Electronic Colloquium on Computational Complexity, Report No. 47 (2018)

A proof of the GM-MDS conjecture

Shachar Lovett

March 6, 2018

Abstract

The GM-MDS conjecture of Dau et al. (ISIT 2014) speculates that the MDS condition, which guarantees the existence of MDS matrices with a prescribed set of zeros over large fields, is in fact sufficient for existence of such matrices over small fields. We prove this conjecture.

1 Introduction

Let $S_1, \ldots, S_k \subset [n]$ be a set system with $k \leq n$. A natural question, motivated by the study of MDS codes, is when does there exist a $k \times n$ matrix G over a finite field $\mathbb{F}$, such that all $k \times k$ minors of G are full rank, and such that $G_{i,j} = 0$ whenever $j \in S_i$.

If there is no limitation on the field size then the answer is well known. Any row can have at most $k-1$ zeros. Any pair of rows at most $k-2$ common zeros, and so on. This is the so-called *MDS condition*:

$$\left| \bigcap_{i \in I} S_i \right| \leq k - |I| \qquad \forall I \subseteq [k]. \tag{1}$$

Concretely, for any set system which satisfies the MDS condition, and for any field of size $|\mathbb{F}| > \binom{n-1}{k-1}$, there exist matrices G with a prescribed set of zeros given by the set system (see for example [DSDY13] for details). In fact, if $|\mathbb{F}| \gg \binom{n}{k}$ then one can simply choose a random matrix G with $G_{i,j} = 0$ if $j \in S_i$, and $G_{i,j} \in \mathbb{F}$ uniformly for all other entries, and obtain that with high probability all the minors of G are nonsingular.

A much more subtle question is that is the minimum field size for which such a matrix exists. Dau et al. [DSY14] conjectured that the MDS condition (1) is sufficient for the existence of a matrix G over much smaller fields.

Conjecture 1.1 (GM-MDS conjecture [DSY14]). *Let $S_1, \ldots, S_k \subset [n]$ be a set system which satisfies the MDS condition. Then for any field $\mathbb{F}$ with $|\mathbb{F}| \geq n + k - 1$, there exists a $k \times n$ matrix G over $\mathbb{F}$ with $G_{i,j} = 0$ whenever $j \in S_i$, such that all $k \times k$ minors of G are nonsingular.*

We prove Conjecture 1.1 in this work. First, we describe an algebraic framework introduced by Dau et al. [DSY14] towards proving Conjecture 1.1.

ISSN 1433-8092

1.1 The algebraic GM-MDS conjecture

Dau et al. [DSY14] formulated an algebraic conjecture that implies Conjecture 1.1: if $S_1, \ldots, S_k$ is a set system that satisfies (1), then there exists a Generalized Reed-Muller code with zeros in locations prescribed by the set system. Otherwise put, there exists $G = AV$ where A is an invertible $k \times k$ matrix and V a $k \times n$ Vandermonde matrix, such that $G_{i,j} = 0$ when $j \in S_i$. Before we explain these ideas further, we first set up some notations.

Let $\mathbb{F}$ be a finite field, and let $x, a_1, \ldots, a_n$ be formal variables, where we shorthand $\mathbf{a} = (a_1, \ldots, a_n)$. We use the standard notations $\mathbb{F}[\mathbf{a}, x]$ for the ring of polynomials over $\mathbb{F}$ in the variables $\mathbf{a}, x$; $\mathbb{F}(\mathbf{a})$ for the field of rational functions over $\mathbb{F}[\mathbf{a}]$; and $\mathbb{F}(\mathbf{a})[x]$ for the ring of univariate polynomials in x over $\mathbb{F}(\mathbf{a})$. Given a set $S \subset [n]$ define a polynomial $p = p(S) \in \mathbb{F}[\mathbf{a}, x]$ as follows:

$$p(\mathbf{a}, x) := \prod_{i \in S} (x - a_i).$$

Given a set system $\mathcal{S} = \{S_1, \ldots, S_k\}$ define $P(\mathcal{S}) := \{p(S_1), \ldots, p(S_k)\}$.

Let $\mathcal{S} = \{S_1, \ldots, S_k\}$ be a set system which satisfies (1). It is possible to assume without loss of generality that each S_i is maximal, namely that $|S_i| = k - 1$ for all $i \in [k]$. For example, if we are allowed to increase n then we can replace each S_i with $S_i \cup T_i$ where $|T_i| = k - 1 - |S_i|$ and $T_1, \ldots, T_k, [n]$ are pairwise disjoint. An improved reduction is given in [DSY14] which does not require increasing n.

