on order ℓ generic zero patterns. In particular, if \mathcal{S} is an order ℓ generic zero pattern containing sets A_1, A_2, \dots, A_ℓ and say d copies of the empty set. Then by applying (5), one can easily show that for all partitions $\mathcal{P} = P_1 \sqcup P_2 \sqcup \dots \sqcup P_s = [\ell]$ we have that

$$\sum_{i=1}^s \left| \bigcap_{j \in P_i} A_j \right| \leq (s-1)k + d. \quad (7)$$

Surprisingly the converse is also true (see Lemma 2.8). A_1, A_2, \dots, A_ℓ can be used to form an order ℓ generic zero pattern with d copies of the empty set iff (7) holds. The proof involves an intricate induction, which on a high level is comparable to the induction used to prove Hall's matching theorem. In the proof, one identifies the partition \mathcal{P} for which the above inequality is tight (if no such partition exists, then one pads with elements). One can then recursively apply the induction hypothesis to each portion of the partition, which can then be combined together to show the result. This result is crucially used to prove that $\text{GZP}(\ell)$ codes are also $\text{MDS}(\ell)$ and to prove Theorem 1.15.

The proof of Theorem 1.15 proceeds as follows. Let d be the RHS of (6). By Lemma 2.8, there exists a order ℓ zero pattern \mathcal{S} with copies of $A_1, \dots, A_\ell \subseteq [n]$ and d copies of the empty set. Then, since a generic matrix W is $\text{GZP}(\ell)$ (Proposition 2.1), there is an invertible $M_{k \times k}$ such that $\widetilde{W} = MW$ has the zero pattern \mathcal{S} . From this, it is straightforward to upper bound the dimension of the intersection $\dim(W_{A_1} \cap \dots \cap W_{A_\ell}) = \dim(\widetilde{W}_{A_1} \cap \dots \cap \widetilde{W}_{A_\ell}) \leq d$. A matching lower bound follows from the pigeonhole principle and dimension counting. Note that this proof also immediately implies that $\text{GZP}(\ell)$ codes are $\text{MDS}(\ell)$ because in the proof of Theorem 1.15, we only used the $\text{GZP}(\ell)$ property of generic matrices to get the correct dimension.

A generalized Hall's theorem. One of the key results in [DSY14] is a *generalized Hall's theorem*. For any generic zero pattern $\mathcal{S} = (S_1, \dots, S_k)$ there exists a generic zero pattern $\mathcal{S}' = (S'_1, \dots, S'_k)$ which contains \mathcal{S} (i.e., for all i , $S'_i \supseteq S_i$) such that $|S'_i| = k-1$ for all i . However, this theorem does not preserve order, if \mathcal{S} is order ℓ , the order of \mathcal{S}' can be as large as k (and in fact must equal k).

In Section 2.1, we further generalize the generalized Hall's theorem from [DSY14]. In particular, we show that if \mathcal{S} is an order ℓ generic zero pattern, then there is an order ℓ generic zero pattern \mathcal{S}'

which contains \mathcal{S} such that for the non-empty A_1, \dots, A_ℓ which define \mathcal{S}' , each A_i appears exactly $k - |A_i|$ times. Such an \mathcal{S}' is called *maximal*.

This new generalized Hall's theorem is used to prove that $\text{MDS}(\ell)$ codes are also $\text{GZP}(\ell)$. Suppose C is an $\text{MDS}(\ell)$ code with generator matrix G . Given an order ℓ generic zero pattern \mathcal{S} , one uses our generalized Hall theorem (Theorem 2.5), to find a maximal order ℓ generic zero pattern \mathcal{S}' containing \mathcal{S} . Let A_1, \dots, A_ℓ be the ℓ non-empty sets in \mathcal{S}' and say \mathcal{S}' has d copies of the empty set. Using the $\text{MDS}(\ell)$ property of G and the fact that \mathcal{S}' satisfies (5), we can prove that $\dim(G_{A_1} \cap \dots \cap G_{A_\ell}) = d$ via Theorem 1.15. By taking the dual of this intersection and performing a dimension-counting argument, one can show that¹⁰ $(G_{A_1})^\perp, \dots, (G_{A_\ell})^\perp$ are linearly independent. One can then show that bases for these spaces can be put together to build a matrix M such that MG has the desired zero pattern. For the proof to work, we absolutely need the fact that each A_i appears exactly $k - |A_i|$ times in the pattern \mathcal{S}' , which is guaranteed by the generalized Hall's theorem.

Equivalence of $\text{MDS}(\ell + 1)$ and $\text{LD-MDS}(\leq \ell)^\perp$. The proof of equivalence mostly follows from Theorem 1.15. We prove the contrapositive: that C is *not* $\text{MDS}(\ell + 1)$ iff C^\perp is *not* $\text{LD-MDS}(\leq \ell)$.

Let G be a generator matrix of C , note that G is a parity check matrix for C^\perp . If C is *not* $\text{MDS}(\ell + 1)$, there exists some choice of $A_1, \dots, A_{\ell+1}$ for which (6) is not satisfied. In fact, using a result of [BGM21], one can assume that the RHS of (6) is 0. This implies there is a nontrivial $z \in G_{A_1} \cap \dots \cap G_{A_{\ell+1}}$ which is not captured by a generic intersection. In particular, for all $i \in [\ell]$, there is u_i with $\text{supp}(u_i) \subseteq A_i$ with $z = Gu_i$. This is almost enough to prove that C^\perp is not $\text{LD-MDS}(\ell)$, but some of the u_i 's may be equal. To get around this, we consider a partition of $[\ell]$ with two A_i 's in the same part if their u_i 's are equal. The resulting inequality arising from using this partition with (6) is enough to prove that C^\perp is not $\text{LD-MDS}(\ell')$ for some $\ell' \leq \ell$.

Now assume that C^\perp is not $\text{LD-MDS}(\leq \ell)$, WLOG say C^\perp is not $\text{LD-MDS}(\ell)$. In particular, this implies that there are *distinct* $u_1, \dots, u_{\ell+1}$ for which $Gu_1 = \dots = Gu_{\ell+1}$ and $\sum_{i=1}^{\ell+1} \text{wt}(u_i) \leq \ell k$. One can then let $A_i = \text{supp}(u_i)$, and consider the intersection $G_{A_1} \cap \dots \cap G_{A_{\ell+1}}$. Using the distinctness of $u_1, \dots, u_{\ell+1}$, one can prove that the dimension of this intersection is strictly greater than the corresponding generic intersection. This is enough to show that C^\perp is not $\text{MDS}(\ell)$.

1.4 Further applications and connections

In this section, we mention some further applications and connections of our work to different areas of coding theory and mathematics.

1.4.1 Generic Gabidulin codes achieve list-decoding capacity

Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be linearly independent over some base field \mathbb{F}_q . A Gabidulin code has the following generator matrix:

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^q & \alpha_2^q & \cdots & \alpha_n^q \\ \alpha_1^{q^2} & \alpha_2^{q^2} & \cdots & \alpha_n^{q^2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{q^{k-1}} & \alpha_2^{q^{k-1}} & \cdots & \alpha_n^{q^{k-1}} \end{pmatrix}. \quad (8)$$

¹⁰The dual is of the linear space $G_{A_1} \subseteq \mathbb{F}^k$. We are *not* taking the dual of the original matrix G .

A generic Gabidulin code is defined by choosing $\alpha_1, \alpha_2, \dots, \alpha_n$ generically over a large enough extension field of \mathbb{F}_q . Gabidulin codes are rank metric codes which achieve the rank metric singleton bound with applications in network coding, space-time coding and cryptography [Gab, Gab21]. GM-MDS theorem was extended to Gabidulin codes over both finite and zero characteristic in [YH19a, YRH20]. Thus generator of matrices of generic Gabidulin codes over both finite and zero characteristic also satisfy $\text{GZP}(\ell)$ for all ℓ . Since dual of a generic Gabidulin code is also a generic Gabidulin code [Gab21], Theorem 1.12 shows that Gabidulin codes are $\text{MDS}(\ell)$ and $\text{LD-MDS}(\ell)$ for all ℓ . This implies that generic Gabidulin codes have optimal list-decoding guarantees with respect to the Hamming metric.

Theorem 1.16. *Generic Gabidulin codes achieve list-decoding capacity (in the Hamming metric). In particular, they are (ρ, L) -average-radius list-decodable for*

$$\rho = 1 - R - \frac{1 - R}{L + 1}.$$

1.4.2 Field size lower bounds for LD-MDS(L) codes

The field size lower bound on $\text{MDS}(\ell)$ of [BGM21] is as follows.

Proposition 1.17 (Corollary 4.2 [BGM21]). *If C is an (n, k) -code over \mathbb{F} which is $\text{MDS}(\ell)$, then*

$$|\mathbb{F}| \gtrsim_{\ell} n^{\min\{k, n-k, \ell\}-1}.$$

As an immediate corollary of Theorem 1.12, we have the following:

Corollary 1.18. *If C is an (n, k) -code over \mathbb{F} which is $\text{LD-MDS}(\leq L)$, then*

$$|\mathbb{F}| \gtrsim_L n^{\min\{k-1, n-k-1, L\}}.$$

In particular, if C is a code of constant rate (thus both k and $n - k$ tend to infinity), we have that $|\mathbb{F}| \gtrsim_L n^L$. In this constant-rate regime, our lower bound significantly improves upon the lower bound from [Rot21] which says that $|\mathbb{F}| \gtrsim_L \left(\frac{n}{n-k}\right)^{\min\{k-1, L\}}$.

1.4.3 Maximally recoverable tensor codes

Gopalan et al. [GHK⁺17] introduced the notion of maximally recoverable (MR) codes with grid-like topologies. These codes have applications in distributed storage in datacenters, where they offer a good trade-off between low latency, durability and storage efficiency [HSX⁺12]. An important special case of such codes are MR tensor codes. A code C is a (m, n, a, b) -tensor code if it can be expressed as $C_{\text{col}} \otimes C_{\text{row}}$, where C_{col} is a $(m, m - a)$ code and C_{row} is a $(n, n - b)$ code. In other words, the codewords of C are $m \times n$ matrices where each row belongs to C_{row} and each column belongs to C_{col} . There are a parity checks per column and b parity checks per row. For example, the f4 storage architecture of Facebook (now Meta) uses an $(m = 3, n = 14, a = 1, b = 4)$ -tensor code [MLR⁺14]. Such a code C is *maximally recoverable* if it can recover from every erasure pattern $E \subseteq [m] \times [n]$ which can be recovered from by choosing a generic C_{col} and C_{row} . Thus MR tensor codes are optimal codes since they can recover from any erasure pattern that is information theoretically possible to recover from. MR tensor codes are poorly understood with no known explicit constructions. Even a characterization of which erasure patterns are correctable by an (m, n, a, b) -MR tensor code is not known except in the case of $a = 1$ [GHK⁺17]. [BGM21] defined $\text{MDS}(\ell)$ codes motivated by the following proposition.

Proposition 1.19 ([BGM21]). *Let $C = C_{\text{col}} \otimes C_{\text{row}}$ be an $(m, n, a = 1, b)$ -tensor code. Here $a = 1$ and thus C_{col} is a parity check code. Then C is maximally recoverable if and only if C_{row} is MDS(m).*

Thus, better understanding higher order MDS codes is essential to understanding maximally recoverable tensor codes. We hope that Theorem 1.12 which shows the importance of higher order MDS codes to various areas of coding theory, will help in designing explicit MDS(ℓ) codes and thus explicit maximally recoverable tensor codes. The following is a direct corollary of Proposition 1.19 and Corollary 1.14.

Corollary 1.20. *The tensor product of a parity check code and a generic Reed-Solomon code is maximally recoverable.*

1.4.4 Connections to invariant theory

Theorem 1.15 has connections to *invariant theory*. Although Theorem 1.15 produces a closed formula for generic intersection dimension, there are exponentially many (in ℓ, k) partitions to consider. This can make computing the dimension cumbersome. We give a deterministic¹¹ polynomial-time algorithm by reducing the intersection dimension to a computation of *non-commutative rank* of a suitable linear matrix. The computation of non-commutative rank in polynomial-time is a recent breakthrough, an analytic algorithm appears in [GGOW16] based on Gurvits operator scaling and an algebraic algorithm in [IQS18] based on their previous work [IQS17] and the degree bounds in [DM17]. These results are part of a larger ambitious program of Mulmuley [Mul17] that attempts to approach central problems in complexity via orbit problems in invariant theory that has seen much progress over the last decade, see [BFG⁺19] and references there-in. In Section 5, we use these methods to prove the following result.

