On the (linear) MDS conjecture

J. De Beule
(joint work with Simeon Ball and Ameera Chowdury)

Department of Mathematics
Vrije Universiteit Brussel

October 19th, 2015
Gent

Codes

- Alphabet A_q with $q \in \mathbb{N}$ characters,
- Words: concatenations of characters, preferably of a fixed length $n \in \mathbb{N}$
- Code C: collection of $M \in \mathbb{N}$ words
- If C is a q-ary code of length n (i.e. all words have length n), then $M \leq q^n$.
- *Hamming distance* between two codewords: number of positions in which the two words differ.

Coding/Decoding

Let C be a code of length n.

- Minimum distance of C, $d(C)$,
- determines the number of transmission errors that can be detected/corrected.

Fundamental problem of coding theory: construct codes with “optimized parameters”.

Linear codes

- The alphabet A_q is the set of elements of a finite field $\mathbb{F}_q$ of order q, $q = p^h$, p prime, $h \geq 1$.
- A linear q-ary code of length n is a subspace of $\mathbb{F}_q^n$.
- For a linear code C, its minimum distance equals its minimum weight.

The Singleton bound

Theorem (Singleton bound)

Let C be a q-ary (n, M, d) code. Then $M \leq q^{n-d+1}$.

Corollary

Let C be a linear $[n, k, d]$-code. Then $k \leq n - d + 1$.

Definition

A linear $[n, k, d]$ code C over $\mathbb{F}_q$ is an MDS code if it satisfies $k = n - d + 1$.

The Singleton bound

Theorem (Singleton bound)

Let C be a q-ary (n, M, d) code. Then $M \leq q^{n-d+1}$.

Corollary

Let C be a linear $[n, k, d]$-code. Then $k \leq n - d + 1$.

Definition

A linear $[n, k, d]$ code C over $\mathbb{F}_q$ is an MDS code if it satisfies $k = n - d + 1$.

Special sets of vectors

Lemma

An MDS code of dimension k and length n is equivalent with a set S of n vectors of $\mathbb{F}_q^r$ with the property that every r vectors of S form a basis of $\mathbb{F}_q^r$, with $r = n - k$.

Definition – Examples

Definition

An arc of a vector space $\mathbb{F}_q^r$ is a set S of vectors with the property that every r vectors of S form a basis of $\mathbb{F}_q^r$.

1. Let $\{e_1, \ldots, e_r\}$ be a basis of $\mathbb{F}_q^r$. Then $\{e_1, \ldots, e_r, e_1 + e_2 + \cdots + e_r\}$ is an arc of size $r + 1$.
2. Let $S = \{(1, t, t^2, \ldots, t^{r-1}) \| t \in \mathbb{F}_q\} \cup \{(0, 0, \ldots, 0, 1)\} \subset \mathbb{F}_q^r$. Then S is an arc of size $q + 1$.

One of the first results

Theorem (Bush 1952)

Let S be an arc of size n of $\mathbb{F}_q^r$, $r > q$. Then $n \leq q + 1$ and if $n = q + 1$, then S is equivalent to example (1)

From now on we may assume $r \leq q$.

One of the first results

Theorem (Bush 1952)

Let S be an arc of size n of $\mathbb{F}_q^r$, $r > q$. Then $n \leq q+1$ and if $n = q+1$, then S is equivalent to example (1)

From now on we may assume $r \leq q$.

The (linear) MDS conjecture

Conjecture

Let $r \leq q$. For an arc of size n in $\mathbb{F}_q^r$, $n \leq q+1$ unless $r = 3$ or $r = q-1$ and q is even, in which case $n \leq q+2$.

Questions of Segre (1955)

(i) Given r, q, what is the maximal value of l for which an l-arc exists?

(ii) For which values of r, q, $r \leq q$, is each $(q+1)$-arc in $\mathrm{PG}(r-1, q)$ a normal rational curve?