Either way, under this assumption the polynomials $P(\mathcal{S})$ form a set of k polynomials of degree $k - 1$, which we denote by $p_1, \ldots, p_k$. Define the $k \times n$ matrix G as $G_{i,j} = p_i(a_j)$. Note that entries of G are polynomials in $\mathbb{F}[\mathbf{a}]$. The condition that all $k \times k$ minors of G are nonsingular is equivalent to the condition that the polynomials $P(\mathcal{S})$ are linearly independent over $\mathbb{F}(\mathbf{a})$ (here, we view the polynomials as elements of $\mathbb{F}(\mathbf{a})[x]$ instead of as elements of $\mathbb{F}[\mathbf{a}, x]$). If this is the case, then one can use the Schwartz-Zippel lemma and show that the formal variables $a_1, \ldots, a_n$ can be replaced with distinct field elements from $\mathbb{F}$, while still maintaining the property that all $k \times k$ minors of G are nonsingular. The bound on the field size $|\mathbb{F}| \geq n + k - 1$ arises from the degrees of the polynomials obtained in the process. For details we refer to the original paper [DSY14].

This motivated [DSY14] to propose the following algebraic conjecture, which implies Conjecture 1.1.

Conjecture 1.2 (Algebraic GM-MDS conjecture [DSY14])**.** *Let $S_1, \ldots, S_k \subset [n]$ be a set system which satisfies the MDS condition, and where $|S_i| = k - 1$ for all i. Then the set of polynomials $P(\mathcal{S})$ are linearly independent over $\mathbb{F}(\mathbf{a})$.*

We remark that given any polynomials $p_1, \ldots, p_k \in \mathbb{F}[\mathbf{a}, x]$ (for example, the polynomials appearing in $P(\mathcal{S})$), an equivalent condition to the polynomials being linearly independent over $\mathbb{F}(\mathbf{a})$ is the following: for any polynomials $w_1, \ldots, w_k \in \mathbb{F}[\mathbf{a}]$, not all zero, it holds that

$$\sum_{i=1}^{k} w_i(\mathbf{a}) p_i(\mathbf{a}, x) \neq 0.$$

Following [DSY14], several works [HHYD14, HS17, YH18] attempted to resolve the GM-MDS conjecture. They showed that Conjecture 1.2 holds in several special cases, but the general case remained open. In this work we prove Conjecture 1.2, which implies Conjecture 1.1.

1.2 A generalized conjecture

We start by considering a more general condition. Let $v \in \mathbb{N}^n$ be a vector, where $\mathbb{N} = \{0, 1, 2, \ldots\}$ stands for non-negative integers. The coordinates of v are $v = (v(1), \ldots, v(n))$. We shorthand $|v| = \sum v(i)$. Given vectors $v_1, \ldots, v_m \in \mathbb{N}^n$ define $\bigwedge v_i \in \mathbb{N}^n$ to be their coordinate-wise minimum:

$$\bigwedge_{i \in [m]} v_i := (\min(v_1(1), \ldots, v_m(1)), \ldots, \min(v_1(n), \ldots, v_m(n))).$$

Note that if $v_1, \ldots, v_m \in \{0, 1\}^n$ are indicator vectors of sets $S_1, \ldots, S_m \subset [n]$, then $\bigwedge v_i$ is the indicator vector of $\cap S_i$.

Given a parameter $k > |v|$ define a set of polynomials in $\mathbb{F}[\mathbf{a}, x]$:

$$P(k, v) := \left\{ \prod_{j \in [n]} (x - a_j)^{v(j)} x^e : e = 0, \ldots, k - 1 - |v| \right\}.$$

Note that $P(k, v)$ consists of $k - |v|$ polynomials of degree $\leq k - 1$, which form a basis for the linear space of polynomials of degree $\leq k - 1$ which have $v(j)$ roots at each a_j. Furthermore, note that if v is the indicator vector of a set $S \subset [n]$ of size $|S| = k - 1$, then $P(k, v) = \{p(S)\}$. Given a set of vectors $\mathcal{V} = \{v_1, \ldots, v_m\} \subset \mathbb{N}^n$ define

$$P(k, \mathcal{V}) := P(k, v_1) \cup \ldots \cup P(k, v_m).$$

We use in this paper the convention that set union can result in a multiset. So for example, if the same polynomial appears in multiple $P(k, v_i)$ then it appears multiple times in $P(k, \mathcal{V})$. Under this assumption we always have the identity:

$$|P(k, \mathcal{V})| = |P(k, v_1)| + \ldots + |P(k, v_m)|.$$

The following definition is the natural extension of the MDS condition (1) to vectors.