Theorem 1.21. *Given k, n and $A_1 \dots A_\ell \subseteq [n]$, we can compute the intersection dimension $\dim(W_{A_1} \cap \dots \cap W_{A_\ell})$ for generic W in $\text{poly}(k, \ell)$ -time.*

Remark 1.22. *Explicitly computing the formula found by Theorem 1.15 takes $\exp(\tilde{O}(\ell))k$ time, as there are $\exp(\tilde{O}(\ell))$ partitions of $[\ell]$ (e.g., [DB81]). Thus, Theorem 1.21 is superior when $\ell \geq \text{polylog}(k)$.*

1.5 Open Questions

There are a number of exciting directions that warrant further exploration. We list a few of these directions.

Constructions of higher-order MDS codes. Despite knowing that generic Reed-Solomon codes are higher-order MDS, we do not know of any good explicit constructions of such higher-order MDS codes in general.¹²

As previously mentioned, Theorem 1.5 and the results of [BGM21] imply that MDS(ℓ) codes exist over fields of size $n^{O(\min\{k, n-k\}\ell)}$.

¹¹We remark that a simple randomized polynomial-time algorithm to compute generic intersection dimension is to randomly sample W over a large enough field and compute the intersection dimension directly by a rank computation [BGM21].

¹²Note that one can always get an “explicit” construction over doubly exponential size fields by choosing α_i to be in a degree k field extension over $\mathbb{F}_2(\alpha_1, \dots, \alpha_{i-1})$ in (1) [ST20].

Conversely, $\text{MDS}(\ell)$ codes require a field of size $\Omega_\ell(n^{\min\{\ell, k, n-k\}-1})$ [BGM21] (see Proposition 1.17). The simplest non-trivial case is when $k = 3, \ell = 3$. The lower bound implies that, we need field size at least $q = \Omega(n^2)$ in this case.

Question 1.23. *Do there exist (explicit) $\text{MDS}(\ell)$ codes of length n over fields of size $O(n^{\ell-1})$? More concretely, can we construct an explicit $\text{MDS}(3)$ $(n, 3)$ -code over a field of size $O(n^2)$?*

Constructing such $\text{MDS}(\ell)$ codes immediately implies codes which get ε -close to list decoding capacity over fields of size $O(n^{1/\varepsilon})$ and list size $1/\varepsilon$. [BGM21] gives $O(n^2)$ field size constructions for notions slightly weaker than $\text{MDS}(3)$. [Rot21] gives an explicit construction of size $O(n^{32})$ and a non-explicit construction over fields of size $O(n^5)$. More generally [Rot21] gives an explicit construction of (n, k) - $\text{MDS}(3)$ code over fields of size $O(n^{k^{2k}})$.

Maximally recoverable tensor codes when $a, b \geq 2$. We saw that $\text{MDS}(\ell)$ codes arise naturally from studying (m, n, a, b) -MR tensor codes when $a = 1$. It would be interesting to study, what properties of the row and column codes would be needed to construct MR tensor codes for $a, b \geq 2$.

As previously mentioned, the work of [GHK⁺17] fully characterized the correctable erasure patterns for a (m, n, a, b) tensor code when $a = 1$. Theorem 1.15, when combined with the results of [BGM21], fully characterizes the linearly independent patterns when $a = 1$. We hope that these results lead to insights which resolve question of characterizing correctable erasure patterns in the general case. More precisely,

Question 1.24. *Given generic vectors $u_1, \dots, u_m \in \mathbb{F}^{m-a}$ and $v_1, \dots, v_n \in \mathbb{F}^{n-b}$, for which $E \subseteq [m] \times [n]$ is $\{u_i \otimes v_j : (i, j) \in E\}$ of full rank? For which E are they linearly independent?*

Efficient list-decoding of LD-MDS($\leq L$) codes. As previously mentioned, the result of Guruswami-Sudan [GS98] shows that any (n, k) -Reed-Solomon code of rate R can be efficiently list-decoded up to radius $\rho = 1 - \sqrt{R}$. A hardness result by Cheng and Wan [CW07] states that it is discrete-logarithm-hard to decode up to radius $\hat{\rho} := 1 - \hat{g}/n$, where

$$\hat{g} = \min \left\{ g : \binom{n}{g} |\mathbb{F}|^{k-g} \leq 1 \right\}$$

However, this result only applies for small field sizes. In particular, if $|\mathbb{F}| > 2^n$, then $\hat{g} = k + 1$, which is precisely list-decoding capacity. Further, for sufficiently large n , and $R = k/n \in (0, 1)$ a constant and $|\mathbb{F}| \gtrsim_L n^L$, one can estimate that

$$\hat{\rho} = 1 - R - O_R \left(\frac{1}{L \log n} \right),$$

On the other hand, LD-MDS($\leq L$) are list decodable only upto list-decoding radius $\rho = 1 - R - \frac{1-R}{L+1}$ with list size L . Thus, given the established field size lower bound for LD-MDS($\leq L$) codes (Corollary 1.18), we believe the following is open in general.

Question 1.25. *Assume C is a (n, k) -Reed-Solomon which is LD-MDS($\leq L$). Given $y \in \mathbb{F}^n$, can one efficiently list all $c \in C$ with distance from y at most $\frac{L}{L+1}(n - k)$?*

Notation

A linear (n, k) -code C is a k -dimensional subspace of \mathbb{F}^n .¹³ A matrix $G_{k \times n}$ is a generator matrix of C , if the rows of G are a basis of C . A matrix $H_{(n-k) \times n}$ is called a parity check matrix for C if $C = \{x : Hx = 0\}$. The dual code C^\perp is defined as $C^\perp = \{y : \langle x, y \rangle = 0 \ \forall x \in C\}$. C^\perp is a $(n, n - k)$ -code and its generator matrix is the parity check matrix of C .

We let $[n]$ denote the set $\{1, 2, \dots, n\}$. Given a collection of sets $A_1, \dots, A_k \subseteq [n]$, and a nonempty set $I \subseteq [k]$, we let $A_I = \bigcap_{i \in I} A_i$.

Let V be a $k \times n$ matrix. For all $i \in [n]$, let v_i denote the i th column of V . Given $A \subseteq [n]$, we let $V_A = \text{span}\{v_j : j \in A\}$. This notation should not be confused with the A_I notation.

Organization

The remainder of the paper is organized as follows. In Section 2, we discuss generic zero patterns in more detail, particularly how they relate to the GM-MDS conjecture. In Section 3, we prove that $\text{GZP}(\ell)$ and $\text{MDS}(\ell)$ are equivalent. In the process, we prove Theorem 1.15. In Section 4, we prove that $\text{MDS}(\ell)$ and $\text{LD-MDS}(\leq \ell - 1)$ are equivalent, up to duality. This completes the proofs of Theorem 1.4 and Theorem 1.12. In Section 5, we show that Theorem 1.15 also holds in the non-commutative setting, yielding a deterministic polynomial-time algorithm for generic intersection dimension. In Appendix A, we prove Conjecture 5.7 from [ST20]. In Appendix B, we give an alternative polynomial-time algorithm for computing the generic intersection dimension.

Acknowledgments

We thank Venkatesan Guruswami, Sergey Yekhanin, and June Huh for valuable discussions and encouragement. We thank anonymous reviewers for numerous helpful comments.

2 Generic Zero Patterns (GZPs)

Recall that a zero pattern $\mathcal{S} = (S_1, S_2, \dots, S_k)$ is called a generic zero pattern if

$$\left| \bigcap_{i \in I} S_i \right| \leq k - |I| \quad \forall I \subset [k]. \quad (9)$$

Also recall that (9) is equivalent to the fact that a generic matrix with zero pattern \mathcal{S} has all of its $k \times k$ minors non-zero. We will now prove a generic matrix can attain any generic zero pattern.

Proposition 2.1. *A generic $k \times n$ matrix can attain any $k \times n$ generic zero pattern. In other words, generic codes are $\text{GZP}(\ell)$ for all ℓ .*

Proof. Let $V_{k \times n}$ be a generic matrix, which is the generator matrix of a generic (n, k) -code. Let $\mathcal{S} = (S_1, \dots, S_k)$ be a generic zero pattern for $k \times n$ matrices, i.e. \mathcal{S} satisfies (9). We want to show that there exists some invertible matrix $M_{k \times k}$ such that MV has zeros in $\bigcup_{i \in [k]} \{i\} \times S_i$. By the generalized Hall's theorem (Theorem 2.2), there exists $S'_i \subset [n]$ such that $S'_i \supset S_i$, $|S'_i| = k - 1$ and $(S'_1, S'_2, \dots, S'_k)$ satisfy (9). Therefore, WLOG we can assume that $|S_i| = k - 1$ for all i . Let

¹³In this paper, we will only work with linear codes. So unless specified otherwise, a (n, k) -code is always a linear code.

v_1, v_2, \dots, v_n be the columns of V . Let m_1, m_2, \dots, m_k be the rows of M . For MV to have zeros in $i \times S_i$, it must be that $\langle m_i, v_j \rangle = 0$ for all $j \in S_i$. Therefore $m_i = V_{S_i}^\perp$ (up to scaling), note that $V_{S_i}^\perp$ is a one-dimensional space since $|S_i| = k - 1$. Moreover the entries of $m_i = V_{S_i}^\perp$ can be expressed as $(k - 1) \times (k - 1)$ minors of V_{S_i} (with some \pm signs) which are some polynomials in the entries of V . Therefore M is completely determined (up to scaling of rows) by V , and the entries of M are some polynomials in the entries of V . Now we just need to prove that $\det(M)$ which is a polynomial in the entries of V is not identically zero. To prove this, we give a particular setting of $V = V^* \in \mathbb{F}^{k \times n}$ for which $\det(M) \neq 0$, for any large enough field \mathbb{F} (of any characteristic). Set all the entries $V_{ij}^* = 0$ whenever $j \in S_i$ and set the remaining entries randomly from \mathbb{F} . Since \mathcal{S} is a generic zero pattern, V^* is an MDS matrix with high probability by Hall's matching theorem. Therefore $m_i = (V_{S_i}^*)^\perp = e_i$ (up to scaling), where e_i is the i th standard basis vector. Therefore $M = I_{k \times k}$ is the $k \times k$ identity matrix (upto scaling of rows), which has non-zero determinant. \square

2.1 Generalized Hall's theorem and maximal GZPs

While formulating the GM-MDS conjecture, [DSY14] proved a variant of a Generalized Hall's Theorem and used it to show that any generic zero pattern can be extended to a maximal generic zero pattern.

Theorem 2.2 (Generalized Hall's Theorem—modern statement [DSY14]). *Let $\mathcal{S} = (S_1, \dots, S_k)$ be a generic zero pattern for (n, k) -codes. Then, there exists a generic zero pattern $\mathcal{S}' = (S'_1, \dots, S'_k)$ such that for all $i \in [k]$, $|S'_i| = k - 1$ and $S_i \subseteq S'_i$.*

Remark 2.3. *Note that Theorem 2.2 is a generalization of the classic Hall's theorem about existence of a bipartite matching when $k = n$. In this case, if we form a bipartite graph between $[k]$ and $[n]$ where $i \in [k]$ has neighborhood \bar{S}_i , (9) becomes the Hall's matching condition that the neighborhood $N(I)$ of any set I satisfies $|N(I)| \geq |I|$.*

If we apply Theorem 2.2 to an order ℓ pattern, the resulting pattern \mathcal{S}' will not be order ℓ in general (in fact, it will be order k). To extend an order ℓ generic zero pattern to a maximal order ℓ generic zero pattern, we need a further generalization of the generalized Hall's theorem (Theorem 2.5). First, we state an equivalence.

Proposition 2.4. *Assume $n \geq k$. Let $A_1, \dots, A_\ell \subseteq [n]$ of size at most k . The following are equivalent.*

(a) *There exist $\delta_1, \dots, \delta_\ell \geq 0$. such that for all nonempty $I \subseteq [\ell]$*

$$|A_I| \leq k - \sum_{i \in I} \delta_i. \quad (10)$$

(b) *The pattern (S_1, \dots, S_k) , with δ_i copies of A_i for $i \in [\ell]$ and additional $k - \sum_{i=1}^\ell \delta_i$ copies of the empty set, is a generic zero pattern order ℓ .*

Proof. First we prove that (a) implies (b). Let $d = k - \sum_{i \in [\ell]} \delta_i$. By (10), we know that d is nonnegative. We need to show that (9) holds for (S_1, \dots, S_k) . Let $I \subseteq [k]$ be any non-empty subset, we want to show that (9) holds for I . If I includes at least one i for which $S_i = \emptyset$, then (9) trivially holds. Further, if $I \subseteq [k]$ includes a nonzero number of copies of A_i , we might as

well include all the δ_i copies, as the LHS of (9) is unchanged and the RHS can only decrease. If I includes 0 or δ_i copies of each A_i , then (9) is exactly (10) for the relevant set of A_i 's.

