Old and new results on the MDS-conjecture

J. De Beule
(joint work with Simeon Ball)

Department of Mathematics
Ghent University

February 9, 2012
Incidence Geometry and Buildings 2012

Definitions

Definition

An arc of a projective space $\mathrm{PG}(k-1,q)$ is a set $\mathcal{K}$ of points such that no k points of $\mathcal{K}$ are incident with a common hyperplane. An arc $\mathcal{K}$ is also called a n-arc if $|\mathcal{K}| = n$.

Definition

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

Lemma

Suppose that C is a linear $[n, k, d]$ over $\mathbb{F}_q$ with parity check matrix H. Then C is an MDS-code if and only if every collection of $n - k$ columns of H is linearly indepent.

Corollary

Linear MDS codes are equivalent with arcs in projective spaces.

Lemma

Suppose that C is a linear $[n, k, d]$ over $\mathbb{F}_q$ with parity check matrix H. Then C is an MDS-code if and only if every collection of $n - k$ columns of H is linearly indepent.

Corollary

Linear MDS codes are equivalent with arcs in projective spaces.

fundamental questions

- What is the largest size of an arc in $\mathrm{PG}(k-1,q)$?
- For which values of $k-1, q$, $q > k$, is each $(q+1)$-arc in $\mathrm{PG}(k-1,q)$ a normal rational curve?

$$\{(1,t,\ldots,t^{k-1}) \mid t \in \mathbb{F}_q\} \cup \{(0,\ldots,0,1)\}$$

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

Early results

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

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

Lemma (Bush, 1952)

An arc in $\mathrm{PG}(k-1, q)$, $k \geq q$, has size at most $k+1$. An arc attaining this bound is equivalent to a frame of $\mathrm{PG}(k-1, q)$.

- $q = 2$, $k = 3$: hyperovals are $(q+2)$-arcs.

MDS-conjecture

Conjecture

An arc of $\mathrm{PG}(k-1,q)$, $k \leq q$, has size at most $q+1$, unless q is even and $k=3$ or $k=q-1$, in which case it has size at most $q+2$.

more (recent) results

- Conjecture is known to be true for all $q \leq 27$, for all $k \leq 5$ and $k \geq q-3$ and for $k = 6, 7, q-4, q-5$, 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):

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

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)

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

coordinate free version

$$T_{\{p_1\}} := \prod(X_1 - a_i X_2)$$
$$T_{\{p_2\}} := \prod(X_2 - b_i X_0)$$
$$T_{\{p_3\}} := \prod(X_0 - c_i X_1)$$

Lemma

$$T_{\{p_1\}}(p_2)T_{\{p_2\}}(p_3)T_{\{p_3\}}(p_1) = (-1)^{t+1}T_{\{p_1\}}(p_3)T_{\{p_2\}}(p_1)T_{\{p_3\}}(p_2)$$

coordinate free version in $\mathrm{PG}(k-1, q)$

Lemma (S. Ball)

Choose $S \subset \mathcal{K}$, $|S| = k-3$, *choose* $p_1, p_2, p_3 \in \mathcal{K} \setminus S$.

$$T_{S\cup\{p_1\}}(p_2)T_{S\cup\{p_2\}}(p_3)T_{S\cup\{p_3\}}(p_1)$$
$$= (-1)^{t+1}T_{S\cup\{p_1\}}(p_3)T_{S\cup\{p_2\}}(p_1)T_{S\cup\{p_3\}}(p_2)$$

Interpolation

Lemma (S. Ball)

Let $|\mathcal{K}| \geq k + t > k$. *Choose* $Y = \{y_1, \ldots, y_{k-2}\} \subset \mathcal{K}$ *and* $E \subset \mathcal{K} \setminus Y$, $|E| = t + 2$. *Then*

$$0 = \sum_{a \in E} T_Y(a) \prod_{z \in E \setminus \{a\}} det(a, z, y_1, \ldots, y_{k-2})^{-1}$$

Exploiting interpolation and Segre's lemma

Let $|\mathcal{K}| \geq k + t > k$. Choose $Y = \{y_1, \ldots, y_{k-2}\} \subset \mathcal{K}$ and $E \subset \mathcal{K} \setminus Y$, $|E| = t + 2$, $r \leq \min(k-1, t+2)$. Let $\theta_i = (a_1, \ldots, a_{i-1}, y_i, \ldots, y_{k-2})$ denote an ordered sequence, for the elements $a_1, \ldots, a_{i-1} \in E$

Lemma (S. Ball)

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

The $r!$ terms in the sum for which $\{a_1, \ldots, a_r\} = A$, $A \subset E$, $|A| = r$, are the same.

