Improved Field Size Bounds for Higher Order MDS Codes

Joshua Brakensiek* Manik Dhar† Sivakanth Gopi‡

Abstract

Higher order MDS codes are an interesting generalization of MDS codes recently introduced by Brakensiek, Gopi and Makam (IEEE Trans. Inf. Theory 2022). In later works, they were shown to be intimately connected to optimally list-decodable codes and maximally recoverable tensor codes. Therefore (explicit) constructions of higher order MDS codes over small fields is an important open problem. Higher order MDS codes are denoted by MDS(ℓ) where ℓ denotes the order of generality, MDS(2) codes are equivalent to the usual MDS codes. The best prior lower bound on the field size of an (n, k)-MDS(ℓ) codes is $\Omega_\ell(n^{\ell-1})$, whereas the best known (non-explicit) upper bound is $O_\ell(n^{k(\ell-1)})$ which is exponential in the dimension.

In this work, we nearly close this exponential gap between upper and lower bounds. We show that an (n, k)-MDS(3) codes requires a field of size $\Omega_k(n^{k-1})$, which is close to the known upper bound. Using the connection between higher order MDS codes and optimally list-decodable codes, we show that even for a list size of 2, a code which meets the optimal list-decoding Singleton bound requires exponential field size; this resolves an open question from Shangguan and Tamo (STOC 2020).

We also give explicit constructions of (n, k)-MDS(ℓ) code over fields of size $n^{(\ell k)^{O(\ell k)}}$. The smallest non-trivial case where we still do not have optimal constructions is $(n, 3)$-MDS(3). In this case, the known lower bound on the field size is $\Omega(n^2)$ and the best known upper bounds are $O(n^5)$ for a non-explicit construction and $O(n^{32})$ for an explicit construction. In this paper, we give an explicit construction over fields of size $O(n^3)$ which comes very close to being optimal.

*Stanford University. Email: jbrakens@cs.stanford.edu

†Department of Computer Science, Princeton University. Email: manikd@princeton.edu. Part of this work was done while this author was interning at Microsoft Research. Research supported by NSF grant DMS-1953807.

‡Microsoft Research. Email: sigopi@microsoft.com

Contents

1 Introduction

The Singleton bounds states that the minimum distance of an (n, k)-code is at most $n - k + 1$ [Sin64].[1] Codes which achieve this bound are called Maximum Distance Separable (MDS) codes. Reed-Solomon codes are a beautiful construction of MDS codes over fields of size just $O(n)$. Field size plays an important role in several applications of MDS codes. In distributed storage where MDS codes are extensively used, field size is the main determinant in the efficiency of encoding the data and recovering from failures [HSX+12, PGM13]. Because of their distance optimality (MDS) and the small field size, Reed-Solomon codes are one of the most widely used codes both in practice and in theory.

In a recent paper,[2] [BGM22b] introduced a generalization of MDS codes called *higher order MDS codes*.

Definition 1.1 (Higher order MDS codes [BGM22b])**.** For a matrix $V \in \mathbb{F}^{k\times n}$ and subset $A \subseteq [n]$, we let V_A be the span of the columns of V indexed by A. 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

$$\dim(G_{A_1} \cap \cdots \cap G_{A_\ell}) = \dim(W_{A_1} \cap \cdots \cap W_{A_\ell}), \tag{1}$$

where $W_{k\times n}$ is a generic matrix over the same field characteristic.[3]

For example, the columns of a generator matrix of an $(n, 3)$-MDS(3) code form n points in the projective plane $\mathbb{PF}^2$ such that no three points are collinear and additionally, no three lines obtained by joining disjoint pairs of points are concurrent. This is in contrast to an ordinary $(n, 3)$-MDS code where we only require that no three points are collinear.

In [BGM22b], it was shown that higher order MDS codes are equivalent to MR tensor codes which were first introduced in [GHK+17]. A subsequent work [BGM22a] showed that higher order MDS codes are equivalent to optimally list-decodable codes. We look at these two equivalences in turn.

A code C is a (m, n, a, b)-*tensor code* if it can be expressed as $C_{col} \otimes C_{row}$, 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. Such a code C is *maximally recoverable* (abbreviated as MR) 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. [BGM22b] defined MDS(ℓ) codes motivated by the following proposition.

Proposition 1.2 (Higher order MDS codes are equivalent to MR tensor codes [BGM22b])**.** *Let $C = C_{col} \otimes C_{row}$ 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)*.*

A generalization of the Singleton bound was recently proved for list-decoding in [ST20, Rot22, GST21]. If an (n, k)-code is (L, ρ)-list-decodable[4], then

$$\rho \leq \frac{L}{L+1}\left(1 - \frac{k}{n}\right). \tag{2}$$

Note that when $L = 1$, this reduces to the usual Singleton bound. Roth [Rot22] defined a higher order generalization of MDS codes as codes achieving this generalized Singleton bound for average-radius list-decoding.

Definition 1.3 (List-decodable-MDS codes [Rot22])**.** Let C be a (n, k)-code. We say that C is list decodable-MDS(L), denoted as LD-MDS(ℓ), if C is (L, ρ)-average-radius list-decodable for $\rho = \frac{L}{L+1}\left(1 - \frac{k}{n}\right)$.

[1] This bound holds for non-linear codes as well, but in this paper we will only focus on linear codes defined over some finite field $\mathbb{F}$. A (linear) (n, k)-code over $\mathbb{F}$ is a k-dimensional subspace of $\mathbb{F}^n$.

[2] The timeline presented in this paper is based on the initial arXiv posting dates of each paper. In particular, such chronological order is [BGM22b, Rot22, BGM22a].

[3] Note 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 (1) then MG also satisfies (1) for any $k \times k$ invertible matrix M.

[4] I.e., there are at most L codewords in any Hamming ball of radius ρn.

In other words, for any $y \in \mathbb{F}^n$, there does not exist $L+1$ *distinct* codewords $c_0, c_1, \ldots, c_L \in C$ such that

$$\sum_{i=0}^{L} \mathrm{wt}(c_i - y) \le (L+1)\rho n = L(n-k).$$

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

An equivalent way to define LD-MDS(L) codes is using the parity check matrix $H_{(n-k)\times n}$ matrix of C [Rot22]. C is LD-MDS(L) if there doesn't exist $L+1$ *distinct* vectors $e_0, e_1, \ldots, e_L \in \mathbb{F}^n$ such that

$$\sum_{i=0}^{L} \mathrm{wt}(e_i) \le L(n-k) \text{ and } He_0 = He_1 = \cdots = He_L.$$

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 $L \ge \frac{1-R-\epsilon}{\epsilon}$. Note that the usual MDS codes are LD-MDS(1). [BGM22a] shows the equivalence between LD-MDS codes and the dual of higher order MDS codes.

Proposition 1.4 (LD-MDS codes are the dual of higher order MDS codes [BGM22a])**.** *If C is a linear code then for all $\ell \ge 1$, C is* MDS($\ell+1$) *if and only if $C^\perp$ is* LD-MDS($\le \ell$).

Besides the connection to MR tensor codes and optimally list-decodable codes, higher order MDS codes are also shown to be intimately related to MDS codes whose generator matrices are constrained to have a specific support and the GM-MDS conjecture [BGM22a]. Such matrices have many applications in coding theory, see [DSY14].

1.1 Our Results

Our main result exponentially improves the lower bound for higher order MDS codes.

Theorem 1.5. *Let C be an (n,k)-code over the field $\mathbb{F}$ which is* MDS(3)*. Then, $|\mathbb{F}| \ge \binom{n-2}{k-1} - 1$.*

By Proposition 1.2, we have the following corollary for MR tensor codes.

Corollary 1.6. *Let C be an $(m,n,1,b)$-tensor code over the field $\mathbb{F}$ then $|\mathbb{F}| \ge \binom{n-2}{b-1} - 1$.*

Proposition 1.4, implies the following corollary for LD-MDS codes.

Corollary 1.7. *Let C be an (n,k)-code over the field $\mathbb{F}$ which is* LD-MDS(≤ 2) *then $\mathbb{F} \ge \binom{n-2}{k-1} - 1$*

In particular, we see that if C is of constant rate and LD-MDS(≤ 2) then we would need exponential in n field size. For applications to list decoding, this is only talking about information-theoretically-optimal[5] average-radius list decoding.

To remedy this situation, starting from Theorem 1.5 we prove lower bounds for the worst-case list decoding setting.

Theorem 1.8. *Let $n \ge k \ge 0$ be such that $n-k$ is divisible by 3. Let C be an (n,k)-MDS code which is $(2, \frac{2(n-k)}{3n})$-worst-case list decodable, i.e., it matches the list-decoding Singleton bound (2) for $L=2$. Then, C requires field size $\binom{(n+2k)/3}{k-1} - 1$.*

In particular, this answers an open question from [ST20], where they asked what is the minimum field size necessary to achieve the list-decoding Singleton bound (2) for $L=2$; we show that exponential field size is necessary and sufficient.

Remark 1.9. This lower bound does *not* say that error-correcting codes achieving list decoding capacity require exponential field size (which contradicts the known list decoding capacity of random linear codes [GHK10]). Instead is just says that codes over subexponential fields cannot achieve capacity with the *exactly optimal* list size.