To prove that (b) implies (a), for every $I \subseteq [\ell]$ for (10), look at the subset $I' \subseteq [k]$ which includes δ_i copies of A_i for each $i \in I$. The truth of (10) is then implied by applying (9) to I' . \square

We now state our generalized Hall's theorem which is a further generalization of Theorem 2.2.

Theorem 2.5 (Generalized Hall's Theorem (new)). *Assume $n \geq k$. Let A_1, \dots, A_ℓ be subsets of $[n]$ of size at most k . Assume there exist $\delta_1, \dots, \delta_\ell \geq 0$ such that for all nonempty $I \subseteq [\ell]$, (10) holds. Then, there exists $A'_i \supseteq A_i$ such that (10) holds for A'_1, \dots, A'_ℓ and for all $i \in [\ell]$, $|A'_i| = k - \delta_i$.*

Proof. It suffices to show that if for some $i \in [\ell]$, we have that $|A_i| < k - \delta_i$, then we can find $A'_i \supset A_i$ for which $|A'_i| = k - \delta_i$ and replacing A'_i with A_i still satisfies (10). WLOG, by permutation of the A_i 's, we may assume that $|A_1| < k - \delta_1$. Note that if $\delta_1 = 0$, we may extend A_1 to an arbitrary superset of size k . Since (10) holds for all I with $1 \notin I$, adding 1 to I can only decrease the LHS but not change the RHS. Thus, this is a valid extension.

We now assume $\delta_1 \geq 1$. By Proposition 2.4, we have that S_1, \dots, S_k , with δ_i copies of A_i for each $i \in [\ell]$ and the rest the empty set is a generic zero pattern. For all $i \in [\ell]$, let $J_i \subseteq [k]$ (possibly empty) be the indices for j for which $S_j = A_i$. Let T be an arbitrary subset of $[n]$ of size k for which $A_1 \subseteq T$. Define $T_i := S_i \cap T$ for all $i \in [k]$. Note that (T_1, \dots, T_k) is a generic zero pattern, as for each (9) the LHS could only decrease going from S_i to T_i .

Note that the " T -complements" $\bar{T}_i := T \setminus T_i$ satisfy the matching conditions of classical Hall's theorem (e.g., [VW01]). That is, for any nonempty $I \subseteq [k]$,

$$\left| \bigcup_{i \in I} \bar{T}_i \right| = |T| - \left| \bigcap_{i \in I} T_i \right| \geq k - (k - |I|) = |I|.$$

Thus, by Hall's theorem, the elements of T can be listed as (t_1, \dots, t_k) such that $t_i \in \bar{T}_i$ for all i . Define $T'_i = T \setminus \{t_i\}$. Note that $T_i \subseteq T'_i \subset T$ for all $i \in [k]$. Since each T'_i excludes a distinct element, the family (T'_1, \dots, T'_k) satisfies (9). For all $i \in [\ell]$, let

$$U_i := \begin{cases} \bigcap_{j \in J_i} T'_j & J_i \text{ nonempty} \\ T & \text{otherwise.} \end{cases}$$

Note that $A_i \cap T \subseteq U_i$ for all i . For $i = 1$, since $A_1 \subseteq T$, so $A_1 \subseteq U_1$. By (9), we have that $|U_1| \leq k - \delta_1$. Further, since $|T \setminus T'_i| = 1$ for all $i \in J_1$, we can deduce by the pigeonhole principle that $|U_1| = k - \delta_1$.

We claim that upon replacing A_1 with U_1 , (10) is still satisfied for all nonempty I . Since we keep the other sets unchanged, (10) holds for all I with $1 \notin I$. Now, assume that $1 \in I$. By applying (9) with $\bigcup_{i \in I} J_i$, we have that

$$\begin{aligned} k - \sum_{i \in I} \delta_i &= k - \sum_{i \in I} |J_i| \\ &\geq \left| \bigcap_{i \in I} \bigcap_{j \in J_i} T'_j \right| \\ &= \left| U_1 \cap \bigcap_{i \in I \setminus \{1\}} U_i \right| \end{aligned}$$

$$\begin{aligned}
&\geq \left| U_1 \cap \bigcap_{i \in I \setminus \{1\}} (A_i \cap T) \right| \\
&= \left| (U_1 \cap T) \cap \bigcap_{i \in I \setminus \{1\}} A_i \right| \\
&= \left| U_1 \cap \bigcap_{i \in I \setminus \{1\}} A_i \right|,
\end{aligned}$$

as desired. Thus, extending A_1 to U_1 was valid.

By recursively applying the argument, we may deduce that each A_i can be extended to a set of size $k - \delta_i$. \square

If a generic pattern (S_1, \dots, S_k) contains δ_i copies of a set A_i , then (9) implies that $|A_i| \leq k - \delta_i$. As an immediate corollary of Theorem 2.5 and Proposition 2.4, we can now show that any generic zero pattern of order ℓ can be extended to a “maximal” generic zero pattern of order ℓ .

Corollary 2.6. *Assume $n \geq k$. Let (S_1, \dots, S_k) be a generic zero pattern order ℓ containing δ_i copies of nonempty A_i for all $i \in [\ell]$. Then, there exists $A'_i \supseteq A_i$ with $|A'_i| = k - \delta_i$ for all i , such that the zero pattern (S'_1, \dots, S'_k) with δ_i copies of A'_i for all i (and the same number of copies of the empty set) is a generic zero pattern of order ℓ .*

Remark 2.7. *Following the methods of [DSY14], Corollary 2.6, as well as the other results in this subsection can be made into efficient algorithms.*

2.2 A characterization of sets in order- ℓ generic zero patterns

Given subsets $A_1, A_2, \dots, A_\ell \subset [n]$, we are interested in knowing if there exists an order- ℓ generic zero pattern $\mathcal{S} = (S_1, S_2, \dots, S_k)$ for $k \times n$ matrices which is formed by copies of A_1, A_2, \dots, A_ℓ and d copies of the empty set. We now give a combinatorial characterization of sets A_1, A_2, \dots, A_ℓ for which this can be done, based on partitions of the ℓ sets. This characterization is essential for relating generic zero patterns with the generic intersection problem (see Section 3 for its application).

Lemma 2.8. *Assume $n \geq k$ and $d \geq 0$. Let $A_1, A_2, \dots, A_\ell \subseteq [n]$ of size at most k . The following are equivalent.*

- (a) *There exists an order at most ℓ generic zero pattern for $k \times n$ matrices which contains only copies of A_1, A_2, \dots, A_ℓ and an additional d copies of the empty set.*
- (b) *There exist $\delta_1, \dots, \delta_\ell \geq 0$ such that $\sum_{i=1}^{\ell} \delta_i = k - d$ and for all nonempty $I \subseteq [\ell]$,*

$$|A_I| \leq k - \sum_{i \in I} \delta_i. \quad (11)$$

- (c) *For all partitions $P_1 \sqcup P_2 \sqcup \dots \sqcup P_s = [\ell]$, we have that*

$$\sum_{i=1}^s |A_{P_i}| \leq (s-1)k + d. \quad (12)$$

Proof. We first prove that (a) iff (b). If (a) is true, let δ_i be the number of times that A_i appears in the generic zero pattern. Note that the empty set must then appear $d = k - \sum_{i=1}^{\ell} \delta_i$ times. Thus, by Proposition 2.4, we have that (b) holds.

If (b) is true, then by Proposition 2.4, there is a generic zero pattern which uses A_1, \dots, A_{ℓ} as its nonempty sets with precisely additional $k - \sum_{i=1}^{\ell} \delta_i = d$ empty sets.

Now we prove that (b) iff (c). The proof that (b) implies (c) is near-immediate, for any partition $P_1 \sqcup P_2 \sqcup \dots \sqcup P_s = [\ell]$, we have that by (11),

$$\begin{aligned} \sum_{i=1}^s |A_{P_i}| &\leq \sum_{i=1}^s \left(k - \sum_{j \in P_i} \delta_j \right) \\ &= sk - \sum_{j=1}^{\ell} \delta_j \\ &= (s-1)k + d. \end{aligned}$$

The proof that (c) implies (b) is rather nontrivial and requires a careful induction on ℓ .¹⁴ The base case $\ell = 1$ follows by taking $\delta_1 = k - d$ and the fact that $|A_1| \leq d$.

Now assume that $\ell \geq 2$. First, by applying the discrete partition $\{1\} \sqcup \{2\} \sqcup \dots \sqcup \{\ell\}$ to (12), we know that

$$\sum_{i=1}^{\ell} |A_i| \leq (\ell-1)k + d, \quad (13)$$

which is at most than nk . Thus, we can pad the A_i 's with additional elements until (12) is an equality for some partition $P_1 \sqcup P_2 \sqcup \dots \sqcup P_s = [\ell]$. We call such a partition *tight*. Note that padding the A_i 's with additional elements can only make (11) more difficult to satisfy, and thus we only need to prove (b) implies (a) for the padded family of sets.

If the tight partition satisfies $s = 1$, that is, $|A_{[\ell]}| = d$, claim that we can continue to pad¹⁵ the A_i 's until a partition with $s \geq 2$ is tight. If (13) is tight, this is already true. Otherwise, we have that

$$\sum_{i=1}^{\ell} |A_i \setminus A_{[\ell]}| < (\ell-1)(k-d),$$

Thus, by the pigeonhole principle, there is $i \in [n] \setminus A_{[\ell]}$ which appears in at most $\lfloor ((\ell-1)(k-d) - 1)/(n-d) \rfloor \leq \ell-2$ of the A_i 's. Thus, we can continue padding the A_i 's, while keeping $|A_{[\ell]}| = d$, until a partition $P_1 \sqcup P_2 \sqcup \dots \sqcup P_s = [\ell]$ with $s \geq 2$ is tight.

Fix $i \in [s]$. For all $j \in P_i$, define $B_j = A_j \setminus A_{P_i}$. Let $k_i = k - |A_{P_i}|$. Since each A_j has size at most k , each B_j has size at most $k_i \leq k$. We claim that for all partitions $Q_1 \sqcup Q_2 \sqcup \dots \sqcup Q_t = P_i$, we have that

$$\sum_{j=1}^t |B_{Q_j}| \leq (t-1)k_i \quad (14)$$

To see why, note that $P_1 \sqcup \dots \sqcup P_{i-1} \sqcup Q_1 \sqcup \dots \sqcup Q_t \sqcup P_{i+1} \sqcup \dots \sqcup P_s = [\ell]$ is a partition. Thus we may apply (14) on this partition and the fact that $P_1 \sqcup P_2 \sqcup \dots \sqcup P_s$ is a tight partition to obtain

¹⁴Although our induction is purely combinatorial, it has some similarities to [YH19b]'s proof of the GM-MDS theorem.

¹⁵A similar padding argument appears in Appendix B of [BGM21].

that.

$$\begin{aligned}
\sum_{j=1}^t |B_{Q_j}| &= \sum_{j=1}^t |A_{Q_j}| - t|A_{P_i}| \\
&= \left(\sum_{j=1}^t |A_{Q_j}| + \sum_{j \in [s] \setminus i} |A_{P_j}| \right) - \sum_{j=1}^s |A_{P_j}| - (t-1)|A_{P_i}| \\
&\leq (s+t-2)k + d - ((s-1)k + d) - (t-1)(k - k_i) \\
&= (t-1)k_i.
\end{aligned}$$

Since $s \geq 2$, we have that $|P_i| < \ell$. Thus, we may apply the induction hypothesis¹⁶ to $(B_j : j \in P_i)$ to get that there exist $\delta_j \geq 0$ for all $j \in P_i$ such that $\sum_{j \in P_i} \delta_j = k_i$ and for all nonempty $J \subseteq P_i$,

$$|B_J| \leq k_i - \sum_{j \in J} \delta_j \quad (15)$$

We can perform this procedure for all $i \in [s]$, and thus obtain a δ_j for all $j \in [\ell]$ via that $i \in [s]$ for which $j \in P_i$. We claim that these exact same δ_j 's satisfy condition (a) for A_1, \dots, A_ℓ . First, observe that

$$\sum_{j=1}^{\ell} \delta_j = \sum_{i=1}^s \sum_{j \in P_i} \delta_j = \sum_{i=1}^s k_i = \sum_{i=1}^s (k - |A_{P_i}|) = k - d,$$

where the last equation uses that the partition is tight.