(iii) For a given r, q, $r < q$, which arcs of $\mathrm{PG}(r-1, q)$ are extendable to a $(q+1)$-arc?

Early results

In the following list, $q = p^h$, and we consider an l-arc in $\mathrm{PG}(r-1, q)$.

- Bose (1947): $l \leq q + 1$ if $p \geq r = 3$.
- Segre (1955): a $(q+1)$-arc in $\mathrm{PG}(2, q)$, q odd, is a conic.
- $q = 2$, $r = 3$: hyperovals are $(q+2)$-arcs.

more (recent) results

- Conjecture is known to be true for all $q \leq 27$, for all $r \leq 5$ and $k \geq q - 3$ and for $r = 6, 7, q - 4, q - 5$, see overview paper of J. Hirschfeld and L. Storme, pointing to results of Segre, J.A. Thas, Casse, Glynn, Bruen, Blokhuis, Voloch, Storme, Hirschfeld and Korchmáros.
- many examples of *hyperovals*, see e.g. Cherowitzo's hyperoval page, pointing to examples of Segre, Glynn, Payne, Cherowitzo, Penttila, Pinneri, Royle and O'Keefe.

more (recent) results

- An example of a $(q+1)$-arc in $\mathrm{PG}(4,9)$, different from a normal rational curve, (Glynn):

$$\mathcal{K} = \{(1,t,t^2+\eta t^6,t^3,t^4) \mid t \in \mathbb{F}_9, \eta^4 = -1\} \cup \{(0,0,0,0,1)\}$$

- An example of a $(q+1)$-arc in $\mathrm{PG}(3,q)$, $q=2^h$, $\gcd(r,h)=1$, different from a normal rational curve, (Hirschfeld):

$$\mathcal{K} = \{(1,t,t^{2^r},t^{2^r+1}) \mid t \in \mathbb{F}_q\} \cup \{(0,0,0,1)\}$$

Observations

Lemma

Let S be an arc of size n of $\mathbb{F}_q^r$. Let $Y \subset S$ be of size $r-2$. There are exactly $t = q + r - 1 - n$ hyperplanes of $\mathbb{F}_q^r$ with the property that $H \cap S = Y$.

Corollary

An arc of $\mathbb{F}_q^3$ has size at most $q + 2$.

Theorem (Segre)

An arc of $\mathbb{F}_q^3$, q odd, has size at most $q + 1$, in case of equality, it is equivalent with example (2).

arcs in $\mathrm{PG}(2, q)$

tangent lines through
$p_1 = (1, 0, 0)$: $X_1 = a_i X_2$
$p_2 = (0, 1, 0)$: $X_2 = b_i X_0$
$p_3 = (0, 0, 1)$: $X_0 = c_i X_1$

Lemma (B. Segre)

$$\prod_{i=1}^{t} a_i b_i c_i = -1$$

arcs in $\mathrm{PG}(2, q)$

tangent lines through
$p_1 = (1, 0, 0)$: $X_1 = a_i X_2$
$p_2 = (0, 1, 0)$: $X_2 = b_i X_0$
$p_3 = (0, 0, 1)$: $X_0 = c_i X_1$

Lemma (B. Segre)

$$\prod_{i=1}^{t} a_i b_i c_i = -1$$

Tangent functions

- Let S be an arc of $\mathbb{F}_q^r$, choose an arbitrary ordering on the elements, $|S| = n$.
- Let $A \subset S$ of size $r - 2$.
- Then there are $t = q + r - 1 - n$ tangent hyperplanes on A to S.
- Let α^i be t linear forms on $\mathbb{F}_q^r$ such that $\ker(\alpha^i)$ are these t tangent hyperplanes

Definition

For a subset $A \subset S$ of size $r - 2$, define its tangent function as

$$f_A(x) := \prod_{i=1}^{t} \alpha^i(x)$$

Interpolation

Let C be a subset of S of size $r-1$. Denote $d_C(x) := \det(x, C)$.