Remark 1.10. Also note that this lower bound only applies to MDS codes, as non-MDS codes already have a suboptimal tradeoff for list-size 1.

[5]Here we mean that the tradeoff between list decoding radius and list size is *exactly* as specified by the generalized Singleton bound.

1.1.1 Explicit constructions

Our first explicit construction is a general construction for $(n, k) - \mathrm{MDS}(\ell)$ codes field size construction. Prior to this work no constructions for general values of n, k, and l were known.

Theorem 1.11. *There is an explicit (n, k)-MDS(ℓ)-code over field size $n^{(\ell k)^{O(\ell k)}}$.*

We now give a high level overview of our construction. We first convert the generic intersection condition (1) into a determinant condition using Lemma 2.3. Let $p \geq n + k - 1$ be a prime power and consider the field extension $\mathbb{F}_p[\alpha_1, \ldots, \alpha_{k\ell}]$ over the base field $\mathbb{F}_p$ where each α_i has an extension degree $D = \ell k^2$ over $\mathbb{F}_p[\alpha_1, \ldots, \alpha_{i-1}]$. In particular, this means that any non-zero polynomial $p(x_1, x_2, \ldots, x_{\ell k})$ with $\mathbb{F}_p$ coefficients and individual degree at most $D-1$, cannot vanish at $(\alpha_1, \alpha_2, \ldots, \alpha_{\ell k})$. Similar ideas were also used in the doubly exponential MDS(3) construction of [Rot22, ST20].

But here, we depart from previous constructions. Our (n, k)-MDS(ℓ) code C is the Reed-Solomon code generated by n $\mathbb{F}_p$-linear combinations of $\alpha_1, \ldots, \alpha_{k\ell}$ such that any ℓk generators are linearly independent over $\mathbb{F}_p$, this can be achieved using a Reed-Solomon code over $\mathbb{F}_p$. The key step is then to show that the determinant obtained from Lemma 2.3 is a non-zero polynomial in $\alpha_1, \alpha_2, \ldots, \alpha_{\ell k}$ (it is easy to see that its individual degree is at most $D - 1$). Here we crucially use the GM-MDS theorem [Lov18, YH19] (which requires $p \geq n + k - 1$) and the $\mathbb{F}_p$ linear independence of our evaluation points to show that there is an $\mathbb{F}_p$ substitution to $\alpha_1, \ldots, \alpha_{\ell k}$ which makes the determinant non-zero. This shows that the determinant polynomial is indeed non-zero.

Our next construction is in the specific case of $(n, 3)$-MDS(3) codes which is the smallest non-trivial case of a higher-order MDS code.

Theorem 1.12. *There exists an explicit $(n, 3)$-MDS(3) code with field size $O(n^3)$.*

This improves on the earlier explicit construction of size $O(n^{32})$ [Rot22] and is only a factor n away from the current best lower bound of $\Omega(n^2)$ [BGM22b]. We also construct some explicit codes for $k = 4$ and $k = 5$.

Theorem 1.13. *There exists an explicit $(n, 4)$-MDS(3) code with field size $O(n^7)$.*

Theorem 1.14. *There exists an explicit $(n, 5)$-MDS(3) code with field size $O(n^{50})$.*

As the dual of MDS(3) is also MDS(3) [Rot22, BGM22b], the three constructions above also give us constructions for $(n, n-k)$-MDS(3) for $k = 3, 4, 5$. The above constructions involve carefully analyzing the algebraic conditions Reed-Solomon codes need to satisfy to have the higher order MDS property and carefully selecting the evaluation points so that we can argue for their correctness directly or in some cases reduce to a simple check which can be performed by a computer program.

1.2 Comparison with prior work

Tables 1 and 2 show known upper and lower bounds on the field size of MDS(ℓ) codes and compare it our work. Since the dual of MDS(3) is also MDS(3) [Rot22, BGM22b] any (n, k)-MDS(3) construction in the Table 1 also gives a $(n, n-k)$-MDS(3) construction as well. As can be seen from Table 1, prior to our work no general explicit constructions were known. We also see that even after our work there is an exponential gap in the exponent of the field size between the explicit and non-explicit constructions.

Noting, that any (n, k)-MDS(ℓ) code is also MDS(ℓ'), $\ell' \leq \ell$ we see that our lower bound is an exponential improvement over the earlier best known lower bounds (say when code rate is constant and ℓ is constant).

1.3 Open Questions

We conclude the introduction with the following intriguing open questions. First, we would like to close the gap between the existential upper and lower bounds for MDS(ℓ) codes.

Question 1.15. *Can we match the existential upper and lower bounds for (n, k)-MDS(ℓ) for $\ell \geq 3$? In particular, can we improve the current lower bound from $\Omega_k(n^k)$ to $\Omega_{\ell,k}(n^{\Omega(\ell k)})$?*

Second, we would like to close the gap between the existential upper bounds and explicit constructions.

Question 1.16. *Can we construct explicit (n, k)-MDS(ℓ) codes with field size $O_{\ell,k}(n^{(\ell-1)k})$?*

Finally, we would like to get a truly optimal construction in the $(n, 3)$-MDS(3) case.

(n,k)-MDS(3)	2^{k^n}	explicit	[ST20]
(n,k)-MDS(4)	$2^{(3k)^n}$	explicit	[ST20]
(n,k)-MDS(3)	$n^{k^{2k}}$	explicit	[Rot22]
(n,k)-MDS(ℓ)	$n^{O(\min\{k,n-k\}(\ell-1))}$	non-explicit	[BGM22b, KMG21, BGM22a]
(n,k)-MDS(ℓ)	$n^{(lk)^{O(lk)}}$	explicit	Theorem 1.11
$(n,3)$-MDS(3)	n^{32}	explicit	[Rot22]
$(n,3)$-MDS(3)	n^{5}	non-explicit	[Rot22]
$(n,3)$-MDS(3)	n^{3}	explicit	Theorem 1.12
$(n,4)$-MDS(3)	n^{7}	explicit	Theorem 1.13
$(n,5)$-MDS(3)	n^{50}	explicit	Theorem 1.13

Table 1: Table showing the best known upper bounds for the field size of (n,k)-MDS(ℓ) codes.

$(n,n-2)$-MDS(4)	$\Omega(n^2)$	[KMG21]
(n,k)-MDS(ℓ)	$\Omega_{\ell,k}(n^{\min\{\ell,k,n-k\}-1})$	[BGM22b]
(n,k)-MDS(3)	$\binom{n-2}{k-1}-1$	Theorem 1.5

Table 2: Table showing the best known lower bounds for the field size of (n,k)-MDS(ℓ) codes.

Question 1.17. *Do there exist $(n,3)$-MDS(3) codes over fields of size $O(n^2)$?*

Because of the rich connections of higher order MDS codes, progress on any of these questions, particularly the constructions of explicit codes, will lead to new insights and applications for distributed storage and list decoding.

2 Preliminaries

In this section, we state a couple of definitions and known theorems about higher order MDS codes which will be useful for us.

An (n,k)-Reed-Solomon code with *generators* $\alpha_1,\dots,\alpha_n \in \mathbb{F}$ is the code with the following generating matrix:

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

We now discuss properties of general higher order MDS codes.

Theorem 2.1 ([BGM22b])**.** *Let V be a $k\times n$ matrix. Then, V is (n,k)-MDS(ℓ) if and only if for all $A_1,\dots,A_\ell \subseteq [n]$ with $|A_i|\le k$ and $|A_1|+\cdots+|A_\ell| = (\ell-1)k$, we have that $V_{A_1}\cap\cdots\cap V_{A_\ell} = 0$ whenever it generically should; that is, for all partitions $P_1\cup\cdots\cup P_s = [\ell]$ we have that*

$$\sum_{i=1}^{s}\left|\bigcap_{j\in P_i} A_j\right| \le (s-1)k.$$

We shall need the following simple corollary for MDS(3).

Corollary 2.2. *Let V be a $k \times n$ MDS matrix. Then, V is (n,k)-MDS(3) if and only if for all $A_1, A_2, A_3 \subseteq [n]$ with $|A_i| \le k-1$ and $|A_1| + |A_2| + |A_3| = 2k$, we have that $V_{A_1} \cap V_{A_2} \cap V_{A_3} = 0$ whenever it generically should; that is, the following conditions hold:*

- $|A_1 \cap A_2 \cap A_3| = 0$.
- $|A_{\pi(1)} \cap A_{\pi(2)}| + |A_{\pi(3)}| \le k$ *for all permutations* $\pi : [3] \to [3]$.

Proof. Note that the combinatorial conditions on the sets A_1, A_2, A_3 follow by considering suitable partitions of [3]. By Theorem 2.1, it suffices to check the intersection $V_{A_1} \cap V_{A_2} \cap V_{A_3}$ when one of the A_i's has size exactly k. Assume without loss of generality that $|A_3| = k$. Then $V_{A_3} = \mathbb{F}^k$, so the intersection is equal to $V_{A_1} \cap V_{A_2}$. Since V is MDS, V is also MDS(2) (see [BGM22b]), so this intersection is 0 if and only if it generically should. ☐

We shall also use the following matrix identity for checking MDS(ℓ) conditions.