Definition 1.3 (Property $V(k)$)**.** *Let $\mathcal{V} = \{v_1, \ldots, v_m\} \subset \mathbb{N}^n$ and $k \geq 1$ be an integer. We say that $\mathcal{V}$ satisfies $V(k)$ if it satisfies:*

(i) $|v_i| \leq k - 1$ for all $i \in [m]$.

(ii) For all $I \subseteq [m]$, $\sum_{i \in I}(k - |v_i|) + \left|\bigwedge_{i \in I} v_i\right| \leq k$.

Note that when $m = k$ and $v_1, \ldots, v_k$ are indicators of sets $S_1, \ldots, S_k \subset [n]$ of size $|S_i| = k-1$, then property $V(k)$ is equivalent to the MDS condition for $S_1, \ldots, S_k$.

Observe that in general, if $\mathcal{V}$ satisfies $V(k)$ then $P(k, \mathcal{V})$ contains $\sum_{i=1}^{m}(k - |v_i|) \leq k$ polynomials of degree $\leq k-1$. The following conjecture is the natural extension of Conjecture 1.2 to vectors.

Conjecture 1.4. *Let $\mathcal{V} \subset \mathbb{N}^n$ and $k \geq 1$. Assume that $\mathcal{V}$ satisfies $V(k)$. Then the polynomials in $P(k, \mathcal{V})$ are linearly independent over $\mathbb{F}(\mathbf{a})$.*

A clarifying remark: as we view the set $P(k, \mathcal{V})$ as a multiset, Conjecture 1.4 (and Theorem 1.6 below) imply in particular that the polynomials in $P(k, \mathcal{V})$ are all distinct, so $P(k, \mathcal{V})$ is in fact a set.

1.3 An intermediate case

We prove Conjecture 1.4 under an additional assumption, which is sufficient to prove Conjecture 1.1. It is still open to prove Conjecture 1.4 in full generality.

Definition 1.5 (Property $V^*(k)$)**.** *Let $\mathcal{V} = \{v_1, \ldots, v_m\} \subset \mathbb{N}^n$ and $k \geq 1$ be an integer. We say that $\mathcal{V}$ satisfies $V^*(k)$ if it satisfies $V(k)$, and additionally it satisfies:*

(iii) $v_i \in \{0,1\}^{n-1} \times \mathbb{N}$ for all $i \in [m]$. Namely, all coordinates in v_i, except perhaps the last, are in $\{0,1\}$.

Theorem 1.6. *Let $\mathcal{V} \subset \mathbb{N}^n$ and $k \geq 1$. Assume that $\mathcal{V}$ satisfies $V^*(k)$. Then the polynomials $P(k, \mathcal{V})$ are linearly independent over $\mathbb{F}(\mathbf{a})$.*

Conjecture 1.2 follows directly from Theorem 1.6. If $S_1, \ldots, S_k \subset [n]$ are sets which satisfy the assumptions of Conjecture 1.2, then their indicator vectors $v_1, \ldots, v_k \in \{0,1\}^n$ satisfy the assumptions of Theorem 1.6, and hence $P(\{S_1, \ldots, S_k\}) = P(k, \{v_1, \ldots, v_k\})$ are linearly independent over $\mathbb{F}(\mathbf{a})$.

2 Proof of Theorem 1.6

Let $n, k \geq 1$. Let $\mathcal{V} = \{v_1, \ldots, v_m\} \subset \mathbb{N}^n$ which satisfies $V^*(k)$. We will prove that the polynomials $P(k, \mathcal{V})$ are linearly independent over $\mathbb{F}(\mathbf{a})$.

To that end, we assume that $\mathcal{V}$ is a minimal counter-example and derive a contradiction. Concretely, the underlying parameters are n, k, m and $d = |P(k, \mathcal{V})| = \sum k - |v_i|$. We will assume that if $\mathcal{V}'$ is a set of vectors with corresponding parameters $n' \leq n, k' \leq k, m' \leq m, d' \leq d$ with at least one of the inequalities being sharp, then Theorem 1.6 holds for $\mathcal{V}'$. In particular, we assume that $m \geq 2$, as Theorem 1.6 clearly holds when $m = 1$.