Now we verify (11). Pick nonempty $I \subseteq [\ell]$. Let $\sigma \subseteq [s]$ be the set of indices i for which $I \cap P_i$ is nonempty. Then,

$$\begin{aligned}
|A_I| &= \left| \bigcap_{i \in \sigma} \bigcap_{j \in I \cap P_i} A_j \right| \\
&= \left| \bigcap_{i \in \sigma} \left(A_{P_i} \cup \bigcap_{j \in I \cap P_i} B_j \right) \right| \\
&\leq \left| \bigcap_{i \in \sigma} A_{P_i} \right| + \sum_{i \in \sigma} |B_{I \cap P_i}| \\
&= \left| \bigcap_{i \in \sigma} A_{P_i} \right| + \sum_{i \in \sigma} \left(k_i - \sum_{j \in I \cap P_i} \delta_j \right) \\
&= \left| \bigcap_{i \in \sigma} A_{P_i} \right| - \sum_{i \in \sigma} |A_{P_i}| + k|\sigma| - \sum_{j \in I} \delta_j \\
&= \left| \bigcap_{i \in \sigma} A_{P_i} \right| + \sum_{i \notin \sigma} |A_{P_i}| - \sum_{i \in [s]} |A_{P_i}| + k|\sigma| - \sum_{j \in I} \delta_j \\
&\leq ((s - |\sigma| + 1) - 1)k + d - ((s-1)k + d) + k|\sigma| - \sum_{j \in I} \delta_j
\end{aligned}$$

¹⁶Note that recursive padding in this induction as the “output” of the recursion is the δ_i 's satisfying (11) and not the subsequent modifications to the sets.

$$= k - \sum_{j \in I} \delta_j,$$

where the last inequality follows from applying (12) to the partition $\{\bigcup_{i \in \sigma} P_i\} \cup \{P_j : j \notin \sigma\}$. \square

3 Equivalence of GZP(ℓ) and MDS(ℓ)

In this section, we prove both Theorem 1.12 on computing the dimension of a generic intersection and that MDS(ℓ) is equivalent to GZP(ℓ) for all $\ell \geq 1$ (and thus that (a) and (c) are equivalent in Theorem 1.12).

3.1 GZP(ℓ) implies MDS(ℓ)

The key result toward proving that GZP(ℓ) implies MDS(ℓ) is the following:

Lemma 3.1. *Let C be an (n, k) -code whose generator matrix $G_{k \times n}$ is GZP(ℓ). Let $A_1, \dots, A_\ell \subseteq [n]$ be sets of size at most k . Then,*

$$\dim(G_{A_1} \cap \dots \cap G_{A_\ell}) = \max_{P_1 \sqcup P_2 \sqcup \dots \sqcup P_s = [\ell]} \left(\sum_{i \in [s]} \left| \bigcap_{j \in P_i} A_j \right| - (s-1)k \right) \quad (16)$$

where the maximum is over all partitions of $[\ell]$.

By Proposition 2.1, a generic matrix is GZP(ℓ) for all ℓ and thus Theorem 1.15 is an immediate corollary of Lemma 3.1. As a result, replacing the RHS of (16) with the LHS of (6), we have that any GZP(ℓ) code is also MDS(ℓ).

Proof of Lemma 3.1. We prove (16) as two inequalities. First we show that \geq direction of (16). Observe that for any $S \subset [\ell]$, $G_{A_S} \subset \bigcap_{j \in S} G_{A_j}$. Thus, for every partition $P_1 \sqcup P_2 \sqcup \dots \sqcup P_s = [\ell]$, we have that

$$\dim \bigcap_{i \in [s]} G_{A_{P_i}} \leq \dim \bigcap_{j \in [\ell]} G_{A_j}.$$

Thus, since G is MDS,¹⁷

$$\dim \bigcap_{j \in [\ell]} G_{A_j} \geq \dim \bigcap_{i \in [s]} G_{A_{P_i}} \geq k - \sum_{i \in [s]} \dim G_{A_{P_i}}^\perp = k - \sum_{i \in [s]} (k - |A_{P_i}|) = \sum_{i \in [s]} |A_{P_i}| - (s-1)k,$$

as desired.

Now we show that \leq direction. Let d be the RHS of (16); that is the minimum choice of d such that condition (b) in Lemma 2.8 holds. Thus, by the lemma, there exist $\delta_1, \dots, \delta_\ell \geq 0$ such that $\sum_{i=1}^\ell \delta_i = k - d$ and for all nonempty $I \subseteq [\ell]$,

$$|A_I| \leq k - \sum_{i \in I} \delta_i.$$

By Proposition 2.4, the pattern $\mathcal{S} := (S_1, \dots, S_k)$ with δ_i copies of A_i for each $i \in [\ell]$ and d copies of the empty set (assume $S_{k-d+1} = \dots = S_k = \emptyset$) is a generic zero pattern of order ℓ . Thus, since C is a GZP(ℓ) code, there exists an invertible matrix $M_{k \times k}$ such that MG has the zero pattern \mathcal{S} .

¹⁷See a similar argument in [BGM21].

Note that $\dim((MG)_{A_1} \cap \cdots \cap (MG)_{A_\ell}) = \dim(G_{A_1} \cap \cdots \cap G_{A_\ell})$. Thus, in order to show that $\dim(G_{A_1} \cap \cdots \cap G_{A_\ell}) \leq d$, it suffices to show that for any $z \in (MG)_{A_1} \cap \cdots \cap (MG)_{A_\ell}$, only the last d coordinates can be nonzero.

For each $i \in [\ell]$, let I_i be the indices j for which $S_j = A_i$. Since $z \in (MG)_{A_i}$, and MG has the zero pattern \mathcal{S} , we have that $z|_{I_i} = 0$. Thus,

$$z|_{\bigcup_{i \in [\ell]} I_i} = 0.$$

Thus, z is only nonzero on the coordinates corresponding to empty S_i 's in the partition. That is, only the last d coordinates of z can be nonzero, proving the dimension upper bound. \square

3.2 MDS(ℓ) implies GZP(ℓ)

The “(a) implies (c)” part of Theorem 1.12 follows from the following lemma.

Lemma 3.2. *Let C be a (n, k) -code which is MDS(ℓ). Let $G_{k \times n}$ be its generator matrix. Let $\mathcal{S} = (S_1, \dots, S_k)$ be a generic zero pattern of order ℓ . Then, G attains \mathcal{S} .*

Proof. By Corollary 2.6, there exists a maximal order- ℓ generic zero pattern \mathcal{S}' which is a superset of \mathcal{S} . That is, there are A_1, \dots, A_ℓ and $\delta_1, \dots, \delta_\ell$, such that \mathcal{S}' is the union for all $i \in [\ell]$ of δ_i copies of A_i plus $d := k - \sum_{i=1}^\ell \delta_i$ copies of the empty set. Further, by “maximality”, each A_i is of size $k - \delta_i$. It suffices to show that C attains \mathcal{S}' .

Because \mathcal{S}' is a generic zero pattern, we have for all nonempty $I \subseteq [\ell]$,

$$|A_I| \leq k - \sum_{i \in I} \delta_i.$$

Thus, by Lemma 2.8, we have that for all partitions \mathcal{P} of $[\ell]$, we have that

$$\sum_{P \in \mathcal{P}} |A_P| \leq (|\mathcal{P}| - 1)k + d.$$

For the partition, $\{1\} \cup \cdots \cup \{\ell\}$, we have equality because each $|A_i| = k - \delta_i$.

Thus, since C is MDS(ℓ), by Theorem 1.15, we have that

$$\dim(G_{A_1} \cap \cdots \cap G_{A_\ell}) = d.$$

Let $X := G_{A_1} \cap \cdots \cap G_{A_\ell}$ be this d -dimensional subspace of \mathbb{F}^k . Thus, by taking the dual,

$$X^\perp = G_{A_1}^\perp + \cdots + G_{A_\ell}^\perp.$$

Note that $\dim(G_{A_i}^\perp) = k - |A_i| = \delta_i$. And $\dim(X^\perp) = k - d = \sum_{i \in [\ell]} \delta_i$. Therefore, if for each $i \in [\ell]$, we pick a basis $(v_1^i, \dots, v_{\delta_i}^i)$ for $G_{A_i}^\perp$, then $(v_j^i : i \in [\ell], j \in [\delta_i])$ is a basis for X^\perp .

Let $M_{k \times k}$ be an arbitrary invertible matrix whose first $k - d$ rows are $(v_j^i : i \in [\ell], j \in [\delta_i])$. We claim that MG has zero pattern \mathcal{S} . For each $i \in [\ell]$ and $j \in [\delta_i]$, let i' be the row of M corresponding to v_j^i . For any $j' \in [n]$, we have that $(MG)_{i', j'}$ is the inner product¹⁸ of v_j^i and $G_{j'}$. If $j' \in A_i$, then $G_{j'} \in G_{A_i}$. Since $v_j^i \in G_{A_i}^\perp$, the inner product is 0.

Thus, MG indeed has the desired zero pattern. \square

¹⁸Here, “inner product” is the informal name for the bilinear form $\langle v, w \rangle = \sum_{i=1}^k v_i w_i$.

3.3 Characterizing the null intersection property

We recall from [BGM21] the following definition.

Definition 3.3. Let $A_1, \dots, A_\ell \subseteq [n]$ be sets of size at most k . We say that A_1, \dots, A_ℓ have the null intersection property if for a generic matrix $W_{k \times n}$ we have that

$$W_{A_1} \cap \dots \cap W_{A_\ell} = 0.$$

Note that Theorem 1.15 characterizes which sets have the null intersection property: they are those for which the RHS of (6) is equal to 0. Notably, [BGM21] also shows that the MDS(ℓ) condition is equivalent to attaining null intersection for any family of ℓ sets with the null intersection property:

Lemma 3.4 (Lemma 3.1 [BGM21]). Let C be a (n, k) -code with generator matrix G . Let $\ell \geq 1$. The following are equivalent.

- (a) C is MDS(ℓ).
- (b) C is MDS and for all $A_1, \dots, A_\ell \subseteq [n]$ of size at most k and $|A_1| + \dots + |A_\ell| = (\ell - 1)k$, we have that

$$G_{A_1} \cap \dots \cap G_{A_\ell} = 0$$

if and only if it holds generically.

Remark 3.5. Composing this lemma and the proof that MDS(ℓ) and GZP(ℓ) are equivalent, one can in fact show that GZP(ℓ) is equivalent to the seemingly weaker property that the matrix G attains all generic zero patterns with at most ℓ distinct sets including the empty set. We omit further details.

4 Applications to List Decoding: Proof of Theorem 1.4

In this section, we show that the recently established notions of higher-order MDS codes in the works of [BGM21] and [Rot21] are in fact equivalent. An equivalent way to define LD-MDS(L) codes is using the parity check matrix $H_{(n-k) \times n}$ matrix of C . C is LD-MDS(L) if there doesn't exist $L + 1$ distinct vectors $u_0, u_1, \dots, u_L \in \mathbb{F}^n$ such that

$$\sum_{i=0}^L \text{wt}(u_i) \leq L(n - k) \text{ and } Hu_0 = Hu_1 = \dots = Hu_L. \quad (17)$$

4.1 Equivalence of MDS and LD-MDS (up to duality)

We now prove that (a) iff (b) in Theorem 1.12. We will break the proof into Propositions 4.1 and 4.2.

Proposition 4.1. C is LD-MDS($\leq L$) $\Rightarrow C^\perp$ is MDS($L + 1$).

Proof. We will prove the contrapositive: C^\perp is not MDS($L + 1$) $\Rightarrow C$ is not LD-MDS($\leq L$).

Let C be a (n, k) -code and $H_{(n-k) \times n}$ be its parity check matrix. Note that H is the generator matrix of C^\perp . By Lemma 3.4, the fact that C^\perp is not MDS($L + 1$) implies that there exists subsets $J_0, J_1, \dots, J_L \subset [n]$ such that

1. $H_{J_0} \cap H_{J_1} \cap \cdots \cap H_{J_L} \neq 0$
2. $W_{J_0} \cap W_{J_1} \cap \cdots \cap W_{J_L} = 0$ for a generic $W_{(n-k) \times n}$.