Lemma 2.3 ([Tia19, BGM22b])**.** *Let V be a $k \times n$ matrix. Consider $A_1, \dots, A_\ell \subseteq [n]$ with $|A_i| \le k$ and $|A_1| + \cdots + |A_\ell| = (\ell-1)k$, we have that $V_{A_1} \cap \cdots \cap V_{A_\ell} = 0$ if and only if*

$$\det \begin{pmatrix} I_k & V_{A_1} & & & \\ I_k & & V_{A_2} & & \\ \vdots & & & \ddots & \\ I_k & & & & V_{A_k} \end{pmatrix} \neq 0,$$

where V_{A_i} denotes the submatrix of V with columns indexed by A_i.

The following is useful for constructing Reed-Solomon codes over $(n,3)$-MDS(3).

Lemma 2.4 ([BGM22b, Rot22])**.** *Let V be an $(n,3)$-Reed-Solomon code with evaluation points $\beta_1, \dots, \beta_n \in \mathbb{F}$. Then, V is MDS(3) if and only if for all injective maps $\alpha : [6] \to [n]$ we have that*

$$\det \begin{pmatrix} 1 & \beta_{\alpha(1)} + \beta_{\alpha(2)} & \beta_{\alpha(1)}\beta_{\alpha(2)} \\ 1 & \beta_{\alpha(3)} + \beta_{\alpha(4)} & \beta_{\alpha(3)}\beta_{\alpha(4)} \\ 1 & \beta_{\alpha(5)} + \beta_{\alpha(6)} & \beta_{\alpha(5)}\beta_{\alpha(6)} \end{pmatrix} \neq 0.$$

We shall also use a variant of the GM-MDS theorem.

Theorem 2.5 (GM-MDS theorem,[DSY14, Lov18, YH19], see [BGM22a])**.** *Let $A_1, \dots, A_\ell$ of total size $(\ell-1)k$ such that $W_{A_1} \cap \cdots \cap W_{A_\ell} = 0$ for a generic (n,k)-matrix. Let $\mathbb{F}$ be a field of size at least $n+k-1$. Then, there exists $\gamma_1, \gamma_2, \dots, \gamma_n \in \mathbb{F}$ such that the (n,k) Reed-Solomon code U generated by $\gamma_1, \dots, \gamma_n$ has that $U_{A_1} \cap \cdots \cap U_{A_\ell} = 0$.*

Remark 2.6. Note the order of the quantifiers. The code U is only guaranteed to meet the MDS(ℓ) criteria for one tuple of sets $(A_1, \dots, A_\ell)$.

3 (n,k)-MDS(3) codes require field size $\binom{n-2}{k-1} - 1$

In this section, we show the exponential (in dimension) lower bound for the field size of MDS(3) codes.

Theorem 1.5. *Let $V \in \mathbb{F}^{k \times n}$ be an MDS(3)-code. Then, $|\mathbb{F}| \ge \binom{n-2}{k-1} - 1$.*

We prove this by in fact showing a slightly stronger lower bound.

Lemma 3.1. *Let $V \in \mathbb{F}^{k \times n}$ be an MDS code such that $V_{A_1} \cap V_{A_2} \cap V_{A_3} = 0$ for all $A_1, A_2, A_3 \subseteq [n]$ with distinct A_2, A_3, $|A_1| = 2, |A_2| = |A_3| = k-1$ and $A_1 \cap (A_2 \cup A_3) = \emptyset$. Then, $|\mathbb{F}| \ge \binom{n-2}{k-1} - 1$.*

Proof of Theorem 1.5. By Corollary 2.2, if $A_2 \neq A_3$, $|A_1| = 2, |A_2| = |A_3| = k-1$ and $A_1 \cap (A_2 \cup A_3) = \emptyset$ then $V_{A_1} \cap V_{A_2} \cap V_{A_3} = 0$ when V is MDS(3). The rest follows from Lemma 3.1. ☐

Proof of Lemma 3.1. Let $e_1, e_2, \ldots, e_k$ be the coordinate vectors in $\mathbb{F}^k$. Via row operations, we may assume that $V_1 = e_1$ and $V_2 = e_2$. Now consider the MDS(3) test on $A_1 = \{1, 2\}$ and two distinct subsets A_2, A_3 of size $k-1$ which are disjoint from A_1 (but not necessarily from each other). By Corollary 2.2, we have that $V_{A_1} \cap V_{A_2} \cap V_{A_3} = 0$.

Note that for any subset $A \subseteq [n]$ of size $k-1$, $V_A^\perp$ is a 1-dimensional space with coordinates $(w_1^A, \ldots, w_k^A)$, where $w_i^A = (-1)^i \det(V|_{A \times ([k] \setminus i)})$. Also $V_{A_1}^\perp = \operatorname{span}\{e_3, e_4, \ldots, e_k\}$. Finally $V_{A_1} \cap V_{A_2} \cap V_{A_3} = 0$ iff $V_{A_1}^\perp + V_{A_2}^\perp + V_{A_3}^\perp = \mathbb{F}^k$. Therefore, we have that the MDS(3) condition on A_1, A_2, A_3 is equivalent to

$$\det \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & w_1^{A_2} & w_1^{A_3} \\ 0 & 0 & \cdots & 0 & 0 & w_2^{A_2} & w_2^{A_3} \\ 1 & 0 & \cdots & 0 & 0 & w_3^{A_2} & w_3^{A_3} \\ 0 & 1 & \cdots & 0 & 0 & w_4^{A_2} & w_4^{A_3} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & w_{k-1}^{A_2} & w_{k-1}^{A_3} \\ 0 & 0 & \cdots & 0 & 1 & w_k^{A_2} & w_k^{A_3}. \end{pmatrix} = \det \begin{pmatrix} w_1^{A_2} & w_1^{A_3} \\ w_2^{A_2} & w_2^{A_3} \end{pmatrix} \neq 0.$$

In other words, $(w_1^{A_2} : w_2^{A_2}) \neq (w_1^{A_3} : w_2^{A_3})$ in $\mathbb{PF}^1$ whenever $A_2, A_3 \subseteq \{3, \ldots, n\}$ are distinct subsets of size $k-2$. Thus, $q \geq \binom{n-2}{k-1} - 1$. $\square$

This result greatly improves on the previous lower bounds for MR tensor codes.

Corollary 3.2. *Let $U \otimes V$ be an (m, n, a, b) MR tensor code with $a \geq 1$ and $m - a \geq 2$. Then the field size must be at least $\binom{n-2}{b-1} - 1$.*

Proof. Let U' be a $(m - a + 1, m - a)$ code formed by puncturing U. Note that $U' \otimes V$ must be an $(m - a + 1, n, 1, b)$ MR tensor code. Thus, V must be an MDS$(m - a + 1)$ code [BGM22b]. Since $m - a + 1 \geq 3$, we have that V is an MDS(3) code. Thus, the field size lower bound of $\binom{n-2}{(n-b)-1} - 1 = \binom{n-2}{b-1} - 1$ applies. $\square$

3.1 Application to list decoding

As mentioned previously the lower bound of Theorem 1.5 is only about average-radius list decoding. Furthermore, the "hard" case identified is a rather extreme example, where one of the codewords has Hamming distance $n - k - 2$ from the received codeword, which is only three less than the minimum distance.

In this section we prove a lower bound for the worst-case list decoding setting by proving Theorem 1.8.

Theorem 1.8. *Let $n \geq k \geq 0$ be such that $n - k$ is divisible by 3. Let C be an (n, k)-MDS code which is $(2, \frac{2(n-k)}{3n})$ worst-case list decodable. Then, C requires field size $\binom{n-2(n-k)/3}{k-1} - 1$.*

To start, we show that the MDS(3) lower bound extends to the case the sets A_1, A_2, A_3 are all the same size.

Lemma 3.3 (Extension to the $(2k/3, 2k/3, 2k/3)$ split.)**.** *Let k be divisible by 3. Let V be an (n, k)-MDS code such that for all $A_1, A_2, A_3 \subseteq [n]$ of size $2k/3$ we have that $V_{A_1} \cap V_{A_2} \cap V_{A_3} = 0$ whenever this holds generically. Then, the field size of the code is at least $\binom{n-2k/3}{k/3+1} - 1$.*

Proof. Let V be an MDS(3) code such that $V_{A_1} \cap V_{A_2} \cap V_{A_3} = 0$ whenever $|A_1| = |A_2| = |A_3| = 2k/3$ and generically the intersection should be 0. By Corollary 2.2, this is equivalent to $|A_1 \cap A_2 \cap A_3| = 0$ and $|A_i \cap A_j| \leq k/3$ for all $i \neq j$.

Pick $2k/3 - 2$ columns $I \subseteq [n]$ of V. Let $k' = k - |I| = k/3 + 2$ Pick an arbitrary projection $\Pi : \mathbb{F}^k \to \mathbb{F}^{k'}$ of rank k' such that $\ker(\Pi) = V_I$. Let V' be the code with columns $\Pi(v_i)$ for $i \in [n] \setminus I$.