To help the reader, we note that the following lemmas construct such $\mathcal{V}'$ with the following parameters:

- Lemma 2.2: $n, k-1, m, d$.

- Lemma 2.4: n, k, e, d' and $n, k, m-e+1, d''$ with $2 \le e \le m-1$ and $d', d'' < d$.
- Lemma 2.5: $n-1, k, m, d$.
- Lemma 2.6: $n, k, m, d-1$.

We use the following notation to simplify the presentation:

$$v_I := \bigwedge_{i \in I} v_i \qquad I \subseteq [m].$$

We introduce sometimes in the proofs an auxiliary set $\mathcal{V}' = \{v'_1, \ldots, v'_{m'}\}$, in which case v'_I for $I \subseteq [m']$ are defined analogously. Below, when we say that $\mathcal{V}$ or $\mathcal{V}'$ satisfy (i), (ii) or (iii), we mean the relevant items in the definition of $V^*(k)$.

Given two vectors $u, v \in \mathbb{N}^n$ we denote $u \le v$ if $u(i) \le v(i)$ for all $i \in [n]$.

Lemma 2.1. *There do not exist distinct $i, j \in [m]$ such that $v_i \le v_j$.*

Proof. Assume the contrary. Applying (i) to j gives $|v_j| \le k-1$. Applying (ii) to $I = \{i, j\}$ gives

$$(k - |v_i|) + (k - |v_j|) + |v_i \wedge v_j| \le k.$$

As $v_i \le v_j$ we have $v_i \wedge v_j = v_i$, and hence obtain that $k - |v_j| \le 0$, a contradiction. □

Lemma 2.1 implies in particular that $n \ge 2$. This is since if $n = 1$ then necessarily $m = 1$, as otherwise there would be i, j for which $v_i \le v_j$. So we assume $n \ge 2$ from now on.

Lemma 2.2. $\bigwedge_{i \in [m]} v_i = 0$.

Proof. Assume not. Then there exists a coordinate $j \in [n]$ with $v_i(j) \ge 1$ for all $i \in [m]$. Define a new set of vectors $\mathcal{V}' = \{v'_1, \ldots, v'_m\} \subset \mathbb{N}^n$ as follows:

$$v'_i := (v_i(1), \ldots, v_i(j-1), v_i(j) - 1, v_i(j+1), \ldots, v_i(n)).$$

In words, v'_i is defined from v_i by decreasing coordinate j by 1.

We first show that $\mathcal{V}'$ satisfies $V^*(k-1)$. Note that $|v'_i| = |v_i| - 1$. It clearly satisfies (i),(iii). To show that it satisfies (ii) let $I \subseteq [m]$. We have

$$\sum_{i \in I} (k - 1 - |v'_i|) + |v'_I| = \sum_{i \in I} (k - |v_i|) + |v_I| - 1 \le k - 1.$$

As we showed that $\mathcal{V}'$ satisfies $V^*(k-1)$, the minimality of $\mathcal{V}$ implies that the polynomials $P(k-1, \mathcal{V}')$ are linearly independent over $\mathbb{F}(\mathbf{a})$. The lemma follows as it is simple to verify that

$$P(k, \mathcal{V}) = \{p(\mathbf{a}, x)(x - a_j) : p \in P(k-1, \mathcal{V}')\}.$$

In particular, the linear independence of $P(k-1, \mathcal{V}')$ implies the linear independence of $P(k, \mathcal{V})$. □

Definition 2.3 (Tight constraint)**.** *A set $I \subseteq [m]$ is* tight for $\mathcal{V}$ *if property (ii) holds with equality for I. Namely if*

$$\sum_{i \in I}(k - |v_i|) + |v_I| = k.$$

Note that if $|I| = 1$ then I is always a tight constraint. The following lemma is an extension of Lemma 2(i) in [YH18]. It shows that in a minimal counter-example there are no tight sets, except for singletons and perhaps the whole set.