By Theorem 1.15, (2) implies that for all partitions $P_1 \sqcup P_2 \sqcup \cdots \sqcup P_s = \{0, 1, \dots, L\}$, we have $\sum_{i=1}^s |J_{P_i}| \leq (s-1)(n-k)$ where $J_{P_i} = \bigcap_{j \in P_i} J_j$. (1) implies that there exist non-zero $u_0, u_1, \dots, u_L \in \mathbb{F}^n$ such that

$$\text{supp}(u_i) \subset J_i \text{ and } Hu_0 = Hu_1 = \cdots = Hu_L.$$

Suppose there are s distinct vectors among u_0, u_1, \dots, u_L . Let $P_1 \sqcup P_2 \sqcup \cdots \sqcup P_s = \{0, 1, \dots, L\}$ be the partition of $L+1$ into s parts such that all the $\{u_j : j \in P_i\}$ are equal for every $i \in [s]$ (and they are distinct if they fall in different parts). Let u_{P_i} be the common vector equal to $\{u_j : j \in P_i\}$. Note that $\text{supp}(u_{P_i}) \subset \bigcap_{j \in P_i} J_j = J_{P_i}$. Therefore we have s distinct non-zero vectors $u_{P_1}, u_{P_2}, \dots, u_{P_s}$ such that

$$\sum_{i=1}^s \text{wt}(u_{P_i}) \leq \sum_{i=1}^s |J_{P_i}| \leq (s-1)(n-k) \text{ and } Hu_{P_1} = Hu_{P_2} = \cdots = Hu_{P_s}.$$

If $s = 1$, we get $\text{wt}(u_{P_1}) \leq 0$ which is not possible since u_{P_1} is non-zero. Therefore $s \geq 2$ and this violates LD-MDS($s-1$) and therefore LD-MDS($\leq L$). \square

Proposition 4.2. C^\perp is MDS($L+1$) $\Rightarrow C$ is LD-MDS($\leq L$)

Proof. Since $\text{MDS}(\ell) \Rightarrow \text{MDS}(\leq \ell)$, it is enough to show that C^\perp is MDS(ℓ) $\Rightarrow C$ is LD-MDS($\ell-1$) for $\ell \geq 2$. We will prove the contrapositive: C is MDS and C is not LD-MDS($\ell-1$) $\Rightarrow C^\perp$ is not MDS(ℓ).

Let C be an MDS (n, k) -code and $H_{(n-k) \times n}$ be its parity check matrix. Note that H is the generator matrix of C^\perp . Since C is not LD-MDS($\ell-1$), there exist *distinct* $u_1, u_2, \dots, u_\ell \in \mathbb{F}^n$ such that

$$\sum_{i=1}^{\ell} \text{wt}(u_i) \leq (\ell-1)(n-k) \text{ and } Hu_1 = Hu_2 = \cdots = Hu_\ell.$$

Let $J_i = \text{supp}(u_i)$. WLOG, we can assume that $|J_i| \leq n-k$. We can also infer that all the u_i are non-zero, because if say $u_1 = 0$, then $\text{wt}(u_i) \geq n-k+1$ for all $i \geq 2$, which violates the $\sum_{i=1}^{\ell} \text{wt}(u_i) \leq (\ell-1)(n-k)$ condition. The following claim completes the proof, since it proves that C^\perp is not MDS(ℓ).

Claim 4.3. $\dim(H_{J_1} \cap H_{J_2} \cap \cdots \cap H_{J_\ell}) > \dim(W_{J_1} \cap W_{J_2} \cap \cdots \cap W_{J_\ell})$ for a generic $W_{(n-k) \times n}$.

Proof. If $\dim(W_{J_1} \cap \cdots \cap W_{J_\ell}) = 0$, then we are done because $Hu_1 \neq 0$ and $Hu_1 \in H_{J_1} \cap \cdots \cap H_{J_\ell}$. Therefore assume that $\dim(W_{J_1} \cap W_{J_2} \cap \cdots \cap W_{J_\ell}) > 0$. By Theorem 1.15,

$$\dim(W_{J_1} \cap \cdots \cap W_{J_\ell}) = \sum_{i=1}^s |J_{P_i}| - (s-1)(n-k)$$

for some partition $P_1 \sqcup \cdots \sqcup P_s = [\ell]$. Note that $s < \ell$, since $\sum_{i=1}^{\ell} |J_i| - (\ell-1)(n-k) \leq 0$. Let

$$V = \{(x_1, x_2, \dots, x_\ell) : Hx_1 = Hx_2 = \cdots = Hx_\ell \text{ and } \text{supp}(x_i) \subset J_i\}$$

which is a subspace of $(\mathbb{F}^n)^\ell$. Clearly $(u_1, u_2, \dots, u_\ell) \in V$. Define the linear map $f : H_{J_1} \cap H_{J_2} \cap \cdots \cap H_{J_\ell} \rightarrow V$ as: $f(y) = (x_1, x_2, \dots, x_\ell)$ where x_i is uniquely defined by $Hx_i = y$ and $\text{supp}(x_i) \subset J_i$. It is clear that f is a bijection which implies that

$$\dim(V) = \dim(H_{J_1} \cap H_{J_2} \cap \cdots \cap H_{J_\ell}).$$

Define

$$V_{\mathcal{P}} = \{(x_1, x_2, \dots, x_\ell) : Hx_1 = Hx_2 = \dots = Hx_\ell, \text{ supp}(x_i) \subset J_i \text{ and } x_j = x_{j'} \text{ if } j, j' \in P_i\}.$$

Clearly $V_{\mathcal{P}}$ is a subspace of V . But $(u_1, u_2, \dots, u_\ell) \notin V_{\mathcal{P}}$ since all the u_i are distinct, but the partition $\mathcal{P} = P_1 \sqcup \dots \sqcup P_s$ has only $s < \ell$ parts. Therefore $\dim(V) > \dim(V_{\mathcal{P}})$. We will now show that $\dim(V_{\mathcal{P}}) \geq \sum_{i=1}^s |J_{P_i}| - (s-1)(n-k)$ which finishes the proof of the claim.

Define the linear map $f_{\mathcal{P}} : H_{J_{P_1}} \cap H_{J_{P_2}} \cap \dots \cap H_{J_{P_s}} \rightarrow V_{\mathcal{P}}$ as: $f_{\mathcal{P}}(y) = (x_1, x_2, \dots, x_\ell)$ where x_i is uniquely defined by $Hx_i = y$ where $\text{supp}(x_i) \subset J_{P_j}$ where $i \in P_j$. Again, $f_{\mathcal{P}}$ is also a bijection. Therefore $\dim(V_{\mathcal{P}}) = \dim(H_{J_{P_1}} \cap \dots \cap H_{J_{P_s}})$. By Theorem 1.15, for a generic $W_{(n-k) \times n}$, $\dim(H_{J_{P_1}} \cap \dots \cap H_{J_{P_s}}) \geq \dim(W_{J_{P_1}} \cap \dots \cap W_{J_{P_s}}) \geq \sum_{i=1}^s |J_{P_i}| - (s-1)(n-k)$. \square

\square

4.2 Reed-Solomon codes

4.2.1 Generic Reed-Solomon codes

Our main result Theorem 1.4 follows from this next result on duals of generic Reed-Solomon codes.

Proposition 4.4. *The dual of a generic Reed-Solomon code is equivalent to a generic Reed-Solomon code (up-to scaling of columns of the generator matrix).*

Proof. Let C be a generic (n, k) -Reed-Solomon code. Let $(\alpha_1, \dots, \alpha_n)$ be the generators of C . Let C' be the $(n, n-k)$ -code also generated by $(\alpha_1, \dots, \alpha_n)$. Let $G'_{n-k, n}$ be the Vandermonde matrix with generators $(\alpha_1, \dots, \alpha_n)$. Note that by definition G' is also generic.

For all $i \in [n]$, let $\Delta_i = \prod_{j \in [n] \setminus \{i\}} (\alpha_i - \alpha_j)$. By standard results¹⁹ on Reed-Solomon codes, C^\perp is a *generalized* Reed-Solomon code with generator matrix H such that $H_{j,i} = \alpha_i^{j-1} / \Delta_i$. Since C is generic, we have that $\Delta_i \neq 0$ for all $i \in [n]$. Therefore, each column of H is a nonzero scalar multiple of a column of G' . Thus C^\perp is equivalent to a generic Reed-Solomon code. \square

Proof of Theorem 1.4. From Theorem 1.11 (GM-MDS), Theorem 1.12, and Proposition 4.4, we know that generic Reed-Solomon codes are LD-MDS(L) for all L . In other words they are (ρ, L) -average-radius list-decodable for $\rho = \frac{L}{L+1}(1-R)$ for all L . This also implies that they are (ρ, L) -list-decodable for the same ρ . \square

4.2.2 Random Reed-Solomon codes

Here we prove Theorem 1.5 and show how one can make Theorem 1.4 more quantitative in order to reason about the list-decoding capabilities of a *random* Reed-Solomon code. For a code parameters (n, k) and a finite field \mathbb{F} , we define a random Reed-Solomon code to be one whose generators $\alpha_1, \dots, \alpha_n$ are chosen uniformly and independently from \mathbb{F} .

Proposition 4.5. *Let n, k, L be positive integers. There exists a function $c(n, k, L) = 2Ln^2 \binom{n}{\leq n-k}^{L+1}$ such that a random (n, k) -Reed-Solomon code is LD-MDS($\leq L$), and thus $(\frac{\ell}{L+1}(1-k/n), \ell)$ -list decodable for all $\ell \leq L$, with probability at least $1 - c/|\mathbb{F}|$.*

¹⁹See, for example, [MS77] or Theorem 5.1.6 in [Hal].

Proof. Let C be the code generated by the random $\alpha_1, \dots, \alpha_n$. With probability at least $1 - n^2/|\mathbb{F}|$, we have that $\alpha_i \neq \alpha_j$ for all $i \neq j \in [n]$ and thus C is MDS. From the proof of Proposition 4.4 and Theorem 1.12, we then have that $(\alpha_1, \dots, \alpha_n)$ generate a LD-MDS($\leq L$) matrix if and only if the $(n, n-k)$ -matrix G' with entries $G'_{j,i} = \alpha_i^{j-1}$ is MDS($L+1$). In order to check that G' is MDS(ℓ), it suffices to show by Lemma 3.4 that for all null intersecting families $A_1, \dots, A_{L+1} \subseteq [n]$, each of size at most $n-k$, with total size $L(n-k)$, we have that

$$G'_{A_1} \cap \dots \cap G'_{A_{L+1}} = 0.$$

This condition is equivalent to (see Appendix B of [BGM21]) the following block matrix being nonsingular:

$$\begin{pmatrix} G'_{A_1} & G'_{A_2} & & & \\ G'_{A_1} & & G'_{A_3} & & \\ \vdots & & & \ddots & \\ G'_{A_1} & & & & G'_{A_{L+1}} \end{pmatrix}$$

The square matrix has size $L(n-k)$ and each entry has degree at most $n-k-1$. Therefore, the determinant, which we know must not symbolically vanish by Corollary 1.14, has total degree at most Ln^2 . Therefore, by the Schwartz-Zippel lemma [Sch80, Zip79], the probability that this determinant is zero is at most $\frac{Ln^2}{|\mathbb{F}|}$. Now, the number of choices²⁰ of $A_1, \dots, A_{L+1} \subseteq [n]$ to consider is at most $\binom{n}{\leq n-k}^{L+1}$. Therefore, the probability that G' is MDS($L+1$), and thus C is LD-MDS($\leq L$) is at most,

$$1 - \frac{n^2 + Ln^2 \binom{n}{\leq n-k}^{L+1}}{|\mathbb{F}|},$$

as desired. \square

Remark 4.6. The work [BGM21] shows that a random linear code achieves MDS(ℓ) at field size $O_\ell(n^{(n-k)(\ell-1)}(n-k)^{2\ell(n-k)})$, and thus is MDS($\leq L$) with field size $n^{O(kL)}$. Since we prove that generic Reed-Solomon codes are LD-MDS($\leq L$), one can adapt their methods to then show that one can take $c(n, k, L) = n^{O(\min(k, n-k)L)}$ in Theorem 1.5.

5 Connections to Invariant Theory

The combinatorial characterization of the generic intersection dimension in Theorem 1.15 allows for a surprising connection between MDS(ℓ) codes and invariant theory. A simple observation characterizes the generic intersection dimension as an instance of the well-known Edmonds problem, i.e., a computation of the rank of a symbolic matrix with linear entries, see [BGM21, Appendix B]. The Edmonds' problem is not known to have a polynomial-time algorithm. Nevertheless, the non-commutative version²¹ of the Edmonds' problem does have a polynomial-time algorithm, but this is highly non-trivial and rests on some deep results in invariant theory, see [GGOW16, IQS18]. The combinatorial characterization in Theorem 1.15 allows us to prove in a curious way that the Edmonds' problem for the generic intersection dimension is equivalent to its non-commutative counterpart, which then immediately yields a polynomial-time algorithm for computing generic intersection dimension.

²⁰This can be optimized.

²¹The symbolic variables are considered non-commutative, the base field remains commutative.

5.1 Linear matrices, non-commutative rank and the blow-up regularity lemma

A matrix $L = t_1X_1 + \cdots + t_mX_m$, where X_i are $p \times q$ matrices with entries in a ground field \mathbb{F} and t_i are indeterminates. is called a linear matrix. There are two important notions of ranks associated to such a linear matrix are the commutative rank and the non-commutative rank. We first state their definitions and then clarify the terminology.