Claim 3.4. *V' is MDS.*

Proof. Pick any set of indices J of size k' disjoint from I, it suffices to prove that $V'_I = \mathbb{F}^{k'}$. Note that

$$\begin{aligned} V'_I &= \operatorname{span}\{\Pi(v_i) : i \in J\} \\ &= \operatorname{span}\{\Pi(v_i) : i \in I \cup J\} \\ &= \Pi(\operatorname{span}\{v_i : i \in I \cup J\}) \\ &= \Pi(\mathbb{F}^k) && (V \text{ MDS}) \\ &= \mathbb{F}^{k'} && (\Pi \text{ max rank}), \end{aligned}$$

as desired. □

To complete the field size lower bound, consider distinct $A'_1, A'_2, A'_3 \subseteq [n] \setminus I$ such that $|A'_1| = 2$, $|A'_2| = |A'_3| = k' - 1 = k/3 + 1$, and $A'_1 \cap (A'_2 \cup A'_3) = 0$. By Lemma 3.1, it suffices to show that $V'_{A'_1} \cap V'_{A'_2} \cap V'_{A'_3} = 0$. Assume for sake of contradiction that there exists nonzero $v_0 \in V'_{A'_1} \cap V'_{A'_2} \cap V'_{A'_3}$. Pick an arbitrary partition $I_2 \cup I_3 = I$ such that $|I_2| = |I_3| = k/3 - 1$. Now let

$$\begin{aligned} A_1 &= I \cup A'_1 \\ A_2 &= I_2 \cup A'_2 \\ A_3 &= I_3 \cup A'_3. \end{aligned}$$

Note that $|A_1| = |A_2| = |A_3| = 2k/3$ and $|A_1 \cap A_2 \cap A_3| = 0$. Further, we can check that

$$\begin{aligned} |A_1 \cap A_2| + |A_3| &= |I_2| + |A_3| = k/3 - 1 + 2k/3 \le k, \\ |A_1 \cap A_3| + |A_2| &= |I_3| + |A_2| = k/3 - 1 + 2k/3 \le k, \\ |A_2 \cap A_3| + |A_1| &= |A'_2 \cap A'_3| + |A_1| \le k/3 + 2k/3 \le k. \end{aligned}$$

Thus, by Corollary 2.2, we know that $V_{A_1} \cap V_{A_2} \cap V_{A_3} = 0$.

Let $W = \Pi^{-1}(\operatorname{span}(v_0))$ (recall that $v_0 \in V'_{A'_1} \cap V'_{A'_2} \cap V'_{A'_3}$). Note that $\dim(W) = k - k' + 1 = 2k/3 - 1$. Since $\operatorname{span}(v_0) \in V'_{A'_1}$, we have that

$$W = \Pi^{-1}(\operatorname{span}(v_0)) \subseteq \Pi^{-1}(V'_{A'_1}) = V_I + V_{A'_1} = V_{A_1}.$$

Also observe that since $v_0 \in V'_{A'_2} = \Pi(V_{A_2})$, there exists $w_0 \in V_{A_2}$ such that $\Pi(w_0) = v_0$. Thus, $w_0 \in W$, too, so $v_0 \in \Pi(W \cap V_{A_2})$. Further, let Π_2 be the map Π but restricted to the domain $W \cap V_{A_2}$. Observe that by the rank-nullity theorem

$$\begin{aligned} \dim(W \cap V_{A_2}) &= \dim \ker \Pi_2 + \dim(\Pi(W \cap V_{A_2})) \\ &\ge \dim V_{I_2} + \dim \operatorname{span}(v_0) \\ &= |I_2| + 1. \end{aligned}$$

Likewise, $\dim(W \cap V_{A_3}) \ge |I_3| + 1$. Thus,

$$\begin{aligned} \dim(V_{A_1} \cap V_{A_2} \cap V_{A_3}) &\ge \dim(W \cap V_{A_2} \cap V_{A_3}) \\ &= \dim((W \cap V_{A_2}) \cap (W \cap V_{A_3})) \\ &\ge \dim(W \cap V_{A_2}) + \dim(W \cap V_{A_3}) - \dim(W) \\ &\ge |I_2| + 1 + |I_3| + 1 - |W| \\ &= 1, \end{aligned}$$

a contradiction. Therefore, by Lemma 3.1 we get a lower bound of

$$q \ge \binom{n - 2k/3}{k/3 + 1} - 1.$$ □

We are now ready to prove Theorem 1.8.

Proof of Theorem 1.8. We adapt the proof of Proposition 4.1 in [BGM22a]. Let H be the parity check matrix of C (i.e., the generator matrix of $C^{\perp}$). If H has the property that for all $A_1, A_2, A_3 \subseteq [n]$ of size $\frac{2}{3}(n-k)$ we have that $H_{A_1} \cap H_{A_2} \cap H_{A_3} = 0$ when it generically should, then the desired field size lower bound holds by Lemma 3.3.

Otherwise, there exists A_1, A_2, A_3 of size $\frac{2}{3}(n-k)$ such that $H_{A_1} \cap H_{A_2} \cap H_{A_3} \neq 0$ even though the generic intersection is 0. Let v_0 be a nonzero vector in this common intersection. By definition, for each $i \in [3]$ there exists a nonzero $e_i \in \mathbb{F}^n$ such that $v_0 = He_i$ and $\operatorname{supp}(e_i) \subseteq A_i$.

If e_1, e_2, e_3 are all distinct, then we have violated that C is $(2, \frac{2(n-k)}{3n})$ worst-case list decodable (see equation 17 of [BGM22a]). If $e_1 = e_2 = e_3$, then $A_1 \cap A_2 \cap A_3 \neq 0$ which contradicts Corollary 2.2. Otherwise, if say WLOG $e_1 = e_2 \neq e_3$, then $\operatorname{supp}(e_1), \operatorname{supp}(e_2) \subset A_1 \cap A_2$. So, by Corollary 2.2,

$$|\operatorname{supp}(e_1 - e_3)| \leq |A_1 \cap A_2| + |A_3| \leq k.$$

However $H(e_1 - e_3) = 0$, so C cannot be MDS. □

4 Doubly-exponential construction of higher-order MDS codes

In [ST20] (c.f., Theorem 1.7), the authors give a doubly-exponential explicit construction of higher order MDS codes. In particular, they construct MDS(3) codes which have field size 2^{k^n} and MDS(4) codes which have field size $2^{(3k)^n}$, although their method can adapted to MDS(ℓ) codes (see their remark after Theorem 1.9). In [Rot22], Roth improves this construction to $n^{k^{O(k)}}$ for MDS(3) codes.

Remark 4.1. We also note that a straightforward construction can be obtained by using ideas from [BGM22a] and [ST20]. For a $k \times n$ matrix V, using the equivalence of $V_{A_1} \cap \ldots \cap V_{A_\ell} = 0$ with $V_{A_1}^{\perp} + \ldots + V_{A_\ell}^{\perp} = \mathbb{F}_q^k$, we can write down a determinantal matrix identity which for Reed-Solomon codes only has individual degree at most $k-1$ in the evaluation points [BGM22a]. This will give us a general (n,k)-MDS(ℓ) construction over fields of size 2^{k^n} by working over the field $\mathbb{F}_2(x_1, \ldots, x_n)$ where x_i has degree k over $\mathbb{F}_2(x_1, \ldots, x_{i-1})$, similar to what was done in [ST20].

In the remainder of this section, we construct MDS(ℓ) codes for all $\ell \geq 4$ with field sizes comparable to Roth's.

Theorem 1.11. *There is an explicit* (n,k)*-MDS(*ℓ*)-code over field size* $n^{(\ell k)^{O(\ell k)}}$.

The proof incorporates ideas from both Shangguan-Tamo [ST20] and Roth [Rot22].

Proof. Pick F_0 to be a finite field of size at least $n+k-1$. For $i \in [\ell k]$, let F_i be a degree ℓk^2 extension of F_{i-1} via generator α_i. Let $\mathbb{F} = F_{\ell k}$. Note that $|\mathbb{F}| = n^{(\ell k)^{O(\ell k)}}$. Pick distinct $\beta_1, \ldots, \beta_n \in F_0$. For all $i \in [n]$, define the multivariate polynomial

$$p_i(x_1, \ldots, x_{\ell k}) = \sum_{j=1}^{\ell k} \beta_i^{j-1} x_j.$$

Let V be the (n,k)-Reed-Solomon code with generators $p_i(\alpha_1, \ldots, \alpha_{\ell k})$ for $i \in [n]$. We claim that V is MDS(ℓ). Let $\widetilde{V}$ be an (n,k)-Reed-Solomon code with generators $p_i(x_1, \ldots, x_{\ell k})$, where the base field is $\widetilde{\mathbb{F}} := F_0(x_1, \ldots, x_{\ell k})$ (i.e., F_0 extended by ℓk free generators).

The desired result follows by the following two claims.