Exploiting interpolation and Segre's lemma

Let $|\mathcal{K}| \geq k + t > k$. Choose $Y = \{y_1, \ldots, y_{k-2}\} \subset \mathcal{K}$ and $E \subset \mathcal{K} \setminus Y$, $|E| = t + 2$, $r \leq \min(k-1, t+2)$. Let $\theta_i = (a_1, \ldots, a_{i-1}, y_i, \ldots, y_{k-2})$ denote an ordered sequence, for the elements $a_1, \ldots, a_{i-1} \in E$

Lemma (S. Ball)

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

avoiding some restriction

Lemma

Suppose that $\mathcal{K}$ is an arc in $\mathrm{PG}(k-1,q)$, then one can construct an arc $\mathcal{K}'$ in $\mathrm{PG}(|\mathcal{K}|-k-1,q)$, with $|\mathcal{K}|=|\mathcal{K}'|$.

Segre product

Let $A = (a_1, \ldots, a_n)$ and $B = (b_0, \ldots, b_{n-1})$ be two subsequences of $\mathcal{K}$ of the same length n and let D be a subset of $\mathcal{K} \setminus (A \cup B)$ of size $k - n - 1$.

Definition

$$P_D(A, B) = \prod_{i=1}^{n} \frac{T_{D \cup \{a_1, \ldots, a_{i-1}, b_i, \ldots, b_{n-1}\}}(a_i)}{T_{D \cup \{a_1, \ldots, a_{i-1}, b_i, \ldots, b_{n-1}\}}(b_{i-1})}$$

and $P_D(\emptyset, \emptyset) = 1$.

Using Segre's lemma again

Lemma

$$P_D(A^*, B) = (-1)^{t+1} P_D(A, B),$$

$$P_D(A, B^*) = (-1)^{t+1} P_D(A, B),$$

where the sequence X^* is obtained from X by interchanging two elements.

Interpolation again

- Suppose that $|\mathcal{K}| = q + 2$.
- Let L of size $p - 1$, Ω of size $p - 2$, X and Y both of size $k - p$ be disjoint ordered sequences of $\mathcal{K}$. Let S_τ denote the sequence $(s_{\tau(i)} \mid i \in \tau)$, $\tau \subseteq \{1, 2, \ldots, |S|\}$ for any sequence S.
- Let $\sigma(X_\tau, X)$ denote the number of transpositions needed to map X onto X_τ.
- $M = \{1, \ldots, k - p\}$

Lemma

$$0 = \sum_{\tau \subseteq M} (-1)^{|\tau| + \sigma(X_\tau, X)} P_{L \cup X_{M \setminus \tau}}(Y_\tau, X_\tau) \prod_{z \in \Omega \cup X_\tau \cup Y_{M \setminus \tau}} \det(z, X_{M \setminus \tau}, Y_\tau, L)^{-1}$$

Interpolation again

- Let $E \subset \Omega$, $|E| = 2p - k - 2$.
- Let $W = (w_1, \ldots, w_{2n})$ be an ordered subssequence of $\mathcal{K}$ disjoint from $L \cup X \cup Y \cup E$.

Corollary

$$0 = \prod_{i=1}^{n} \det(y_{n+1-i}, X, L) \prod_{z \in E \cup Y \cup W_{2n}} \det(z, X, L)^{-1}$$

...which is a contradiction

Corollary (Ball and DB)

An arc in $\mathrm{PG}(k-1, q)$, $q = p^h$, p prime, $h > 1$, $k \leq 2p - 2$ has size at most $q + 1$.

- B. Cherowitzo.
  Bill Cherowtizo's Hyperoval Page.
  http://www-math.cudenver.edu/~wcherowi/research/
  1999.

- J. W. P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces: update 2001, in *Developments in Mathematics*, **3**, Kluwer Academic Publishers. *Finite Geometries*, Proceedings of the *Fourth Isle of Thorns Conference*, pp. 201–246.