Definition 5.1. *Let $L = t_1X_1 + \cdots + t_mX_m$ be a linear matrix.*

- *The commutative rank $\text{crk}(L)$ is defined as $\text{rank}(L)$ viewed as a matrix with entries in the function field $\mathbb{F}(t_1, \dots, t_m)$.*
- *The non-commutative rank $\text{ncrk}(L)$ is defined as $\text{rank}(L)$ viewed as a matrix with entries in the free skew-field $\mathbb{F}\langle t_1, \dots, t_m \rangle$.*

The reader not interested in skew-fields can very much ignore the skew-fields as long as they accept the characterization of non-commutative rank in terms of blow-ups in (18) below, and perhaps take that to be the definition of non-commutative rank. For the interested readers, we give a few details, but point to references for more details.

First, we note that most of linear algebra works over skew-fields (a.k.a. division algebras). Rank is defined in terms of maximum number of (left)-linearly independent columns. This is sometimes called left column rank. Similarly one can define left and right row and column ranks. Left column rank equals the right row rank and the right column rank equals the left row rank, but the left column rank may not equal the right column rank when working over a general division algebra. For linear matrices interpreted as matrices with entries in the free skew-field, all ranks, i.e., left/right row/column ranks, are all the same.

The free skew-field itself is a technically challenging object to explain, but we will try to give a brief idea of its purpose. If you start with a (commutative) field \mathbb{F} and add m elements t_1, \dots, t_m that have no extra relations on them other than the ones imposed by the axioms of a commutative field (that is one way to define a set of indeterminates), the field generated will be the function field $\mathbb{F}(t_1, \dots, t_m)$. The analogous object where you impose no extra relations other than the ones imposed by the axioms of a skew-field will create the free skew-field. However, unlike the well understood function field, the free skew-field is far more difficult to understand and there are several intricacies in constructing it or even showing its existence. For the reader interested in the details of free skew-fields, we refer to [GGOW16] for a gentle introduction and references therein for more technical details, we will not really need them here.

Computing the commutative rank of a linear matrix is the Edmonds' problem and computing the non-commutative rank is the non-commutative version of the Edmonds' problem. Interpolating between these two ranks are the ranks of *blow-ups*, a tool that originated in invariant theory and is crucial in understanding the non-commutative rank. These blow-ups are also crucial for our purposes.

Definition 5.2. *Let $L = t_1X_1 + \cdots + t_mX_m$ be a linear matrix of size $p \times q$. Then, for $d \in \mathbb{Z}_{\geq 1}$, we define the d^{th} blow-up of L to be the $dp \times dq$ matrix*

$$L(T_1, \dots, T_m) := X_1 \otimes T_1 + \cdots + X_m \otimes T_m,$$

where T_i are $d \times d$ matrices whose entries are all distinct variables, say $t_{j,k}^{(i)}$. We define the d^{th} blow-up rank of L by

$$\text{rank}_d(L) := \text{crk}(L(T_1, \dots, T_m)),$$

i.e., the latter rank is taken by viewing $L(T_1, \dots, T_m)$ as a matrix with entries in the function field $\mathbb{F}(t_{j,k}^{(i)})$.

Let us first justify the notation $L(T_1, \dots, T_m) := X_1 \otimes T_1 + \dots + X_m \otimes T_m$. To get $\sum_i X_i \otimes T_i$ from L we replace each entry with a $d \times d$ matrix as follows: if the $(\alpha, \beta)^{th}$ entry of L is of the form $\sum_i c_i t_i$, then we replace it with $\sum_i c_i T_i$. Thus, it is as if we plugged in T_i for t_i . We have the equality (see [IQS17, IQS18]):

$$\text{ncrk}(L) = \lim_{d \rightarrow \infty} \frac{\text{rank}_d(L)}{d} = \sup_d \frac{\text{rank}_d(L)}{d} = \max_d \frac{\text{rank}_d(L)}{d}. \quad (18)$$

Dividing the rank of the blow-up by d is a normalization is to be expected because we blow-up the size of the matrix by a factor of d . There are a few subtleties, for example the sequence $\frac{\text{rank}_d(L)}{d}$ is not always monotone. But perhaps the major subtlety the reader may have noticed is that while $\text{ncrk}(L)$ is an integer by definition, it is not so clear why any of the other expressions are integers. This is a consequence of an amazing result called the blow-up regularity lemma²² that was first proved by Ivanyos, Qiao and Subrahmanyam in [IQS17]. A more conceptual proof can be found in [DM18].

Theorem 5.3 (Blow-up regularity Lemma, [IQS17]). *Let $L = \sum_{i=1}^m t_i X_i$ be a linear matrix. Then $\frac{\text{rank}_d(L)}{d}$ is an integer.*

5.2 Polynomial time computability of generic intersection ranks

Let $W = (w_{ij})$ be a $k \times n$ matrix of indeterminates. Let $\mathcal{A} = (A_1, \dots, A_\ell)$ be a ℓ -tuple of subsets of $[n]$. Define

$$L_{\mathcal{A}}(W) = \begin{pmatrix} W^{A_1} & W^{A_2} & 0 & 0 & 0 \\ W^{A_1} & 0 & W^{A_3} & 0 & 0 \\ \vdots & 0 & 0 & \ddots & 0 \\ W^{A_1} & 0 & 0 & 0 & W^{A_\ell} \end{pmatrix}$$

where W^{A_i} is the submatrix of W obtained by restricted to the columns of A_i .

Observe that $L_{\mathcal{A}}(W)$ is a linear matrix, i.e., each entry is a linear function in the w_{ij} 's (it's much more special than that of course, indeed each entry is either a variable or 0). So, we can write $L_{\mathcal{A}}(W) = \sum_{i,j} w_{ij} X_{ij}$.

The following definition is perhaps a little unnecessary, but it allows us to present easier the arguments in this section.

Definition 5.4 (Generic Intersection rank). *The function rank_{GI} takes as input the configuration $(k, n, \mathcal{A} = (A_1, \dots, A_\ell))$ where $A_i \subseteq [n]$ and returns $\dim(\bigcap_i W_{A_i})$ where W is a $d \times n$ matrix of indeterminates, i.e.,*

$$\text{rank}_{GI}(k, n, \mathcal{A}) = \dim \left(\bigcap_i W_{A_i} \right).$$

From Appendix B of [BGM21], we have that

$$\text{rank}_{GI}(k, n, \mathcal{A}) = \sum_i |A_i| - \text{crk}(L_{\mathcal{A}}(W)). \quad (19)$$

²²This is just called the regularity lemma, but we call it the blow-up regularity lemma to avoid confusion with the regularity criterion.

5.2.1 A doubling operation

Given a configuration (k, n, \mathcal{A}) , we will define a doubling operation as follows. We will assume without loss of generality that $|A_i| \leq d$ for all i . First, identify $[2n]$ with $\{1, \tilde{1}, 2, \tilde{2}, \dots, n, \tilde{n}\}$. Then, for each $A_i \in \mathcal{A}$, define

$$A_i^{(2)} := A_i \cup \tilde{A}_i \subseteq \{1, \tilde{1}, 2, \tilde{2}, \dots, n, \tilde{n}\},$$

where $\tilde{A}_i := \{\tilde{a} : a \in A_i\}$. We insist that we will order the elements in $A_i^{(2)}$ in the increasing order where the order is given by $1 < \tilde{1} < 2 < \dots < n < \tilde{n}$, so for example if $A_i = \{1, 2\}$, then $A_i^{(2)} = \{1, \tilde{1}, 2, \tilde{2}\}$. Finally, define

$$\mathcal{A}^{(2)} := (A_1^{(2)}, \dots, A_\ell^{(2)}).$$

Definition 5.5 (Doubling configuration). *To the configuration $(k, n, \mathcal{A} = (A_1, \dots, A_\ell))$ with each $A_i \subseteq [n]$, we will define the doubled configuration $(2k, 2n, \mathcal{A}^{(2)} = (A_1^{(2)}, \dots, A_\ell^{(2)}))$ as defined above.*

Now, consider a $2k \times 2n$ matrix U consisting of indeterminates, but let us index the rows and columns a little differently. Let us index the rows by $R = \{1, 1', 2, 2', \dots, d, d'\}$, and the columns by $C = \{1, \tilde{1}, 2, \tilde{2}, \dots, n, \tilde{n}\}$. So, the $(i, j)^{th}$ entry of U is u_{ij} for $i \in R, j \in C$. So, for example if I am looking at the $(3', 4)$ entry, I will denote it $u_{3', 4}$.

If one looks at the picture above of $L_{\mathcal{A}}(W)$ and replaces each w_{ij} with $U_{ij} = \begin{pmatrix} u_{ij} & u_{i, \tilde{j}} \\ u_{i'j} & u_{i', \tilde{j}} \end{pmatrix}$, it should be evident that one obtains $L_{\mathcal{A}^{(2)}}(U)$ – we picked our indexing precisely to orchestrate this. In other words, we have

$$L_{\mathcal{A}^{(2)}}(U) = L_{\mathcal{A}}(W)(U_{11}, U_{12}, \dots, U_{nn}),$$

where by $L_{\mathcal{A}}(W)(U_{11}, U_{12}, \dots, U_{nn})$, we mean take the matrix $L_{\mathcal{A}}(W)$ and replace w_{ij} by U_{ij} for all i, j (note that this is consistent with the notation in Definition 5.2). In particular, since the U_{ij} are 2×2 matrices whose entries are all independent indeterminates, we conclude that $\text{rank}_2(L_{\mathcal{A}}(W)) = \text{crk}(L_{\mathcal{A}^{(2)}}(U))$. This yields

Corollary 5.6. *Let W be a $d \times n$ matrix with indeterminates. Let (k, n, \mathcal{A}) be a configuration, and let $(2k, 2n, \mathcal{A}^{(2)})$ be the doubled configuration. Then*

$$\text{rank}_{GI}(2k, 2n, \mathcal{A}^{(2)}) = 2\left(\sum_i |A_i| - \text{rank}_2(L_{\mathcal{A}}(W))\right).$$

Further, this means that $\text{rank}_{GI}(2k, 2n, \mathcal{A}^{(2)})$ is a multiple of 2.

Proof. The equality $\text{rank}_{GI}(2k, 2n, \mathcal{A}^{(2)}) = 2\sum_i |A_i| - \text{rank}_2(L_{\mathcal{A}}(W))$ follows from the above discussion along with (19). By the blow-up regularity lemma, i.e., Theorem 5.3, we know that $\text{rank}_2(L_{\mathcal{A}}(V))$ is a multiple of 2, and hence so is $\text{rank}_{GI}(2k, 2n, \mathcal{A}^{(2)})$. \square

Analogously, for $t \in \mathbb{Z}_{\geq 1}$, we define the t -pled configuration $(tk, tn, \mathcal{A}^{(t)} = (A_1^{(t)}, \dots, A_\ell^{(t)}))$.

Corollary 5.7. *Let W be a $k \times n$ matrix with indeterminates. Let (k, n, \mathcal{A}) be a configuration, and let $(tk, tn, \mathcal{A}^{(t)})$ be the t -pled configuration. Then*

$$\text{rank}_{GI}(tk, tn, \mathcal{A}^{(t)}) = t\left(\sum_i |A_i| - \text{rank}_t(L_{\mathcal{A}}(W))\right).$$

Further, this means that $\text{rank}_{GI}(tk, tn, \mathcal{A}^{(t)})$ is a multiple of t .