Lemma 2.4. *If $I \subseteq [m]$ is a tight constraint, then $|I| = 1$ or $|I| = m$.*

Proof. Assume towards a contradiction that there exist a tight I with $1 < |I| < m$. We will use the minimality of $\mathcal{V}$ to derive a contradiction. Assume for simplicity of notation that $I = \{e, \dots, m\}$ for $2 \le e \le m-1$. Define a new set of vectors $\mathcal{V}' = \{v'_1, \dots, v'_e\}$ given by

$$v'_1 := v_1, \dots, v'_{e-1} := v_{e-1}, v'_e := v_I.$$

We first show that $\mathcal{V}'$ satisfies $V^*(k)$. It clearly satisfies (i) and (iii). To see that it satisfies (ii) let $I' \subseteq [e]$. If $e \notin I'$ then $\mathcal{V}'$ satisfies (ii) for I' as it is same condition as for $\mathcal{V}$, so assume $e \in I'$. Let $I'' = I' \cup \{e+1, \dots, m\}$. Then

$$\sum_{i \in I'}(k - |v'_i|) + |v'_{I'}| = \sum_{i \in I''}(k - |v_i|) + |v_{I''}| \le k,$$

where the equality holds since $k - |v'_e| = \sum_{i \in I}(k - |v_i|)$ since we assume I is tight, and since by definition of I'' we have $v'_I = v_{I''}$.

As we assume that $\mathcal{V}$ is a minimal counter-example for Theorem 1.6, the theorem holds for $\mathcal{V}'$. So, the polynomials $P(k, \mathcal{V}')$ are linearly independent. Observe that $|P(k, \mathcal{V}')| = |P(k, \mathcal{V})|$ since

$$|P(k, \mathcal{V}')| = \sum_{i \in [e]}(k - |v'_i|) = \sum_{i \in [m]}(k - |v_i|) = |P(k, \mathcal{V})|.$$

Thus, it will suffice to prove that $P(k, \mathcal{V})$ and $P(k, \mathcal{V}')$ span the same space of polynomials over $\mathbb{F}(\mathbf{a})$. To that end, it suffices to prove that $F := P(k, \{v_e, \dots, v_m\})$ and $F' := P(k, v'_e)$ span the same space of polynomials.

Let us shorthand $v = v'_e$. Define the polynomial $p(\mathbf{a}, x) := \prod_{j \in [n]}(x - a_j)^{v(j)}$. Observe that p divides all polynomials in F, F'. Moreover, $F' = \{p(\mathbf{a}, x)x^d : d = 0, \dots, k-1-|v|\}$ spans the linear space of all multiples of p of degree $\le k-1$. As $|F| = |F'|$ it suffices to prove that F are linearly independent over $\mathbb{F}(\mathbf{a})$, as then they must span the same linear space. However, this follows from the minimality of $\mathcal{V}$, since $F = P(k, \mathcal{V}'')$ for $\mathcal{V}'' = \{v_e, \dots, v_m\}$. □

The following lemma identifies a concrete vector that must exist in a minimal counter-example. It is in its proof that we actually use the assumption that $\mathcal{V}$ satisfies (iii), namely $V^*(k)$ and not merely $V(k)$.

Lemma 2.5. *There exists $i \in [m]$ such that $v_i = (1, \dots, 1, 0)$.*

Proof. Lemma 2.2 guarantees that there exists $i^* \in [m]$ for which $v_{i^*}(n) = 0$. We will prove that $v_{i^*} = (1, \ldots, 1, 0)$. If not, then by (iii) there exists $j^* \in [n-1]$ be such that $v_{i^*}(j^*) = 0$. For simplicity of notation assume that $i^* = m, j^* = n-1$. Define a new set of vectors $\mathcal{V}' = \{v'_1, \ldots, v'_m\} \subset \mathbb{N}^{n-1}$ as follows:

$$v'_i := (v_i(1), \ldots, v_i(n-2), v_i(n-1) + v_i(n)) .$$

In words, $v'_i \in \mathbb{N}^{n-1}$ is obtained by adding the last two coordinates of $v_i \in \mathbb{N}^n$.

We first show that $\mathcal{V}'$ satisfies $V^*(k)$. Note that $|v'_i| = |v_i|$. It clearly satisfies (i),(iii). To show that it satisfies (ii) let $I \subseteq [m]$. Note that (ii) always holds if $|I| = 1$, so we may assume $|I| > 1$. We have by definition

$$\sum_{i \in I}(k - |v'_i|) + |v'_I| - v'_I(n-1) = \sum_{i \in I}(k - |v_i|) + |v_I| - v_I(n-1) - v_I(n). \tag{2}$$