Claim 4.2. *V is MDS(ℓ) if and only if $\widetilde{V}$ is MDS(ℓ).*

Proof. To verify, consider $A_1, \ldots, A_\ell$ of total size $(\ell-1)k$ such that $W_{A_1} \cap \cdots \cap W_{A_\ell} = 0$ for a generic (n,k)-matrix. It suffices to check by Lemma 2.3 that

$$\det \begin{pmatrix} I_k & V_{A_1} & & & \\ I_k & & V_{A_2} & & \\ \vdots & & & \ddots & \\ I_k & & & & V_{A_k} \end{pmatrix} \neq 0 \iff \det \begin{pmatrix} I_k & \widetilde{V}_{A_1} & & & \\ I_k & & \widetilde{V}_{A_2} & & \\ \vdots & & & \ddots & \\ I_k & & & & \widetilde{V}_{A_k} \end{pmatrix} \neq 0 \qquad (3)$$

Note that each term in the determinant is the product of at most ℓk expressions of the form p_i^j for $j \le k-1$. Since each α_i is from a degree ℓk^2 extension, we have that the LHS determinant is nonzero in $F_0[\alpha_1, \ldots, \alpha_{\ell k}]$ iff RHS determinant is nonzero in $F_0(x_1, \ldots, x_{\ell k})$. ☐

Claim 4.3. *$\widetilde{V}$ is* MDS(ℓ)*.*

Proof. Again, consider $A_1, \ldots, A_\ell$ of total size $(\ell-1)k$ such that $W_{A_1} \cap \cdots \cap W_{A_\ell} = 0$ for a generic (n,k)-matrix. Since $|F_0| \ge n+k-1$, Theorem 2.5, there exists $\gamma_1, \gamma_2, \ldots, \gamma_k \in F_0$ such that the (n,k) Reed-Solomon code U generated by $\gamma_1, \ldots, \gamma_n$ has that $U_{A_1} \cap \cdots \cap U_{A_\ell} = 0$. Thus, it suffices to prove that there exists an assignment $\pi : \{x_1, \ldots, x_{\ell k}\} \to F_0$ such that

$$\gamma_i = p_i(\pi(x_1), \ldots, \pi(x_{\ell k})).$$

This shows that the RHS of (3) holds. Finding such a π is equivalent to solving the following linear system:

$$\begin{pmatrix} 1 & \beta_1 & \cdots & \beta_1^{\ell k-1} \\ 1 & \beta_2 & \cdots & \beta_2^{\ell k-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \beta_{\ell k} & \cdots & \beta_{\ell k}^{\ell k-1} \end{pmatrix} \begin{pmatrix} \pi(x_1) \\ \pi(x_2) \\ \vdots \\ \pi(x_{\ell k}) \end{pmatrix} = \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_{\ell k} \end{pmatrix}$$

Since the square matrix on the LHS is a Vandermonde matrix, it is invertible, so such a π does indeed exist. ☐

Thus, V is indeed MDS(ℓ). ☐

Remark 4.4. Using techniques, we can also get an explicit construction of $(n, n-b)$-MDS(ℓ) codes over fields of size $n^{\ell b^{O(\ell b)}}$ by adapting the non-constructive upper bound in [BGM22b] (see their Appendix A). In particular, the MDS(ℓ) conditions are equivalent to the maximal recoverability of a suitable tensor code. By looking at the parity check matrix of the tensor code, these recoverability conditions can be expressed as ensuring nonzero determinants of matrices of size at most $(\ell-1)b$. Likewise, one can show the degree of each variables in the determinant is poly(ℓ, b), yielding the stated bound.

5 New explicit constructions for $(n,3)$-MDS(3)

First, we present a hand-verifiable $O(n^4)$ construction for $(n,3)$-MDS(3). After that we present an $O(n^3)$ construction, where a portion of the proof involves computation of a Groebner basis (for more details, refer to [CLO13]). We compute the Groebner bases in Julia [BEKS17] using the OSCAR library [OSC22, DEF+24]. We provide the code we used to perform these computations.[6]

5.1 A simple $O(n^4)$ construction

Theorem 5.1. *There exists an explicit $(n,3)$-MDS(3) code with field size $O(n^4)$.*

Proof. Assume q is an odd prime power of size at least n. Let $\mathbb{F}_q[\gamma]$ be a degree four extension. Let $\alpha : [n] \to \mathbb{F}_q$ be some injective map. We claim that

$$\beta_i = \alpha(i) + \gamma\alpha(i)^2, i \in [n]$$

form the generators of a $(n,3)-$MDS(3) code. In particular, by Lemma 2.4, we must check that

$$\det \begin{pmatrix} 1 & \beta_1+\beta_2 & \beta_1\beta_2 \\ 1 & \beta_3+\beta_4 & \beta_3\beta_4 \\ 1 & \beta_5+\beta_6 & \beta_5\beta_6 \end{pmatrix} \ne 0$$

for all injective $\alpha : [6] \to \mathbb{F}_q$. When expanded, LHS is a degree three polynomial in γ; that is, the symbolic determinant can be written as

$$P(\gamma) = p_0(\alpha)\gamma^0 + p_1(\alpha)\gamma^1 + p_2(\alpha)\gamma^2 + p_3(\alpha)\gamma^3,$$

[6] https://github.com/jbrakensiek/MDS3-Groebner

where p_i is some polynomial in $\mathbb{F}_q[x_1, \dots, x_6]$ evaluated at $\alpha(1), \dots, \alpha(6)$. A notable observation that will be useful later is that

$$p_1(\alpha) = p_0(\alpha)(\alpha_1 + \cdots + \alpha_6).$$

Since γ is a degree four field extension, we have that $P(\gamma) = 0$ if and only if $p_i(\alpha) = 0$ for all $i \in \{0, 1, 2, 3\}$. Let $J \subseteq \mathbb{F}_q[x_1, \dots, x_6]$ be the ideal generated by p_0, p_1, p_2, p_3. It suffices to prove that there exists $h \in J$ such that $h(\alpha) \neq 0$. We show this as follows.

Claim 5.2. *Let $S = \{(3, 6), (2, 4), (2, 6), (3, 5), (4, 5), (4, 6), (2, 5), (2, 3)\}$. Let $h = \prod_{(i,j)\in S}(x_i - x_j)$. Then, $h \in J$.*

Proof. It suffices to find $Q_0, Q_1, Q_2, Q_3 \in \mathbb{F}_q[x_1, \dots, x_6]$ such that $h = Q_0p_0 + Q_1p_1 + Q_2p_2 + Q_3p_3$. Note since p_0 divides p_1, we may assume $Q_1 = 0$.

Now, let $g(x) = x_2x_3 + x_2x_4 - x_2x_5 - x_2x_6 - x_3x_4 + x_5x_6$. We have that

$$Q_2 = x_2 \cdot g$$
$$Q_3 = -\frac{1}{2}g$$

Finally,

$$\begin{aligned}
Q_0 = \frac{1}{2}(&-2x_1x_2^3x_3 - 2x_1x_2^3x_4 + 2x_1x_2^3x_5 + 2x_1x_2^3x_6 - x_1x_2^2x_3^2 - x_1x_2^2x_4^2 + x_1x_2^2x_5^2 \\
&+ x_1x_2^2x_6^2 + 2x_1x_2x_3^2x_4 + 2x_1x_2x_3x_4^2 - 2x_1x_2x_5^2x_6 - 2x_1x_2x_5x_6^2 - x_1x_3^2x_4^2 \\
&+ x_1x_5^2x_6^2 - 2x_2^3x_3^2 - 2x_2^3x_3x_4 - 2x_2^3x_4^2 + 2x_2^3x_5^2 + 2x_2^3x_5x_6 \\
&+ 2x_2^3x_6^2 - x_2^2x_3^2x_4 - x_2^2x_3x_4^2 + x_2^2x_3x_4x_5 + x_2^2x_3x_4x_6 - x_2^2x_3x_5x_6 \\
&- x_2^2x_4x_5x_6 + x_2^2x_5^2x_6 + x_2^2x_5x_6^2 + 3x_2x_3^2x_4^2 + x_2x_3^2x_4x_5 + x_2x_3^2x_4x_6 \\
&- x_2x_3^2x_5x_6 + x_2x_3x_4^2x_5 + x_2x_3x_4^2x_6 + x_2x_3x_4x_5^2 + x_2x_3x_4x_6^2 \\
&- x_2x_3x_5^2x_6 - x_2x_3x_5x_6^2 - x_2x_4^2x_5x_6 - x_2x_4x_5^2x_6 - x_2x_4x_5x_6^2 \\
&- 3x_2x_5^2x_6^2 - x_3^2x_4^2x_5 - x_3^2x_4^2x_6 + x_3^2x_4x_5x_6 + x_3x_4^2x_5x_6 \\
&- x_3x_4x_5^2x_6 - x_3x_4x_5x_6^2 + x_3x_5^2x_6^2 + x_4x_5^2x_6^2)
\end{aligned}$$

We leave checking the claimed identity for h to the reader (or a CAS).

