Old and recent results on the linear MDS conjecture

J. De Beule
(joint work with Simeon Ball)

Department of Mathematics
Ghent University

April 24th, 2015
Zagreb

Linear codes

- Let C be a linear $[n, k, d]$-code with generator matrix G and parity check matrix H.

Lemma

A linear $[n, k]$ code has minimum distance d if and only if every $d - 1$ columns of H are linearly independent and there exists d linearly dependent columns.

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

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 $n \leq r + 1$ 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 $n \leq r + 1$ 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 $n \leq q+1$.

Questions of Segre (1955)

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

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

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

Questions of Segre (1955)

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

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

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

Questions of Segre (1955)

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

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

(iii) For a given $r-1, q$, $q > r$, 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 $\mathrm{PG}(3,q)$, $q = 2^h$, $\mathrm{gcd}(r,h) = 1$, 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 size n of $\mathbb{F}_q^r$.
- Choose a set $A \subset S$ of size $r-2$.
- Then there are $t = q + r - 1 - n$ tangent hyperplanes on A to S.
- Let f_A^i be t linear forms on $\mathbb{F}_q^r$ such that $\ker(f_A^i)$ are these t tangent hyperplanes

Definition

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

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

Generalization

Lemma (S. Ball, [1])

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

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

Interpolation

Lemma

For a subset $E \subset \mathbb{F}_q$ of size $t+1$ and $f \in \mathbb{F}_q[X]$, a polynomial of degree t,

$$f(X) = \sum_{e \in E} f(e) \prod_{y \in E \setminus \{e\}} \frac{X - y}{e - y}$$

Interpolation

Lemma

For a subset $E \subset \mathbb{F}_q^2$ of size $t+1$ with the property that $(u_1, u_2), (y_1, y_2) \in E$ implies $u_2 \neq 0$, $y_2 \neq 0$ and $\frac{u_1}{u_2} \neq \frac{y_1}{y_2}$ and $f \in \mathbb{F}_q[X_1, X_2]$, a homogenous polynomial of degree t,

$$f(X_1, X_2) = \sum_{(e_1,e_2)\in E} f(e_1, e_2) \prod_{(y_1,y_2)\in E\setminus\{(e_1,e_2)\}} \frac{y_2 X_1 - y_1 X_2}{e_1 y_2 - y_1 e_2}$$

Interpolation

Corollary

For a subset $E \subset \mathbb{F}_q^2$ of size $t+2$ with the property that $(u_1, u_2), (y_1, y_2) \in E$ implies $u_2 \neq 0$, $y_2 \neq 0$ and $\frac{u_1}{u_2} \neq \frac{y_1}{y_2}$ and $f \in \mathbb{F}_q[X_1, X_2]$, a homogenous polynomial of degree t,

$$\sum_{(x_1,x_2)\in E} f(x_1, x_2) \prod_{y_1,y_2\in E\setminus\{(x_1,x_2)\}} (x_1 y_2 - y_1 x_2)^{-1} = 0$$

Interpolation of tangent functions

Lemma

Let S be an arc of $\mathbb{F}_q^k$. Let $A \subset S$ be a subset of size $k-2$. Then for every subset $E \subset S \setminus A$ of size $t+2$,

$$\sum_{x \in E} F_A(x) \prod_{y \in E \setminus \{x\}} \det(x, y, A)^{-1} = 0$$

Generalization

Lemma (S. Ball, [1])

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

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

Using the generalization

Lemma

Let S be an arc of $\mathbb{F}_q^k$. For a subset $D \subset S$ of size $k-4$ and $\{x_1, x_2, x_3, z_1, z_2\} \subset S \setminus D$, switching x_1 and x_2, or switching x_2 and x_3, or switching z_1 and z_2 in

$$\frac{F_{D\cup\{z_1,z_2\}}(x_1)F_{D\cup\{z_2,x_1\}}(x_2)F_{D\cup\{x_1,x_2\}}(x_3)}{F_{D\cup\{z_2,x_1\}}(z_1)F_{D\cup\{x_1,x_2\}}(z_2)}$$

changes the sign by $(-1)^{t+1}$.

The Segre product

- Let $r \in \{1, \dots, k-2\}$.
- Let $D \subset S$ of size $k-2-r$ and let $A = \{x_1, \dots, x_{r+1}\}$ and $B = \{z_1, \dots, z_r\}$ be disjoint.

Definition

$$P_D(A, B) :=$$

$$\frac{F_{D \cup \{z_r, \dots, z_1\}}(x_1) F_{D \cup \{z_r, \dots, z_2, x_1\}}(x_2) \cdots F_{D \cup \{z_r, x_{r-1} \dots, x_1\}}(x_r) F_{D \cup \{x_r, \dots, x_1\}}(x_{r+1})}{F_{D \cup \{z_r, \dots, z_2, x_1\}}(z_1) \cdots F_{D \cup \{z_r, x_{r-1} \dots, x_1\}}(z_{r-1})}$$

Exploiting the lemma of tangents

Lemma

Let $D \subset S$ be of size $k-2-r$ and let $A = \{x_1, \dots, x_{r+1}\}$ or $A = \{x_1, \dots, x_r\}$ and $B = \{z_1, \dots, z_r\}$ be disjoint subsets of $S \setminus D$. Switching the order in A (or B) by a transposition changes the sign of $P_D(A, B)$ by $(-1)^{t+1}$.

One more notation

For any subset B of an ordered set L, let $\sigma(B, L)$ be $(t+1)$ times the number of transpositions needed to order L so that the elements of B are the last $|B|$ elements.

Exploiting the Segre product

Lemma

Let A of size n, L of size r, D of size $k-1-r$ and Ω of size $t+1-n$ be pairwise disjoint subsequences of S. If $n \leq r \leq n+p-1$ and $r \leq t+2$, where $q = p^h$, then

$$\sum_{\substack{B \subseteq L \\ |B|=n}} (-1)^{\sigma(B,L)} P_{D \cup (L \setminus B)}(A, B) \prod_{z \in \Omega \cup B} \det(z, A, L \setminus B, D)^{-1} =$$

$$(-1)^{(r-n)(nt+n+1)} \sum_{\substack{\Delta \subseteq \Omega \\ |\Delta|=r-n}} P_D(A \cup \Delta, L) \prod_{z \in (\Omega \setminus \Delta) \cup L} \det(z, A, \Delta, D)^{-1}.$$

Theorem (S. Ball, [1])

If $k \leq p$ then $|S| \leq q+1$.

Proof.

- We may assume $k+t \leq q+2$.
- Apply previous lemma with with $r = t+2 = k-1$ and $n = 0$ and get
$$\prod_{z \in \Omega} \det(z, L)^{-1} = 0,$$
which is a contradiction.

□

A generalization

Theorem (S. Ball and JDB, [2])

If q is non-prime and $k \leq 2p - 2$, then $|S| \leq q + 1$.

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.