5.2.2 Scalability of generic intersection dimension

Lemma 5.8. *Let (k, n, \mathcal{A}) be a configuration, and let $(tk, tn, \mathcal{A}^{(t)})$ be the t -pled configuration. Then*

$$\text{rank}_{GI}(tk, tn, \mathcal{A}^{(t)}) = t \cdot \text{rank}_{GI}(k, n, \mathcal{A}).$$

Proof. Suppose \mathcal{A} consists of ℓ sets. Then, so does $\mathcal{A}^{(t)}$. With this observation, the lemma follows immediately from Theorem 1.15 since the dimension of the t -pled configuration $(tk, tn, \mathcal{A}^{(t)})$ is also a maximum over all partitions of ℓ (i.e., the number of parts in \mathcal{A}) and each corresponding term is t times larger than the one for the configuration (k, n, \mathcal{A}) . \square

Corollary 5.9. *Given the configuration (k, n, \mathcal{A}) , we have*

$$\text{rank}_{GI}(k, n, \mathcal{A}) = \sum_i |A_i| - \text{ncrk}(L_{\mathcal{A}}(W)).$$

Proof. From the above lemma and Corollary 5.7, it follows that for any $t \in \mathbb{Z}_{\geq 1}$,

$$t(\sum_i |A_i|) - \text{rank}_t(L_{\mathcal{A}}(W)) = \text{rank}_{GI}(tk, tn, \mathcal{A}^{(t)}) = t(\text{rank}_{GI}(k, n, \mathcal{A})) = t(\sum_i |A_i|) - t \cdot \text{crk}(L_{\mathcal{A}}(W)).$$

This means that $t \cdot \text{crk}(L_{\mathcal{A}}(W)) = \text{rank}_t(L_{\mathcal{A}}(W))$, so

$$\text{ncrk}(L_{\mathcal{A}}(W)) = \lim_{t \rightarrow \infty} \text{rank}_t(L_{\mathcal{A}}(W))/t = \text{crk}(L_{\mathcal{A}}(W)).$$

Thus, we conclude that

$$\text{rank}_{GI}(k, n, \mathcal{A}) = \sum_i |A_i| - \text{ncrk}(L_{\mathcal{A}}(W)). \quad \square$$

Proof of Theorem 1.21. Let $\mathcal{A} = (A_1, \dots, A_{\ell})$. Then, in the notation of this section, we have $\dim(W_{A_1} \cap W_{A_2} \cap \dots \cap W_{A_{\ell}}) = \text{rank}_{GI}(k, n, \mathcal{A})$. By the above corollary, we have $\text{rank}_{GI}(k, n, \mathcal{A}) = \sum_i |A_i| - \text{ncrk}(L_{\mathcal{A}}(W))$, so it suffices to compute $\text{ncrk}(L_{\mathcal{A}}(W))$. But there is a polynomial time algorithm for this [IQS18].²³ Note that the size of $L_{\mathcal{A}}(W)$ is $\text{poly}(k, \ell)$, so there is no dependence on n in the runtime. \square

References

- [BFG⁺19] Peter Bürgisser, Cole Franks, Ankit Garg, Rafael Oliveira, Michael Walter, and Avi Wigderson. Towards a theory of non-commutative optimization: Geodesic 1st and 2nd order methods for moment maps and polytopes. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 845–861. IEEE, 2019.
- [BGM21] Joshua Brakensiek, Sivakanth Gopi, and Visu Makam. Lower bounds for maximally recoverable tensor code and higher order MDS codes. *arXiv preprint arXiv:2107.10822*, 2021.
- [BSKR09] Eli Ben-Sasson, Swastik Kopparty, and Jaikumar Radhakrishnan. Subspace polynomials and limits to list decoding of Reed-Solomon codes. *IEEE Transactions on Information Theory*, 56(1):113–120, 2009.

²³Alternately, one can use the algorithm in [GGOW16], but this needs to be appropriately modified because the algorithm as stated can only check if the non-commutative rank of a square matrix is full or not.

- [CW07] Qi Cheng and Daqing Wan. On the list and bounded distance decodability of Reed-Solomon codes. *SIAM Journal on Computing*, 37(1):195–209, 2007.
- [DB81] Nicolaas Govert De Bruijn. *Asymptotic methods in analysis*, volume 4. Courier Corporation, 1981.
- [DL12] Zeev Dvir and Shachar Lovett. Subspace evasive sets. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 351–358, 2012.
- [DM17] Harm Derksen and Visu Makam. Polynomial degree bounds for matrix semi-invariants. *Adv. Math.*, 310:44–63, 2017.
- [DM18] Harm Derksen and Visu Makam. On non-commutative rank and tensor rank. *Linear Multilinear Algebra*, 66(6):1069–1084, 2018.
- [DSDY13] Son Hoang Dau, Wentu Song, Zheng Dong, and Chau Yuen. Balanced sparsest generator matrices for mds codes. In *2013 IEEE International Symposium on Information Theory*, pages 1889–1893. IEEE, 2013.
- [DSY14] Son Hoang Dau, Wentu Song, and Chau Yuen. On the existence of MDS codes over small fields with constrained generator matrices. In *2014 IEEE International Symposium on Information Theory*, pages 1787–1791. IEEE, 2014.
- [Eli57] P Elias. List decoding for noisy channels. In *IRE WESCON Convention Record, 1957*, volume 2, pages 94–104, 1957.
- [FKS22] Asaf Ferber, Matthew Kwan, and Lisa Sauermann. List-decodability with large radius for Reed-Solomon codes. *IEEE Transactions on Information Theory*, 2022.
- [Gab] Ernst M Gabidulin. Rank-metric codes and applications. *Moscow Inst. Phys. Technol., State Univ., Dolgoprudny, Russia.*[Online]. Available: <http://iitp.ru/upload/content/839/Gabidulin.pdf>.
- [Gab21] Ernst M Gabidulin. *Rank codes*. TUM. University Press, 2021.
- [GGOW16] Ankit Garg, Leonid Gurvits, Rafael Oliveira, and Avi Wigderson. A deterministic polynomial time algorithm for non-commutative rational identity testing. In *57th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2016*, pages 109–117. IEEE Computer Soc., Los Alamitos, CA, 2016.
- [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 Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 2092–2108. SIAM, 2017.
- [GLS93] Martin Grötschel, László Lovász, and Alexander Schrijver. *Geometric Algorithms and Combinatorial Optimization*, volume 2. Springer Science & Business Media, 1993.
- [GLS⁺22] Zeyu Guo, Ray Li, Chong Shangguan, Itzhak Tamo, and Mary Wootters. Improved list-decodability and list-recoverability of Reed-Solomon codes via tree packings. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 708–719. IEEE, 2022.

- [GM21] Venkatesan Guruswami and Jonathan Mosheiff. Punctured low-bias codes behave like random linear codes. *arXiv preprint arXiv:2109.11725*, 2021.
- [GR08] Venkatesan Guruswami and Atri Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Transactions on Information Theory*, 54(1):135–150, 2008.
- [GRS12] Venkatesan Guruswami, Atri Rudra, and Madhu Sudan. Essential coding theory. *Draft available at <http://www.cse.buffalo.edu/~atri/courses/coding-theory/book>*, 2012.
- [GS98] V. Guruswami and M. Sudan. Improved Decoding of Reed-Solomon and Algebraic-Geometric Codes. In *39th Annual Symposium on Foundations of Computer Science, 1998. Proceedings*, pages 28–37, November 1998.
- [GST21a] Eitan Goldberg, Chong Shangguan, and Itzhak Tamo. List-decoding and list-recovery of Reed-Solomon codes beyond the johnson radius for any rate. *arXiv preprint arXiv:2105.14754*, 2021.
- [GST21b] Eitan Goldberg, Chong Shangguan, and Itzhak Tamo. Singleton-type bounds for list-decoding and list-recovery, and related results. *arXiv preprint arXiv:2112.05592*, 2021.
- [GX12] Venkatesan Guruswami and Chaoping Xing. Folded codes from function field towers and improved optimal rate list decoding. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 339–350, 2012.
- [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.
- [Hal] JI Hall. Notes on coding theory (chapter 5—generalized Reed-Solomon codes). *Department of Mathematics, Michigan State University available online at <http://users.math.msu.edu/users/jhall/classes/codenotes/coding-notes.html> (Jan. 7, 2015 revision)*.
- [HHYD14] Wael Halbawi, Tracey Ho, Hongyi Yao, and Iwan Duursma. Distributed reed-solomon codes for simple multiple access networks. In *2014 IEEE International Symposium on Information Theory*, pages 651–655, 2014.
- [HSX⁺12] Cheng Huang, Huseyin Simitci, Yikang Xu, Aaron Ogus, Brad Calder, Parikshit Gopalan, Jin Li, and Sergey Yekhanin. Erasure coding in windows azure storage. In *2012 USENIX Annual Technical Conference (USENIX ATC 12)*, pages 15–26, 2012.
- [IQS17] Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Non-commutative Edmonds’ problem and matrix semi-invariants. *Comput. Complexity*, 26(3):717–763, 2017.
- [IQS18] Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Constructive non-commutative rank computation is in deterministic polynomial time. *Comput. Complexity*, 27(4):561–593, 2018.
- [Joh62] Selmer Johnson. A new upper bound for error-correcting codes. *IRE Transactions on Information Theory*, 8(3):203–207, 1962.

- [KRZSW18] Swastik Kopparty, Noga Ron-Zewi, Shubhangi Saraf, and Mary Wootters. Improved decoding of folded Reed-Solomon and multiplicity codes. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 212–223. IEEE, 2018.
- [Lov18] Shachar Lovett. MDS matrices over small fields: A proof of the GM-MDS conjecture. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 194–199. IEEE, 2018.
- [MLR⁺14] Subramanian Muralidhar, Wyatt Lloyd, Sabyasachi Roy, Cory Hill, Ernest Lin, Weiqi Liu, Satadru Pan, Shiva Shankar, Viswanath Sivakumar, Linpeng Tang, et al. f4: Facebook’s warm BLOB storage system. In *11th USENIX Symposium on Operating Systems Design and Implementation (OSDI 14)*, pages 383–398, 2014.
- [MRRZ⁺20] Jonathan Mosheiff, Nicolas Resch, Noga Ron-Zewi, Shashwat Silas, and Mary Wootters. LDPC codes achieve list decoding capacity. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 458–469. IEEE, 2020.
- [MS77] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error correcting codes*, volume 16. Elsevier, 1977.
- [Mul17] Ketan Mulmuley. Geometric complexity theory v: Efficient algorithms for noether normalization. *Journal of the American Mathematical Society*, 30(1):225–309, 2017.
- [PV05] Farzad Parvaresh and Alexander Vardy. Correcting errors beyond the guruswami-sudan radius in polynomial time. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS’05)*, pages 285–294. IEEE, 2005.
- [Rot21] Ron M Roth. Higher-order MDS codes. *arXiv preprint arXiv:2111.03210*, 2021.
- [RS60] Irving S Reed and Gustave Solomon. Polynomial codes over certain finite fields. *Journal of the society for industrial and applied mathematics*, 8(2):300–304, 1960.
- [RW14] Atri Rudra and Mary Wootters. Every list-decodable code for high noise has abundant near-optimal rate puncturings. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 764–773, 2014.
- [Sch80] Jacob T Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM (JACM)*, 27(4):701–717, 1980.
- [ST20] Chong Shangquan and Itzhak Tamo. Combinatorial list-decoding of Reed-Solomon codes beyond the johnson radius. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 538–551, 2020.
- [Sud97] Madhu Sudan. Decoding of Reed Solomon codes beyond the error-correction bound. *Journal of complexity*, 13(1):180–193, 1997.
- [VW01] Van Lint, Jacobus Hendricus and Wilson, Richard Michael. *A course in combinatorics*. Cambridge university press, 2001.
- [WB99] Stephen B Wicker and Vijay K Bhargava. *Reed-Solomon codes and their applications*. John Wiley & Sons, 1999.
- [Woz58] John M Wozencraft. List decoding. *Quarterly Progress Report*, 48:90–95, 1958.

- [YH19a] Hikmet Yildiz and Babak Hassibi. Gabidulin codes with support constrained generator matrices. *IEEE Transactions on Information Theory*, 66(6):3638–3649, 2019.
- [YH19b] Hikmet Yildiz and Babak Hassibi. Optimum linear codes with support-constrained generator matrices over small fields. *IEEE Transactions on Information Theory*, 65(12):7868–7875, 2019.
- [YRH20] Hikmet Yildiz, Netanel Raviv, and Babak Hassibi. Support constrained generator matrices of Gabidulin codes in characteristic zero. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 60–65, 2020.
- [YS13] Muxi Yan and Alex Sprintson. Algorithms for weakly secure data exchange. In *2013 International Symposium on Network Coding (NetCod)*, pages 1–6. IEEE, 2013.
- [Zip79] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *International symposium on symbolic and algebraic manipulation*, pages 216–226. Springer, 1979.
- [ZP81] Victor Vasilievich Zyablov and Mark Semenovich Pinsker. List cascade decoding. *Problemy Peredachi Informatsii*, 17(4):29–33, 1981.

A Resolution of Conjecture 5.7 of [ST20]

Shangguan and Tamo [ST20] made an algebraic conjecture in their paper (see Conjecture 5.7 from [ST20]) about the non-singularity of certain symbolic matrices, which would imply that generic Reed-Solomon codes achieve list decoding capacity. We prove this conjecture here, the proof follows from some of the results in our paper which we use to prove Theorem 1.4. We first introduce the necessary notation to properly state Conjecture 5.7 of [ST20].

Let C be a (n, k) -code with generator matrix G . Let $J_1, \dots, J_t \subseteq [n]$. We define a block matrix $M_{G, (J_1, \dots, J_t)}$ as follows. For each $i, j \in [t]$ with $i < j$, there is a block of k columns of M corresponding to (i, j) . The rows of M are filled in as follows.