Lemma

Let $A \subset B \subset S$, $|B| = t + r - 1$. Then

$$f_A(x) = \sum_{e \in B \setminus A} f_A(e) \prod_{u \in B \setminus (A \cup e)} \frac{d_{A,u}(x)}{d_{A,u}(e)}$$

Interpolation

Corollary

Let $A \subset E \subset S$, $|E| = t + r$. Then

$$\sum_{e \in E \setminus A} f_A(e) \prod_{u \in E \setminus (A \cup e)} d_{A,e}(u)^{-1} = 0$$

Segre's lemma

Lemma (S. Ball, [1])

Let S be an arc of $\mathbb{F}_q^r$. For a subset $D \subset S$ of size $r-3$ and $\{x, y, z\} \subset S \setminus D$,

$$F_{D\cup\{x\}}(y)F_{D\cup\{y\}}(z)F_{D\cup\{z\}}(x) = (-1)^{t+1}F_{D\cup\{x\}}(z)F_{D\cup\{y\}}(x)F_{D\cup\{z\}}(y)$$

Theorem (Ball, [1])

Let S be an arc of $\mathbb{F}_q^r$, $r \leq q$. then

$$|S| \leq q + r + 1 - \min(r, p)$$

Segre's lemma

Lemma (S. Ball, [1])

Let S be an arc of $\mathbb{F}_q^r$. For a subset $D \subset S$ of size $r-3$ and $\{x,y,z\} \subset S \setminus D$,

$$F_{D\cup\{x\}}(y)F_{D\cup\{y\}}(z)F_{D\cup\{z\}}(x) = (-1)^{t+1}F_{D\cup\{x\}}(z)F_{D\cup\{y\}}(x)F_{D\cup\{z\}}(y)$$

Theorem (Ball, [1])

Let S be an arc of $\mathbb{F}_q^r$, $r \leq q$. then

$$|S| \leq q+r+1-\min(r,p)$$

The Segre product

Let $A \subset E \subset S$, $|E| = t + r$, define

$$g_A(x) := f_A(x) \prod_{u \in E \setminus (A \cup x)} d_{A,u}(x)^{-1}$$

Let F be the first $r - 2$ elements of E with respect to the ordering of S, define

$$\alpha_A := \prod_{i=1}^{s} \frac{g_{D \cup \{z_s, \ldots, z_i, x_{i-1}, \ldots, x_1\}}(x_i)}{g_{D \cup \{z_s, \ldots, z_{i+1}, x_i, \ldots, x_1\}}(z_i)}$$

where $D = A \cap F$, $A \setminus F = \{x_1, \ldots, x_s\}$ and $F \setminus A = \{z_1, \ldots, z_s\}$.

The Segre product

Theorem

Let $E \subset S$, $|E| = r + t$. For any subset A of E of size $r - 2$,

$$\sum \alpha_C = 0$$

where the sum runs over the subsets C of E of size $r - 1$ containing A.

Theorem (Ball, DB [2])

Let S be an arc of $\mathbb{F}_q^r$, $q = p^h$, p odd, $r \leq 2p - 2$. then

$$|S| \leq q + 1$$

Small dimensions

Consider the set $\{1, \ldots, n\}$. Define

- row indices: subsets of size a of $\{1, \ldots, n\}$
- column indices: subsets of size b of $\{1, \ldots, n\}$
- $I_n(a, b)$: matrix, has 1 in entry $(A, B) \iff A \subset B$ and 0 otherwise.

Define

$$T = \{i \mid 0 \leq i \leq b, \binom{a-i}{b-i} \neq 0 \mod p\}$$

Small dimensions

Lemma (Wilson's formula for the p-rank)

If $n \geq a + b$ then the p-rank of $I_n(a, b)$ is

$$\sum_{i \in T} \left(\binom{n}{i} - \binom{n}{i-1} \right)$$

MDS conjecture for $r \leq p$

Theorem

The MDS-conjecture is true for $r \leq p$.