First, consider first the case where $|I| < m$. Lemma 2.4 gives that I is not tight, and hence

$$\sum_{i \in I}(k - |v_i|) + |v_I| \leq k - 1.$$

As $\mathcal{V}$ satisfies (iii) we have $v_i(n-1) \in \{0, 1\}$ for all i. This implies $v_I(n-1) \in \{0, 1\}$ and $v'_I(n-1) \in \{v_I(n), v_I(n) + 1\}$. So Equation (2) gives

$$\sum_{i \in I}(k - |v'_i|) + |v'_I| \leq \sum_{i \in I}(k - |v_i|) + |v_I| + 1 \leq k.$$

Next, consider the case of $|I| = m$. As $v_m(n-1) = v_m(n) = 0$ we have $v'_m(n-1) = 0$ and hence $v_I(n-1) = v_I(n) = v'_I(n-1) = 0$. Equation (2) then gives

$$\sum_{i \in I}(k - |v'_i|) + |v'_I| = \sum_{i \in I}(k - |v_i|) + |v_I| \leq k.$$

As we showed that $\mathcal{V}'$ satisfies $V^*(k)$, the minimality of $\mathcal{V}$ implies that the polynomials $P(k, \mathcal{V}')$ are linearly independent over $\mathbb{F}(\mathbf{a})$. We next show that this implies that $P(k, \mathcal{V})$ are also linearly independent over $\mathbb{F}(\mathbf{a})$.

Let $s_i := k - |v_i|$ for $i \in [m]$. We have $P(k, \mathcal{V}) = \{p_{i,e} : i \in [m], e \in [s_i]\}$ and $P(k, \mathcal{V}') = \{p'_{i,e} : i \in [m], e \in [s_i]\}$ where

$$p_{i,e}(\mathbf{a}, x) := x^{e-1} \prod_{j \in [n-2]} (x - a_j)^{v_i(j)} \cdot (x - a_{n-1})^{v_i(n-1)} (x - a_n)^{v(n)} ,$$
$$p'_{i,e}(\mathbf{a}, x) := x^{e-1} \prod_{j \in [n-2]} (x - a_j)^{v_i(j)} \cdot (x - a_{n-1})^{v_i(n-1) + v_i(n)} .$$

Observe that $p'_{i,e}$ can be obtained from $p_{i,e}$ by substituting a_{n-1} for a_n. Namely

$$p'_{i,e}(a_1, \ldots, a_{n-1}, x) = p_{i,e}(a_1, \ldots, a_{n-1}, a_{n-1}, x).$$

Assume towards a contradiction that $\{p_{i,e}\}$ are linearly dependent over $\mathbb{F}(\mathbf{a})$. Equivalently, there exist polynomials $w_{i,e}(\mathbf{a})$, not all zero, such that

$$\sum_{i\in[m]}\sum_{j\in[s_i]} w_{i,e}(\mathbf{a})p_{i,e}(\mathbf{a},x)=0.$$

We may assume that the polynomials $\{w_{i,e}\}$ do not all have a common factor, as otherwise we can divide them by it. Let $w'_{i,e}(\mathbf{a})$ be obtained from $w_{i,e}(\mathbf{a})$ by substituting a_{n-1} for a_n. That is, $w'_{i,e}(a_1,\dots,a_{n-1})=w_{i,e}(a_1,\dots,a_{n-1},a_{n-1})$. Then we obtain

$$\sum_{i\in[m]}\sum_{j\in[s_i]} w'_{i,e}(\mathbf{a})p'_{i,e}(\mathbf{a},x)=0.$$

As the polynomials $\{p'_{i,e}\}$ are linearly independent over $\mathbb{F}(\mathbf{a})$, this implies that $w'_{i,e}\equiv 0$ for all i,e. That is, the polynomials $w_{i,e}$ satisfy

$$w_{i,e}(a_1,\dots,a_{n-1},a_{n-1})\equiv 0.$$

This implies that $(a_{n-1}-a_n)$ divides $w_{i,e}$ for all i,e, which is a contradiction to the assumption that $\{w_{i,e}\}$ do not all have a common factor. □

Lemma 2.5 implies that the vector $(1,\dots,1,0)$ belongs to $\mathcal{V}$. Without loss of generality, we may assume that it is v_m. This implies that $v_i(n)\geq 1$ for all $i\in[m-1]$, as otherwise we would have $v_i\leq v_m$, violating Lemma 2.1.