- (a) For each $i, j \subseteq [t - 1]$ with $i < j$, we add k rows for which the identity matrix I_k appears in the (i, j) and (j, t) blocks. The matrix $-I_k$ appears in the (i, t) block. All other blocks are zero.
- (b) For each $\{i, j\} \subseteq [t]$, we add $|J_i \cap J_j|$ rows for which the $\{i, j\}$ block equals $G_{J_i \cap J_j}^\top$, with all other blocks being zero.

Thus, M has $\binom{t}{2}k$ columns and $\binom{t-1}{2}k + \sum_{i \neq j} |J_i \cap J_j|$ rows. The following lemma of [ST20] relates $M_{G, (J_1, \dots, J_t)}$ to list decoding properties of C .

Lemma A.1 ([ST20]). *Let $L, \tau \geq 1$. Assume there exists $c_0, c_1, \dots, c_L \in C \cap B_\tau(y)$. Then, there exist J_0, \dots, J_L such that $|J_i| \geq n - \tau$ for all i and $M_{G, (J_0, \dots, J_L)}$ does not have full column rank.*

To give intuition about M , we include an adaptation of [ST20]’s proof of this lemma for completeness.

Proof. For all $i \in \{0, 1, \dots, L\}$, let J_i be the set of coordinates for c_i and y are equal. Since $c_i \in B_\tau(y)$, we have that $|J_i| \geq n - \tau$. Since G is the generator matrix of C , for all $i \in \{0, 1, \dots, L\}$,

there exists a unique $f_i \in \mathbb{F}^k$ such that $c_i = G^\top f_i$. For all $i, j \in \{0, 1, \dots, L\}$ with $i < j$ let $f_{ij} = f_j - f_i$.

Let v be a column vector of length $\binom{t}{2}k$ which is the f_{ij} 's concatenated together in the order as the block columns (i, j) of M are indexed. To complete, the proof suffices to show that $v \neq 0$ but $Mv = 0$.

First, to see why $v \neq 0$, note that

$$G^\top f_{01} = G^\top (f_1 - f_0) = c_1 - c_0 \neq 0.$$

Thus, $f_{01} \neq 0$, so $v \neq 0$.

Second, to see why $Mv = 0$, we split the analysis into the type (a) rows and the type (b) rows. For the type (a) rows, for each $i < j \in \{0, 1, \dots, L-1\}$ note that Mv restricted to this block equals $f_{ij} + f_{jt} - f_{it} = (f_j - f_i) + (f_t - f_j) - (f_t - f_i) = 0$. For the type (b) rows, it suffices to check for all $i < j \in \{0, 1, \dots, L\}$ that $G_{J_i \cap J_j}^\top f_{ij} = 0$. Observe that

$$G_{J_i \cap J_j}^\top f_{ij} = G_{J_i \cap J_j}^\top (f_j - f_i) = (c_j - c_i)|_{J_i \cap J_j}$$

Note that, by definition, for all indices $a \in J_i \cap J_j$, we have that $(c_j)_a = y_a = (c_i)_a$. Thus, the above expression does indeed equal zero. Therefore, $Mv = 0$.

Thus, M lacks full column rank. \square

As a result of this lemma, [ST20] formulated the following conjecture whose resolution also implies that generic Reed-Solomon codes reach list-decoding capacity.

Conjecture A.2 (Conjecture 5.7 of [ST20]–restated). *Let $J_1, \dots, J_t \subseteq [n]$ be such that for all $S \subseteq [t]$,*

$$\sum_{i \in S} |J_i| - \left| \bigcup_{i \in S} J_i \right| \leq (|S| - 1)k, \quad (20)$$

and further that (20) is an equality when $S = [t]$. Let G be a generic (n, k) -Vandermonde matrix. Then, $M_{G, (J_1, \dots, J_t)}$ has full column rank.

We now prove this conjecture.

Proof. Note that $M_{G, (J_1, \dots, J_t)}$ only includes entries from the i th column of G if $i \in J_j$ for some $j \in [t]$. Thus, we may assume without loss of generality that

$$\bigcup_{i \in [t]} J_i = [n] \quad (21)$$

Assume for sake of contradiction that $M_{G, (J_1, \dots, J_t)}$ lacks full column rank. Thus, there exists nonzero $v \in \mathbb{F}^{\binom{t}{2}k}$ such that $Mv = 0$. For each $i < j \in [n]$, let $f_{ij} \in \mathbb{F}^k$ be the block of v corresponding to (i, j) . Further, define $f_t = 0$ and $f_i = -f_{it}$ for all $i \in [t-1]$. We claim that for all $i < j \in [n]$ that $f_{ij} = f_j - f_i$. This is by definition when $j = t$. Otherwise, if $j < t$, then by the type (a) rows of M , we may deduce that $f_{ij} - f_{it} + f_{jt} = 0$, which implies that $f_{ij} = f_j - f_i$.

For all $i \in [t]$, define $c_i = G_{J_i \cap J_j}^\top f_i$. Since $v \neq 0$, we know that $f_{ij} \neq 0$ for some $i < j$. Thus, for some $i < j$, we have that $c_i < c_j$.

Due to the type (b) rows of M , we can deduce for all $i < j \in [n]$ that $G_{J_i \cap J_j}^\top f_{ij} = 0$, so $G_{J_i \cap J_j}^\top f_i = G_{J_i \cap J_j}^\top f_j$. Therefore, $c_i|_{J_i \cap J_j} = c_j|_{J_i \cap J_j}$.

Let $y \in \mathbb{F}^n$ be a vector such that $y_{J_i} = (c_i)|_{J_i}$ for all i . Note that at least one y must exist because each of the c_i 's are consistent.

For all $i \in [t]$, let $\bar{J}_i = [n] \setminus J_i$ and $u_i = c_i - y$. Note that $\text{supp}(u_i) \subseteq \bar{J}_i$. Let H be the parity-check matrix of C . Then, since $Hc_1 = \dots = Hc_t$, we have that $Hu_1 = \dots = Hu_t$. Thus, the vector $(-u_1, u_2, u_3, \dots, u_t)$ is in the kernel of the following matrix.

$$\begin{pmatrix} H_{\bar{J}_1} & H_{\bar{J}_2} & & & \\ H_{\bar{J}_1} & & H_{\bar{J}_3} & & \\ \vdots & & & \ddots & \\ H_{\bar{J}_1} & & & & H_{\bar{J}_t} \end{pmatrix}$$

Since the c_i 's are not all equal, the u_i 's are not all 0. Therefore, we have that $H_{\bar{J}_1} \cap \dots \cap H_{\bar{J}_t} \neq 0$.

Observe that by (20) we have that for any nonempty $S \subseteq [t]$, we have that

$$\begin{aligned} \left| \bigcap_{i \in S} \bar{J}_i \right| &= n - \left| \bigcup_{i \in S} J_i \right| \\ &\leq n + (|S| - 1)k - \sum_{i \in S} |J_i| \\ &= \sum_{i \in S} |\bar{J}_i| - (|S| - 1)(n - k), \end{aligned}$$

with equality when $S = [t]$. Thus, for any partition $P_1 \sqcup P_2 \sqcup \dots \sqcup P_s = [t]$, we have that

$$\begin{aligned} \sum_{i=1}^s \left| \bigcap_{j \in P_i} \bar{J}_j \right| &\leq \sum_{i \in [t]} |\bar{J}_i| - \sum_{i=1}^s (|P_i| - 1)(n - k) \\ &= \left| \bigcap_{i \in [t]} \bar{J}_i \right| + (t - 1)(n - k) - (t - s)(n - k) \\ &= n - \left| \bigcup_{i \in [t]} J_i \right| + (s - 1)(n - k) \\ &= (s - 1)(n - k), \end{aligned}$$

The last equality follows from our WLOG assumption (21). Therefore, by Theorem 1.15 the generic intersection dimension of $\bar{J}_1, \dots, \bar{J}_t$ is zero. By Proposition 4.4 and Corollary 1.14, the dual of a generic Reed-Solomon code is MDS(t). Thus, $H_{\bar{J}_1} \cap \dots \cap H_{\bar{J}_t} = 0$, a contradiction. \square

B An alternative algorithm for computing generic intersection dimension in polynomial time

In this appendix, we present an alternative polynomial-time algorithm for computing the generic intersection dimension of a family of sets. Let $A_1, \dots, A_\ell \subseteq [n]$ be sets of size at most k . Consider the following linear program:

Primal LP

$$\begin{aligned}
& \textbf{minimize:} && k - \sum_{i=1}^{\ell} \delta_i \\
& \textbf{subject to:} && \forall i \in [\ell], && \delta_i \geq 0 \\
& && \forall I \subseteq [\ell] \ (I \neq \emptyset), && \sum_{i \in I} \delta_i \leq k - |A_I|.
\end{aligned}$$

By Theorem 1.15 and Lemma 2.8, we know that the optimal *integral* solution to this linear program is equal to the generic intersection dimension of A_1, \dots, A_ℓ . In fact, we shall prove that the optimal “fractional” has the same objective value.

Lemma B.1. *The objective value of the Primal LP is equal to the k -dimensional generic intersection dimension of A_1, \dots, A_ℓ .*

Even with this observation, it is not obvious that the Primal LP can be solved in $\text{poly}(n, k, \ell)$ time, as there are roughly 2^ℓ constraints. However, we shall demonstrate the Primal LP can still be solved efficiently.

Lemma B.2. *One can solve the Primal LP in $\text{poly}(n, k, \ell)$ time.*

As a result of these two lemmas, we get the following corollary.

Corollary B.3. *Given sets $A_1, \dots, A_\ell \subseteq [n]$ of size at most k as input, one can compute the k -dimensional generic intersection dimension of these sets in $\text{poly}(n, k, \ell)$ time.*

We note that while this is the same result as that proved in Section 5, the proof methods are very different and seem to highlight different structural aspects of generic intersections.

The remainder of this appendix is devoted to proving the two lemmas.

B.1 Proof of Lemma B.1

By the theory of LP duality, the objective value of the Primal LP is equal to the objective value of the Dual LP.

Dual LP

$$\begin{aligned}
& \textbf{maximize:} && k - \sum_{\substack{I \subseteq [\ell] \\ I \neq \emptyset}} (k - |A_I|) \mu_I \\
& \textbf{subject to:} && \forall I \subseteq [\ell] \ (I \neq \emptyset), && \mu_I \geq 0 \\
& && \forall i \in [\ell], && \sum_{\substack{I \subseteq [\ell] \\ i \in I}} \mu_I \geq 1.
\end{aligned}$$

By Theorem 1.15 and Lemma 2.8, we have that there exists a partition $P_1 \sqcup \dots \sqcup P_s = [\ell]$ such that

$$\sum_{j=1}^s |A_{P_j}| = (s-1)k + d,$$

where d is the generic intersection dimension. Consider the following assignment to the Dual LP: $\mu_{P_j} = 1$ for all $j \in [s]$ and $\mu_S = 0$ otherwise. Note that since each $i \in [\ell]$ is a member of (at least) one of the P_j 's, we have that this assignment is feasible for the Dual LP. The objective value is then

$$k - \sum_{j=1}^s (k - |A_{P_j}|) = \sum_{j=1}^s |A_{P_j}| - (s-1)k = d.$$

Thus, by duality, the objective value of the Primal LP is at least the generic intersection dimension d . Since we previously mentioned that this value d is attainable by an integral assignment (via Lemma 2.8), we have that the objective value of the Primal LP (and the Dual LP) is exactly the generic intersection dimension.

B.2 Proof of Lemma B.2

To solve the Primal LP, it suffices to implement an efficient (i.e., in $\text{poly}(n, k, \ell)$ time) separation oracle (c.f., [GLS93]). In particular, given nonnegative $\delta_1, \dots, \delta_\ell \in \mathbb{Q}$, we need to efficiently compute that either (1) the δ 's satisfy the primal LP or (2) exhibit a nonempty $I \subseteq [\ell]$ for which $\sum_{i \in I} \delta_i > k - |A_I|$.

Consider the function $f : 2^{[\ell]} \rightarrow \mathbb{Q}$ defined by

$$f(I) = k - |A_I| - \sum_{i \in I} \delta_i.$$

with $f(\emptyset) = 0$. Observe that computing the separation oracle is thus equivalent to either verifying that f is nonnegative or exhibiting an $I \subseteq [\ell]$ such that $f(I) < 0$.

It is straightforward to verify that f is *submodular*, that is for all $I, J \subseteq [\ell]$,

$$f(I) + f(J) \geq f(I \cup J) + f(I \cap J).$$

Minimizing such a function can be done in $\text{poly}(\ell)$ queries to f (c.f., [GLS93]), and thus we can efficiently determine whether there exist $I \subseteq [\ell]$ such that $f(I) < 0$ (note that such an I must be nonempty). Therefore, the Primal LP can be solved efficiently.