For a simpler perspective, we can make the following substitutions:

$$s_2 = \alpha_3 + \alpha_4, \qquad p_2 = \alpha_3\alpha_4,$$
$$s_3 = \alpha_5 + \alpha_6, \qquad p_3 = \alpha_5\alpha_6.$$

Then, we have that

$$\begin{aligned}
g &= x_2(s_2 - s_3) - p_2 + p_3 \\
2Q_0 &= -2x_1x_2^3(s_2 - s_3) - x_1x_2^2(s_2^2 - 2p_2 - s_3^2 + 2p_3) \\
&\quad + 2x_1x_2(s_2p_2 - s_3p_3) - x_1(p_2 - p_3)(p_2 + p_3) \\
&\quad - 2x_2^3(s_2^2 - p_2 - s_3^2 + p_3) - x_2^2(s_2 - s_3)(p_2 + p_3) \\
&\quad + x_2(3p_2^2 - 3p_3^2 + (s_2 + s_3)(p_2s_3 - s_2p_3)) - (p_2s_3 - s_2p_3)(p_2 + p_3).
\end{aligned}$$

□

Note that $h(\alpha)$ is nonzero, as α is injective. Thus, we have proved our construction is MDS(3).

□

Remark 5.3. One can adapt this construction for characteristic 2. Let $F = \mathbb{F}_2[x]/(p(x))$ be a suitable extension field, with $p(x)$ an irreducible of degree $\lceil \log_2 n \rceil + 1$. For all $i \in [n]$, pick distinct $\alpha_i \in F$ such that each α_i has 1 as its x^0 coefficient. Pick γ from a degree four extension of F, and let $\beta_i = \alpha_i + \gamma\alpha_i^3$. We can define p_0, p_1, p_2, p_3 as in the proof of Theorem 5.1, and show that the ideal they generate includes

$$\prod_{i<j\in[6]}(x_i + x_j) \prod_{i<j<k\in[6]}(x_i + x_j + x_k) \neq 0,$$

proving the code is MDS(3).

5.2 An $O(n^3)$ construction.

With another trick, we can shave the field size by another factor of n.

Theorem 1.12. *There exists an explicit* $(n, 3)$-MDS(3) *code with field size* $O(n^3)$.

Proof. Assume q is a power of 7 and let $\mathbb{F}_q[\gamma]$ be the degree three extension such that $\gamma^3 = 2$. (Observe that $x^3 - 2$ is irreducible over $\mathbb{F}_7$ as it has no roots over $\mathbb{F}_7$.) Let $S \subseteq \mathbb{F}_q$ of size n such that no six sum to 0. It is clear that we can have $|S| \geq q/7$, so we can do this as long as $q \geq 7n$.

We claim that

$$\beta_\alpha = \alpha + \gamma\alpha^2, \alpha \in S.$$

form the generators of a $(n, 3) - \text{MDS}(3)$ code. To check this, consider an injective map $\alpha : [6] \to S$. Let β_i be shorthand for $\beta_{\alpha(i)}$. By Lemma 2.4, we must check that

$$\det \begin{pmatrix} 1 & \beta_1 + \beta_2 & \beta_1\beta_2 \\ 1 & \beta_3 + \beta_4 & \beta_3\beta_4 \\ 1 & \beta_5 + \beta_6 & \beta_5\beta_6 \end{pmatrix} \neq 0$$

When we expand, without using the identity that $\gamma^3 = 2$, the LHS is a degree three polynomial in γ; that is, the symbolic determinant can be written as

$$P(\gamma) = p_0(\alpha)\gamma^0 + p_1(\alpha)\gamma^1 + p_2(\alpha)\gamma^2 + p_3(\alpha)\gamma^3,$$

where p_i is some polynomial in $\mathbb{F}_q[x_1, \ldots, x_6]$ evaluated at $\alpha(1), \ldots, \alpha(6)$. Once we apply that $\gamma^3 = 2$, we get instead that

$$P(\gamma) = (p_0(\alpha) + 2p_3(\alpha))\gamma^0 + p_1(\alpha)\gamma^1 + p_2(\alpha)\gamma^2,$$

Thus, it suffices to check that the ideal

$$J := (p_0 + 2p_3, p_1, p_2)$$

contains a polynomial which is nonzero when evaluated at $\alpha(1), \ldots, \alpha(6)$.

Claim 5.4. $(x_1 + \cdots + x_6) \prod_{1 \leq i < j \leq 6}(x_j - x_i) \in J$.

Proof. We verify this by computing a Groebner basis of J and that the remainder upon dividing the LHS by the Groebner basis is 0. We verify this in OSCAR. ☐

By Claim 5.4, it suffices to prove that

$$(\alpha(1) + \cdots \alpha(6)) \prod_{1 \leq i < j \leq 6} (\alpha(j) - \alpha(i)) \neq 0$$

for all injective maps $\alpha : [6] \to S$. Note that the first term in the product is nonzero by the definition of S, and the remaining terms are nonzero since α is injective. Thus, $P(\gamma) \neq 0$, so our code is indeed MDS(3). ☐

6 Constructions of $(n, 4)$-MDS(3) and $(n, 5)$-MDS(3) codes

In this section, we give some structural observations about MDS(3) codes which shall lead to explicit constructions of $(n, 4)$-MDS(3) and $(n, 5)$-MDS(3) codes.

6.1 MDS(ℓ) equivalent conditions for Reed-Solomon codes

First, we give an alternative characterization of the higher-order MDS conditions when considering a Reed-Solomon code.

Assume we have a (n,k)-RS code V with evaluation points $\beta_1, \ldots, \beta_n \in \mathbb{F}$. For $A \subseteq [n]$ define

$$\Pi_A(x) = \prod_{i \in A} (x - \beta_i).$$

Define $\Pi_A^d(x)$ to be the following (row) vector of polynomials:

$$\Pi_A^d(x) := (\Pi_A(x), x\Pi_A(x), \cdots, x^{d-1}\Pi_A(x)).$$

Lemma 6.1. *Assume that $A_1, \ldots, A_\ell \subseteq [n]$ such that $|A_i| \le k$ for all $i \in [\ell]$. Let $|A_1| + \cdots + |A_\ell| = (\ell-1)k$. Let $\delta_i = k - |A_i|$. Assume without loss of generality that $A_1 = \{1, 2, \ldots, k - \delta_1\}$. We have that $V_{A_1} \cap \cdots \cap V_{A_\ell} = 0$ if and only if*

$$\det \begin{pmatrix} \Pi_{A_2}^{\delta_2}(\beta_1) & \Pi_{A_3}^{\delta_3}(\beta_1) & \cdots & \Pi_{A_\ell}^{\delta_\ell}(\beta_1) \\ \Pi_{A_2}^{\delta_2}(\beta_2) & \Pi_{A_3}^{\delta_3}(\beta_2) & \cdots & \Pi_{A_\ell}^{\delta_\ell}(\beta_2) \\ \vdots & \vdots & \ddots & \vdots \\ \Pi_{A_2}^{\delta_2}(\beta_{k-\delta_1}) & \Pi_{A_3}^{\delta_3}(\beta_{k-\delta_1}) & \cdots & \Pi_{A_\ell}^{\delta_\ell}(\beta_{k-\delta_1}) \end{pmatrix} \neq 0. \tag{4}$$

Proof. Starting with the equality $V_{A_1} \cap \cdots \cap V_{A_\ell} = 0$, take the dual to get

$$V_{A_1}^\perp + \cdots + V_{A_\ell}^\perp = \mathbb{F}^k. \tag{5}$$

Identify each vector $(c_0, \ldots, c_{k-1})^T \in \mathbb{F}^k$ with the polynomial $c_0 + c_1 x + \cdots + c_{k-1}x^{k-1}$. Observe that a degree $\le k-1$ polynomial p is in $V_{A_i}^\perp$ if and only if $p(\beta_i) = 0$ for all $i \in A_i$ which is true if and only if $\Pi_{A_i} | p$. Thus, the polynomials $(\Pi_{A_i}(x), x\Pi_{A_i}(x), \ldots, x^{\delta_i - 1}\Pi_{A_i}(x)) = \Pi_{A_i}^{\delta_i}(x)$ form a basis of $V_{A_i}^\perp$.

Consider the linear transformation $\Lambda : \mathbb{F}^k \to \mathbb{F}^k$ which sends a polynomial p to the evaluations $(p(\beta_1), \ldots, p(\beta_k))$. Since the β_i's are distinct, this map is invertible because the Vandermonde matrix is nonsingular. Applying Λ to the basis $\Pi_{A_i}^{\delta_i}(x)$, we have that $V_{A_i}^\perp$ also has the following columns as a basis:

$$\begin{pmatrix} \Pi_{A_i}^{\delta_i}(\beta_1) \\ \Pi_{A_i}^{\delta_i}(\beta_2) \\ \vdots \\ \Pi_{A_i}^{\delta_i}(\beta_k) \end{pmatrix}.$$

Thus, (5) is equivalent to

$$\det \begin{pmatrix} \Pi_{A_1}^{\delta_1}(\beta_1) & \Pi_{A_2}^{\delta_2}(\beta_1) & \cdots & \Pi_{A_\ell}^{\delta_\ell}(\beta_1) \\ \Pi_{A_1}^{\delta_1}(\beta_2) & \Pi_{A_2}^{\delta_2}(\beta_2) & \cdots & \Pi_{A_\ell}^{\delta_\ell}(\beta_2) \\ \vdots & \vdots & \ddots & \vdots \\ \Pi_{A_1}^{\delta_1}(\beta_k) & \Pi_{A_2}^{\delta_2}(\beta_k) & \cdots & \Pi_{A_\ell}^{\delta_\ell}(\beta_k) \end{pmatrix} \neq 0. \tag{6}$$

The upper-left $(k - \delta_i) \times \delta_i$ submatrix in (6) is all 0's since $A_1 = \{\beta_1, \beta_2, \ldots, \beta_{k-\delta_1}\}$. The lower-left $\delta_i \times \delta_i$ submatrix in (6) has full rank since after removing common factors $\Pi_{A_1}(\beta_i)$ in each row, we are left with a Vandermonde matrix. Thus, by elementary column operations, (6) holds if and only if (4) holds. ☐

We also have the following corollary when $\ell = 3$ that we can WLOG assume the sets are disjoint.