MDS conjecture for $r \leq p$

Proof.

- We may assume that $r \leq \frac{|S|}{2}$
- Let $|S| = q + 2$, then $t = q + r - 1 - n = r - 3$
- Let $M = I_{r+t}(r-1, r-2)$, then M is a square matrix.
- Let v be a vector with entry α_C at position C, $C \subset E$, $|E| = r + t$.
- Then $vM = 0$ (this is $\sum \alpha_C = 0$)
- But M has full rank when $r \leq p$ and $\alpha_C \neq 0$, a contradiction

$\square$

slightly larger dimension

Generalize the “matrix approach”

- Let G be a subset of size $r+t+m$, $m>0$.
- row indices: subsets $C \subset G$, $|C| = r-1$
- column indices: pairs (A,U), $U \subset G$, $|U| = m$, $A \subset E(U) := G \setminus U$, $|A| = r-2$.
- entry $(C,(A,U))$ has value $\prod_{u \in U} \det(u, C)$.
- Call this matrix $M_{r-3}^{\uparrow m}$.

slightly larger dimension

Lemma

If v is a vector whose corrdinates are indexed by the subsets C of G of size $r-1$ and whose C coordinate is $\alpha_C \prod_{u \in U} \det(u, C)^{-1}$, then $vM_t^{\uparrow m} = 0$

Lemma

If $r \leq 2p-2$, there exists a vector of weight one in the column space of $M_{r-3}^{\uparrow 1}$

slightly larger dimension

Theorem (Ball, DB)

The MDS-conjecture is true for $r \leq 2p - 2$.

possible generalisations

we have actually observed that (for q odd)

- if $r \leq p$, then $M^{\uparrow 0}$ has full rank, which leads to a contradiction assuming the existence of a $q+2$-arc,
- if $r \leq 2p-2$, then $M^{\uparrow 1}$ has full rank, which leads to the above conclusion again.

Computational results indicate that for odd q, and $r \leq p + m(p-2)$, $M^{\uparrow m}$ has full rank. If this is the case, it could prove the MDS-conjecture for $r \leq q/3$ (and hence also for $r \geq 2q/3$.

possible generalisations

we have actually observed that (for q odd)

- if $r \leq p$, then $M^{\uparrow 0}$ has full rank, which leads to a contradiction assuming the existence of a $q+2$-arc,
- if $r \leq 2p-2$, then $M^{\uparrow 1}$ has full rank, which leads to the above conclusion again.

Computational results indicate that for odd q, and $r \leq p + m(p-2)$, $M^{\uparrow m}$ has full rank. If this is the case, it could prove the MDS-conjecture for $r \leq q/3$ (and hence also for $r \geq 2q/3$.

q even

Lemma (Segre (1967), Blokhuis, Bruen and Thas (1990))

Let S be an arc of $\mathbb{F}_q^r$, q even. Then there is a polynomial $\phi(v_1, \ldots, v_r)$ of degree t such that $\phi(C) = 0$ if $|C \cap S| = r - 2$.

It seems that this is connected with the Segre product!

Lemma

$\phi(C) = \alpha_C$ if $|C \cap S| = r - 1$.

q even

Lemma (Segre (1967), Blokhuis, Bruen and Thas (1990))

Let S be an arc of $\mathbb{F}_q^r$, q even. Then there is a polynomial $\phi(v_1, \ldots, v_r)$ of degree t such that $\phi(C) = 0$ if $|C \cap S| = r - 2$.

It seems that this is connected with the Segre product!

Lemma

$\phi(C) = \alpha_C$ *if* $|C \cap S| = r - 1$.

References

S. Ball, On sets of vectors of a finite vector space in which every subset of basis size is a basis, *Journal European Math. Soc.*, 14, 733–748, 2012

S. Ball, and J. De Beule. On sets of vectors of a finite vector space in which every subset of basis size is a basis II. *Des. Codes Cryptogr.*, 65(1–2):5–14, 2012.