Segre's lemma of tangents and linear MDS codes

J. De Beule
(joint work with Simeon Ball)

Department of Mathematics
Ghent University
Department of Mathematics
Vrije Universiteit Brussel

June, 2013
Journées estivales de la Méthode Polynomiale
Lille

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.

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.

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.

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.

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.

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".

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 sub vector space 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). 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 $k = n - d + 1$.

Is there an upper bound on d (for fixed k and q)?

The Singleton bound

Theorem (Singleton bound)

Let C be a q-ary (n, M, d). 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 $k = n - d + 1$.

Is there an upper bound on d (for fixed k and q)?

The Singleton bound

Theorem (Singleton bound)

Let C be a q-ary (n, M, d). 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 $k = n - d + 1$.

Is there an upper bound on d (for fixed k and q)?

Special sets of vectors

Definition

Let C be an $[n, k, d]$ code. An $k \times n$ matrix is a generator matrix for C if and only if C is the row space of G.

Lemma

An $k \times n$ matrix is a generator matrix of an MDS code if and only if every subset of k columns of G is linearly independent.

Corollary

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

Special sets of vectors

Definition

Let C be an $[n, k, d]$ code. An $k \times n$ matrix is a generator matrix for C if and only if C is the row space of G.

Lemma

An $k \times n$ matrix is a generator matrix of an MDS code if and only if every subset of k columns of G is linearly independent.

Corollary

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

Special sets of vectors

Definition

Let C be an $[n,k,d]$ code. An $k \times n$ matrix is a generator matrix for C if and only if C is the row space of G.

Lemma

An $k \times n$ matrix is a generator matrix of an MDS code if and only if every subset of k columns of G is linearly independent.

Corollary

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

Definition – Examples

Definition

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

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

Definition – Examples

Definition

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

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

Bound on the size of arcs (case 1)

When $k \geq q+1$, example (1) is *better* than (2).

Theorem (Bush 1952)

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

Bound on the size of arcs (case 1)

When $k \geq q+1$, example (1) is *better* than (2).

Theorem (Bush 1952)

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

The MDS conjecture

Conjecture

Let $k \geq q$. For an arc of size n in $\mathbb{F}_q^k$, $n \leq q+1$ unless $k=3$ or $k=q-1$ 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 $k-1, q, q > k$, is each $(q+1)$-arc in $\mathrm{PG}(k-1, q)$ a normal rational curve?

(iii) For a given $k-1, q, q > k$, which arcs of $\mathrm{PG}(k-1, q)$ 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 $k-1, q$, $q > k$, is each $(q+1)$-arc in $\mathrm{PG}(k-1, q)$ a normal rational curve?

(iii) For a given $k-1, q$, $q > k$, which arcs of $\mathrm{PG}(k-1, q)$ 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 $k-1, q$, $q > k$, is each $(q+1)$-arc in $\mathrm{PG}(k-1, q)$ a normal rational curve?

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

Observations

Lemma

Let S be an arc of size n of $\mathbb{F}_q^k$. Let $Y \subset S$ be of size $k-2$. There are exactly $t = q+k-1-n$ hyperplanes of $\mathbb{F}_q^k$ 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).

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,

$$f(X_1, X_2) = \sum_{(e_1,e_2)\in E} f(e_1, e_2) \prod_{(y_1,y_2)\in E\setminus\{(e_1,e_2)\}} \frac{y_2X_1 - y_1X_2}{e_1y_2 - y_1e_2}$$

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,

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

Tangent functions

- Let S be an arc of size n of $\mathbb{F}_q^k$.
- Choose a set $A \subset S$ of size $k-2$.
- Then there are $t = q + k - 1 - n$ tangent hyperplanes on A to S.
- Let f_A^i be t linear forms on $\mathbb{F}_q^k$ such that $\ker(f_A^i)$ are these t tangent hyperplanes

Definition

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

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

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

Definition

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

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

Exploiting the lemma of tangents

Lemma

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