Corollary 6.2. *Let $A_1, A_2, A_3 \subseteq [n]$ be such that $|A_1| + |A_2| + |A_3| = 2k$, $|A_1|, |A_2|, |A_3| \le k$ and $|A_1 \cap A_2 \cap A_3| = 0$. Let $A_1' = A_1 \setminus (A_2 \cup A_3), A_2' = A_2 \setminus (A_1 \cup A_3), A_3' = A_3 \setminus (A_1 \cup A_2)$ with $k' = \frac{1}{2}(|A_1'| + |A_2'| + |A_3'|)$. Let V' be the (n,k')-RS code with the same generators as V. Then, $V_{A_1} \cap V_{A_2} \cap V_{A_3} = 0$ if and only if $V'_{A_1} \cap V'_{A_2} \cap V'_{A_3} = 0$. Furthermore, $k' - |A_i'| \le k - |A_i|$ for all $i \in [3]$.*

Remark 6.3. This effectively reduces checking only the MDS conditions in which the sets are disjoint, see similar ideas in [BGM22b] and [Rot22] (i.e., Theorem 18).

Proof. We prove this result by induction on k. The base case of $k = 0$ is trivial. For positive k, note that if A_1, A_2 and A_3 are disjoint, the result immediately follows. Otherwise, assume WLOG that there is some $i \in A_2 \cap A_3$. Let $\delta_i = k - |A_i|$ and assume WLOG that that $A_1 = \{1, 2, \dots, k - \delta_1\}$. Note that $i \notin A_1$ by assumption. We will use Lemma 6.1 to reduce intersection condition to a determinant condition. Now, $x - \beta_i$ is a factor of both Π_{A_2} and Π_{A_3}. Thus,

$$\det \begin{pmatrix} \Pi^{\delta_2}_{A_2}(\beta_1) & \Pi^{\delta_3}_{A_3}(\beta_1) \\ \Pi^{\delta_2}_{A_2}(\beta_2) & \Pi^{\delta_3}_{A_3}(\beta_2) \\ \vdots & \vdots \\ \Pi^{\delta_2}_{A_2}(\beta_{k-\delta_1}) & \Pi^{\delta_3}_{A_3}(\beta_{k-\delta_1}) \end{pmatrix} = \prod_{j=1}^{k-\delta_1} (\beta_j - \beta_i) \det \begin{pmatrix} \Pi^{\delta_2}_{A_2\setminus\{i\}}(\beta_1) & \Pi^{\delta_3}_{A_3\setminus\{i\}}(\beta_1) \\ \Pi^{\delta_2}_{A_2\setminus\{i\}}(\beta_2) & \Pi^{\delta_3}_{A_3\setminus\{i\}}(\beta_2) \\ \vdots & \vdots \\ \Pi^{\delta_2}_{A_2\setminus\{i\}}(\beta_{k-\delta_1}) & \Pi^{\delta_3}_{A_3\setminus\{i\}}(\beta_{k-\delta_1}) \end{pmatrix}.$$

Since $\beta_i \neq \beta_j$ for all $j \in A_1$. We have that one of the two determinants is nonzero if and only if the other is nonzero. Let V' be the $(n, k-1)$-RS code with the generators $\beta_1, \dots, \beta_n$. The determinant on the RHS being nonzero is equivalent to whether $V'_{A_1} \cap V'_{A_2\setminus\{i\}} \cap V'_{A_3\setminus\{i\}} = 0$. Note that $(k-1) - |A_1| \le k - |A_1|$, $(k-1) - |A_2 \setminus \{i\}| \le k - |A_2|$ and $(k-1) - |A_3 \setminus \{i\}| \le k - |A_3|$. Thus, by induction, we may iterate on $(A_1, A_2 \setminus \{i\}, A_3 \setminus \{i\})$ until the three sets are pairwise disjoint. ☐

6.2 $(n, 4)$-MDS(3)

The goal of this section is the following theorem.

Theorem 6.4. *There exists an explicit (n, k)-MDS code V over field size $O(n)^{2k-1}$ such that for any $A_1, A_2, A_3 \subseteq [n]$ such that $|A_1| = 2$ and $|A_2| = |A_3| = k - 1$ we have that $V_{A_1} \cap V_{A_2} \cap V_{A_3} = 0$ whenever it generically should.*

This result immediately implies a $(n, 4)$-MDS(3) construction..

Corollary 6.5. *There exists an explicit $(n, 4)$-MDS(3) code over field size $O(n^7)$.*

Proof. By Corollary 2.2, the only nontrivial condition for $(n, 4)$-MDS(3) is $|A_1| = 2$ and $|A_2| = |A_3| = 3$, so the construction applies. ☐

Remark 6.6. By similar logic, Theorem 6.4 allows one to construct a $(n, 3)$-MDS(3) code over field size $O(n^5)$, although the constructions in Section 5 are superior.

Proof of Theorem 6.4. Let $q \ge n$ be a prime power with characteristic at least k. Let K be the a degree-$2k - 1$ extension of $\mathbb{F}_q$. We let γ be a generator of this extension.

Pick an arbitrary injective map $\alpha : [n] \to \mathbb{F}_q$. We shall let our RS field evaluations be

$$\beta_i = \gamma\alpha_i - \alpha_i^2.$$

We let $V(\alpha, \gamma)$ be the dimension k RS code with $\beta_1, \dots, \beta_n$ (as defined above) as evaluation points.

Let A_1, A_2, A_3 be such that $|A_1| = 2$ and $|A_2| = |A_3| = k - 1$, and $W_{A_1} \cap W_{A_2} \cap W_{A_3} = 0$ for a generic matrix W. By Corollary 6.2, to check that $V_{A_1} \cap V_{A_2} \cap V_{A_3} = 0$, it suffices to check our construction works for $A'_i \subseteq A_i$ in the code V' (i.e., the (n, k')-RS code with generators $\beta_1, \dots, \beta_n$) where $k' = \frac{1}{2}(|A'_1| + |A'_2| + |A'_3|)$ which are pairwise disjoint.

If $|A'_2|$ or $|A'_3|$ is at least k', then $V_{A'_1} \cap V_{A'_2} \cap V_{A'_3}$ would be what it generically should be based on V being MDS. Otherwise, $|A'_2| + |A'_3| \le 2k' - 2$, so $|A'_1| \ge 2 = |A_1|$. Thus, we may assume without loss of generality that $A'_1 = A_1 = \{1, 2\}$ and that $|A'_2| = |A'_3| = k' - 1$. We may also assume $k' > |A_1| = 2$ by the same reasoning.

We seek to show that (4) has full row rank (i.e., nonzero determinant). That is, it suffices to consider the determinant.

$$\Pi_{A'_2}(\beta_1)\Pi_{A'_3}(\beta_2) - \Pi_{A'_2}(\beta_2)\Pi_{A'_3}(\beta_1).$$

Now, observe that for some nonzero $a \in \mathbb{F}_q$, we have that

$$\Pi_{A_2'}(\beta_1)\Pi_{A_3'}(\beta_2) = a \prod_{i \in A_2'} (\gamma - (\alpha_1 + \alpha_i)) \prod_{j \in A_3'} (\gamma - (\alpha_2 + \alpha_j)).$$

Likewise for some nonzero $b \in \mathbb{F}_q$,

$$\Pi_{A_2'}(\beta_2)\Pi_{A_3'}(\beta_1) = b \prod_{i \in A_2'} (\gamma - (\alpha_2 + \alpha_i)) \prod_{j \in A_3'} (\gamma - (\alpha_1 + \alpha_j)).$$

Assume for sake of contradiction that $\Pi_{A_2'}(\beta_1)\Pi_{A_3'}(\beta_2) = \Pi_{A_2'}(\beta_2)\Pi_{A_3'}(\beta_1)$. Since γ is a degree n^{2k-1} extension, by comparing the lead coefficients, we know that $a = b$, and the polynomials in γ must have the same roots. Thus, there exists a permutation $\pi : (\{1\} \times A_2') \cup (\{2\} \times A_3') \to (\{2\} \times A_2') \cup (\{1\} \times A_3')$ such that whenever $\pi(i_1, i_2) = (j_1, j_2)$ we have that $\alpha_{i_1} + \alpha_{i_2} = \alpha_{j_1} + \alpha_{j_2}$. Since we are assuming that A_2' and A_3' are disjoint, we can never map $\{1\} \times A_2'$ to $\{1\} \times A_3'$ nor $\{2\} \times A_3'$ to $\{2\} \times A_2'$. Thus, we can decompose π into a pair of permutations $\tau_2 : A_2' \to A_2'$ and $\tau_3 : A_3' \to A_3'$ such that for all $i \in A_2'$ we have that $\alpha_1 + \alpha_i = \alpha_2 + \alpha_{\tau_2(i)}$ with a similar definition for τ_3. Now observe that since $\mathbb{F}_q$ has characteristic at least k we have that

$$0 \neq |A_2'|(\alpha_2 - \alpha_1) = \sum_{i \in A_2'} (\alpha_i - \alpha_{\tau_2(i)}) = \sum_{i \in A_2'} \alpha_i - \sum_{i \in A_2'} \alpha_i = 0,$$

a contradiction. ◻

6.3 $(n, 5)$-MDS(3)

We generalize the construction a bit in the weak-MDS case; that is, where the sets considered are disjoint (c.f., [BGM22b, Rot22]).