Lemma 2.6. *$n=k$.*

Proof. Let $v_m=(1,\dots,1,0)$. We know by (i) that $n-1=|v_m|\leq k-1$, so $n\leq k$. Assume towards a contradiction that $n<k$. Define a new set of vectors $\mathcal{V}'=\{v'_1,\dots,v'_m\}\subset\mathbb{N}^n$ as follows:

$$v'_1:=v_1,\dots,v'_{m-1}:=v_{m-1},v'_m:=(1,\dots,1,1).$$

In words, we increase the last coordinate of v_m by 1.

We claim that $\mathcal{V}'$ satisfies $V^*(k)$. It satisfies (i) by our assumption that $|v'_m|=n\leq k-1$, and it satisfies (iii) clearly. To show that it satisfies (ii), let $I\subseteq[m]$. If $m\notin I$ then it clearly satisfies (ii) for I, as it is the same constraint as for $\mathcal{V}$, so assume $m\in I$. In this case we have

$$\sum_{i\in I}(k-|v'_i|)+|v'_I|=\left(\sum_{i\in I}(k-|v_i|)-1\right)+(|v_I|+1)\leq k.$$

Note that $|P(k,\mathcal{V}')|=|P(k,\mathcal{V})|-1$. As $\mathcal{V}$ is a minimal counter-example, we have that $\mathcal{V}'$ satisfies $V^*(k)$. Let $p(\mathbf{a},x):=\prod_{j\in[n-1]}(x-a_j)$. The construction of $\mathcal{V}'$ satisfies that

$$P(k,\mathcal{V})=P(k,\mathcal{V}')\cup\{p\}.$$

Denote for simplicity of presentation the polynomials of $P(k,\mathcal{V}')$ by $p_1,\dots,p_{d-1}$, where $d=|P(k,\mathcal{V})|$. Assume that the polynomials $P(k,\mathcal{V})$ are linearly dependent. As $P(k,\mathcal{V}')$ are linearly independent, it implies that there exist polynomials $w, w_1, \ldots, w_{d-1} \in \mathbb{F}[\mathbf{a}]$, where $w \neq 0$, such that

$$w(\mathbf{a})p(\mathbf{a}, x) + \sum_{i=1}^{d-1} w_i(\mathbf{a})p_i(\mathbf{a}, x) \equiv 0.$$

Note that by construction, $v'_i(n) \geq 1$ for all $i \in [m]$. This implies that $p_1, \ldots, p_{d-1}$ are all divisible by $(x-a_n)$, while p is not. Substituting $x = a_n$ then gives $w \equiv 0$, a contradiction. $\square$

We can now reach a contradiction to $\mathcal{V}$ being a counter-example. We know that $v_m = (1, \ldots, 1, 0)$ with $|v_m| = n-1 = k-1$. Let $\mathcal{V}' = \{v_1, \ldots, v_{m-1}\}$. As it satisfies $V^*(k)$ we have that the polynomials $P(k, \mathcal{V}')$ are linearly independent. Moreover, as $|v_m| = k-1$ we have $P(k, v_m) = \{p\}$ where $p(\mathbf{a}, x) = \prod_{j \in [n-1]}(x - a_j)$. Note that all polynomials in $P(k, \mathcal{V}')$ are divisible by $(x - a_n)$, while p is not. So by the same argument as in the proof of Lemma 2.6, $P(k, v_m)$ cannot be linearly dependent of $P(k, \mathcal{V}')$. So $P(k, \mathcal{V})$ are linearly independent.

References

[DSDY13] Son Hoang Dau, Wentu Song, Zheng Dong, and Chau Yuen. Balanced sparsest generator matrices for MDS codes. In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, 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 *Information Theory (ISIT), 2014 IEEE International Symposium on*, pages 1787–1791. IEEE, 2014.

[HHYD14] Wael Halbawi, Tracey Ho, Hongyi Yao, and Iwan Duursma. Distributed Reed-Solomon codes for simple multiple access networks. In *Information Theory (ISIT), 2014 IEEE International Symposium on*, pages 651–655. IEEE, 2014.

[HS17] Anoosheh Heidarzadeh and Alex Sprintson. An algebraic-combinatorial proof technique for the GM-MDS conjecture. In *Information Theory (ISIT), 2017 IEEE International Symposium on*, pages 11–15. IEEE, 2017.

[YH18] Hikmet Yildiz and Babak Hassibi. Further progress on the GM-MDS conjecture for Reed-Solomon codes. *arXiv preprint arXiv:1801.07865*, 2018.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il