The prime case of the MDS conjecture

Simeon Ball
Presented by Joseph Briggs

Contents

1a: Introduction-The Singleton Bound

Singleton Bound. $k \leq n - d + 1$, for any $[n, k, d]$ code.
Proof. Any 2 codewords disagree in the first $n - d + 1$ coordinates somewhere, so there are $\leq q^{n-d+1}$ in total ■

Linear codes achieving equality are called *M*aximum Distance Separable (MDS) codes. A general question: given d and k, what is the greatest length n of an MDS code?

1b: MDS codes and generic subsets of $\mathbb{F}_q^k$

List k rows generating MDS code C as a $k \times n$ matrix A.
Claim. The columns of A give rise to a set S of n vectors, such that any $k = n - d + 1$ of them are LI. We call such an S *generic*.
Proof. Any k-dependence in columns

$$\Rightarrow \sum_{\delta \in K} c_\delta A_\delta = \mathbf{0}\,(|K| = k)$$

$$\Rightarrow \sum_{\delta \in K} c_\delta x_\delta = 0\,\forall \text{ rows } x \text{ of } A(\Rightarrow \forall x \in C).$$

So not all q^{n-d+1} choices for the $n - d + 1$ such $(x_\delta)_{\delta \in K}$ appear in C. Contradiction! ■
Conversely, any generic S gives rise to an MDS code of length $|S|$.

1c: (Supposedly) best example

We have a correspondence:
Length of MDS code $\leftrightarrow$Size of generic $S \subset \mathbb{F}_q^k$
Try RM codes! We know they meet the Singleton Bound.
$Enc : f \mapsto (f(a_1), \ldots, f(a_n))$ as an RS encoder needs to use *distinct* a_i, so we can obtain a length of up to $n = q$ by using all possible elements of $\mathbb{F}_q$.
Under this correspondence, the generic S obtained is the "normal rational curve" $\{(1, t, t^2, \ldots, t^{k-1}) : t \in \mathbb{F}_q\}$-any k such form a VDM matrix, hence are LI! We can add $(0, \ldots, 0, 1)$ to this S, reaching $n = q + 1$.

MDS Conjecture:

If $k \leq q$, then a generic $|S| \leq q + 1$. We prove case $k \leq p (= q)$.

2a: Segre's Tangent Function

Say $S \subset \mathbb{F}_p^k$ is generic. Then, if $Z \subset S$ has $|Z| = k-2$, consider the codimension-1 hyperplanes $\Sigma \supset Z$ with normal vectors v_Σ. We define a t-variable polynomial

$$T_Z(X) := \prod_{\Sigma \cap S = Z} < v_\Sigma, X > .$$

Then, if $\{x, y, z\} \cup Y \subset S$ is a basis, we have

$$\begin{aligned} & T_{Y\cup\{x\}}(y)\, T_{Y\cup\{y\}}(z)\, T_{Y\cup\{z\}}(x) \\ = (-1)^{t+1}\, & T_{Y\cup\{x\}}(z)\, T_{Y\cup\{y\}}(x)\, T_{Y\cup\{z\}}(y), \end{aligned}$$

where $t = p + k - 1 - |S|$.

2b: Interpolating T

For $E = \{a_1, \ldots, a_{t+2}\}$ and $|Y| = k-2$ disjoint in S,

$$0 = \sum_{a \in E} T_Y(a) \prod_{b \in E \setminus a} \det(b, a, Y)^{-1}$$

But all we needed was that $\{b, a\} \cup Y$ was a basis $\forall a \neq b \in E$. We never split up Y!

Idea: exchange elements of E and Y. More generally, if $Y = \{y_1, \ldots, y_{k-2}\}$,

$$0 = \sum_{a_1, \ldots, a_r \in E} \left(\prod_{i=1}^{r-1} \frac{T_{\theta_i}(a_i)}{T_{\theta_{i+1}(y_i)}} \right) T_{\theta_r}(a_r) \prod_{z \in E \cup Y \setminus (\theta_r \cup \{a_r\})} \frac{1}{\det(a_r, z, \theta_r)}$$

Here $\theta_i = (a_1, \ldots, a_{i-1}, y_i, \ldots, y_{k-2})$, as a set and a tuple.

2c: Using Segre's lemma to simplify the interpolation equation

Any order of $a_1, \ldots, a_r$ give the same term in the sum!
So, we have

$$0 = r! \sum_{a_1 < \cdots < a_r \in E} \prod_{i=1}^{r-1} \frac{T_{\theta_i}(a_i)}{T_{\theta_{i+1}(y_i)}} T_{\theta_r}(a_r) \prod_{z \notin \theta_r \cup \{a_r\}} \frac{1}{\det(a_r, z, \theta_r)}$$

Set $r = t + 2$ (use all of E). Then the above is a product of many nonzero elements of $\mathbb{F}_p$, together with $(t+2)!$, so $(t+2)! = 0$. Hence $p \leq t + 2 = p + k + 1 - |S|$, so $|S| \leq k + 1 \leq p + 1$ ■

3a: Caveats

If $r = t + 2 > k - 1$, we use θ_r...which only has $k - 2$ entries. But $t = q + k - 1 - |S|$.

If $|S| < t + k$, we have no room for disjoint $|E| = t + 2$ and $|Y| = k - 2$ in S. Here, we can use the "dual" generic set $S' \subset \mathbb{F}_q^{k'} = \mathbb{F}_q^{n-k}$ corresponding to the dual code, with $|S| = n = |S'|$. Then, if also $|S'| < t' + k'$, have

$$n < \frac{t + k' + t' + k}{2} = q - 1.$$

3b: Potential to generalise

The same argument gives, for $q > p$, that $|S| \leq q+k+1-\min\{k,p\}$. But we cannot hope to replace p by q in this proof because of the final step: $p! = 0$ in $\mathbb{F}_q$.

Nevertheless, in a follow-up paper, Ball relaxed the condition from $k \leq p$ to $k \leq 2p-2$, for MDS to hold.

Also, when $p = 2$ and $k = 3$ or $q-1$, the conjecture isn't quite true-instead $|S| \leq q+2$ is known. For $k = 3$ we may add $(0,1,0)$ to the aforementioned normal rational curve, making $q+2$ vectors in total-a "hyperoval". Similarly, when $k = q-1$, we may add e_{k-1}.

3c: The maximal examples

1. For the prime case, or more generally $k \leq p$, every such S of size $q+1$ is equivalent to the normal rational curve (with $(0,\ldots,0,1)$).
2. Constructions such as $\{(1, x, x^2 + \eta x^6, x^3, x^4) : x \in \mathbb{F}_9\}$ (Glynn, 1986) not containing the normal rational curve are known, but they are all (extensions of) RS codes.
3. The MDS conjecture only talks about $k \leq q$. $k > q$ allows for $|S| = k+1$ uniquely via $S = \{(\lambda_1, 0\ldots, 0), \ldots, (0, \ldots, 0, \lambda_k)\} \cup \{(1, \ldots, 1)\}$.