Theorem 6.7. *There exists an explicit (n, k)-MDS code V over field size $O(n)^{2k^2}$ such that for any $A_1, A_2, A_3 \subseteq [n]$ such that $|A_1| + |A_2| = k + 1$ and $|A_3| = k - 1$ we have that $V_{A_1} \cap V_{A_2} \cap V_{A_3} = 0$ whenever it generically should.*

Note that for any $k \le 5$, if $|A_1| + |A_2| + |A_3| = 2k$ and each has size at most $k - 1$, then at least one $|A_i| = k - 1$. Thus, we have the following immediately corollary.

Corollary 6.8. *There exists an explicit $(n, 5)$-MDS(3) code over field size $O(n^{50})$*

Proof of Theorem 6.7. Pick distinct $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ such that $\alpha_{i_1} + \alpha_{i_2} = \alpha_{j_1} + \alpha_{j_2}$ iff $\{i_1, i_2\} = \{j_1, j_2\}$. It is clear that this works for $q \approx n^2$. For example, over characteristic 2, we can take $\alpha_1, \ldots, \alpha_n$ to be the columns of a parity check matrix of a BCH code with distance 5. Let $\mathbb{F}_q[x]$ be the univariate polynomial ring over $\mathbb{F}_q$. We define our Reed-Solomon evaluation polynomials to be $\beta_i(x) = \alpha_i x - \alpha_i^2$ for all $i \in [n]$. A key observation is that due to our choice of α_i's, whenever $i_1 \neq i_2$, $j_1 \neq j_2$, and $\{i_1, i_2\} \neq \{j_1, j_2\}$ we have that[7]

$$\gcd(\beta_{i_1} - \beta_{i_2}, \beta_{j_1} - \beta_{j_2}) = 1. \tag{7}$$

Let $V(x)$ be the (n, k)-RS code generated by these evaluation points. We claim that for any $A_1, A_2, A_3 \subseteq [n]$ with $|A_1| + |A_2| = k + 1$ and $|A_3| = k - 1$ and $W_{A_1} \cap W_{A_2} \cap W_{A_3}$, we have that

$$V_{A_1}(x) \cap V_{A_2}(x) \cap V_{A_3}(x) = 0. \tag{8}$$

Since this condition can be written as a degree $\le k^2$ polynomial in x, by evaluating V at some degree k^2 irreducible of $\mathbb{F}_q$, we then immediately get an n^{2k^2} construction.[8]

By Corollary 6.2, it suffices to prove $V'_{A_1'}(x) \cap V'_{A_2'}(x) \cap V'_{A_3'}(x) = 0$, where V' is the (n, k')-RS code with the same generators where $k' = (|A_1'| + |A_2'| + |A_3'|)/2$, $A_i' \subseteq A_i$, and A_1', A_2', A_3' are disjoint. If $|A_i'| \ge k'$ for some i, then the condition on V' follows from V' being MDS. Since $|A_3'| \ge k' - 1$ by Corollary 6.2, we may assume that $|A_1'| = a'$, $|A_2'| = k' + 1 - a'$ and $|A_3'| = k' - 1$.

[7] Here we assume that gcd always returns a monic polynomial.
[8] We suspect this construction works over a smaller field extension.

Assume without loss of generality that $A'_1 = \{1, 2, \ldots, a'\}$. By Lemma 6.1, we have that (8) holds iff

$$\det \begin{pmatrix} \Pi_{A'_2}^{a'-1}(\beta_1) & \Pi_{A'_3}(\beta_1) \\ \Pi_{A'_2}^{a'-1}(\beta_2) & \Pi_{A'_3}(\beta_2) \\ \vdots & \vdots \\ \Pi_{A'_2}^{a'-1}(\beta_{a'}) & \Pi_{A'_3}(\beta_{a'}) \end{pmatrix} \neq 0.$$

We now use an infinite descent argument. Assume for sake of contradiction that the determinant equals zero. Then, there exists $g_1, \ldots, g_{a'} \in \mathbb{F}_q[x]$ with $\gcd(g_1, \ldots, g_{a'}) = 1$ such that for all $i \in [a']$,

$$\left(\sum_{j=1}^{a'-1} \beta_i^{j-1} g_j\right) \Pi_{A'_2}(\beta_i) + g_{a'} \Pi_{A'_3}(\beta_i) = 0.$$

Note that by (7), we have that $\gcd(\Pi_{A'_2}(\beta_i), \Pi_{A'_3}(\beta_i)) = 1$ for all $i \in [a]$. Thus, $\Pi_{A'_2}(\beta_i)$ divides $g_{a'}$ for all $i \in [a']$. Further, by (7), we have further that $\prod_{i=1}^{a'} \Pi_{A'_2}(\beta_i)$ divides $g_{a'}$. Thus, for some $h_{a'} \in \mathbb{F}_q[x]$ (possibly zero), we have that for all $i \in [a']$,

$$\sum_{j=1}^{a'-1} \beta_i^{j-1} g_j + h_{a'} \Pi_{A'_3}(\beta_i) \prod_{\substack{j=1 \\ j \neq i}}^{a'} \Pi_{A'_2}(\beta_j) = 0.$$

In particular, we have that for all $i \in [a' - 1]$,

$$\sum_{j=1}^{a'-1} \beta_i^{j-1} g_j \equiv 0 \mod \Pi_{A'_2}(\beta_{a'}).$$

By standard properties of the Vandermonde determinant, we have that for each $i \in [a' - 1]$ there exists a polynomial $h_i \in \mathbb{F}_q[x]$ such that g_i can be written as $h_i \Pi_{A'_2}(\beta_{a'}) / \prod_{1 \le i < j \le a'-1}(\beta_j - \beta_i)$.

Using (7) one last time, we have that $\prod_{1 \le i < j \le a'-1}(\beta_j - \beta_i)$ is relatively prime to $\Pi_{A'_2}(\beta_{a'})$. Thus, each g_i is divisible by $\Pi_{A'_2}(\beta_{a'})$. This violates the assumption that $\gcd(g_1, \ldots, g_{a'}) = 1$. Therefore, (8) holds and our construction is valid. □

References

[BEKS17] Jeff Bezanson, Alan Edelman, Stefan Karpinski, and Viral B Shah. Julia: A fresh approach to numerical computing. *SIAM review*, 59(1):65–98, 2017.

[BGM22a] Joshua Brakensiek, Sivakanth Gopi, and Visu Makam. Generic reed-solomon codes achieve list-decoding capacity. *ArXiv*, abs/2206.05256, 2022.

[BGM22b] Joshua Brakensiek, Sivakanth Gopi, and Visu Makam. Lower bounds for maximally recoverable tensor codes and higher order MDS codes. *IEEE Transactions on Information Theory*, 68(11):7125–7140, 2022.

[CLO13] David Cox, John Little, and Donal OShea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Science & Business Media, 2013.

[DEF+24] Wolfram Decker, Christian Eder, Claus Fieker, Max Horn, and Michael Joswig, editors. *The OSCAR book*. 2024.

[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.

[GHK10] Venkatesan Guruswami, Johan Håstad, and Swastik Kopparty. On the list-decodability of random linear codes. *IEEE Transactions on Information Theory*, 57:718–725, 2010.

[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.

[GST21] 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.

[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.

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

[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.

[OSC22] Oscar – open source computer algebra research system, version 0.11.3-dev, 2022.

[PGM13] James S. Plank, Kevin M. Greenan, and E. L. Miller. Screaming fast galois field arithmetic using intel simd instructions. In *USENIX Conference on File and Storage Technologies*, 2013.

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

[Sin64] Richard Singleton. Maximum distance q-nary codes. *IEEE Transactions on Information Theory*, 10(2):116–118, 1964.

[ST20] Chong Shangguan and Itzhak Tamo. Combinatorial list-decoding of Reed-Solomon codes beyond the johnson radius. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 538–551, 2020.

[Tia19] Yongge Tian. Formulas for calculating the dimensions of the sums and the intersections of a family of linear subspaces with applications. *Beiträge zur Algebra und Geometrie/Contributions to Algebra and Geometry*, 60(3):471–485, 2019.

[YH19] Hikmet Yildiz and Babak Hassibi. Optimum linear codes with support-constrained generator matrices over small fields. *IEEE Transactions on Information Theory*, 65(12):7868–7875, 2019.