MDS codes, arcs and tensors

Michel Lavrauw

Sabancı University

based on joint work with Simeon Ball

MDS codes

Let A be a set of size q (the alphabet).

A code $C \subseteq A^n$ has minimum distance d if any two n-tuples in C differ in at least d coordinates.

[Singleton bound] $|C| \leqslant q^{n-d+1}$.

A code for which $|C| = q^{n-d+1}$ is called maximum distance separable (MDS).

MDS codes appear in quantum mechanics, distributed storage systems, burst error-correction codes, representation of matroids, threshold sharing schemes.

We are interested in linear codes: $C \leq \mathbb{F}_q^n$ of dimension k.

A well-known example of an MDS code: Reed-Solomon code.

How many errors can a code correct?

Fixing k and q, how large can d (or $n = d + k - 1$) be?

The larger d, the more errors we can correct/detect.

Example: *Let G be an abelian group of size q. Then*

$$C = \{(a_1, \ldots, a_k, a_1 + \cdots + a_k) \mid a_i \in G\}$$

is an MDS code with $n = k + 1$ and $d = 2$.

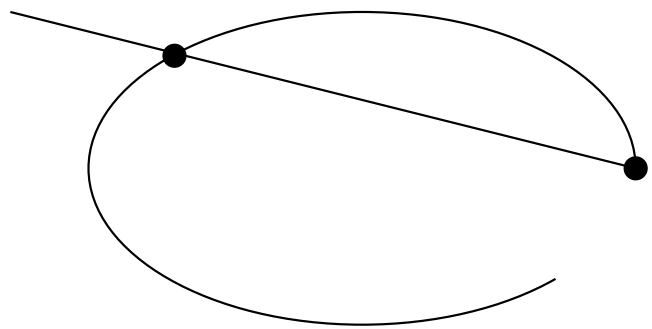
The "trivial" bound $n \leqslant q + k - 1$ can be obtained using elementary projective geometry over $\mathbb{F}_q$.

Arcs

Arcs in $\mathrm{PG}(k-1,q)$

An arc in $\mathrm{PG}(k-1,q)$ is a set of points no k in a hyperplane.

An arc in $\mathrm{PG}(2,q)$ is called a planar arc.



Examples of arcs

1. a frame (basis + all-1-vector) in $\mathrm{PG}(k-1,q)$ (size $k+1$)

2. a conic in a plane $\quad (\nu_2(\mathbb{P}^1))$

$$\{(1,t,t^2) \ : \ t \in \mathbb{F}_q\} \cup \{(0,0,1)\}$$

3. a normal rational curve (NRC) $\quad (\nu_{k-1}(\mathbb{P}^1))$

$$\{(1,t,t^2,\ldots,t^{k-1}) \ : \ t \in \mathbb{F}_q\} \cup \{(0,0,\ldots,0,1)\}$$

Exercise 1: Prove that these are arcs.

Exercise 2: Which of these examples is complete?

Arc $\mathcal{A} \leftrightarrow$ MDS code $C_{\mathcal{A}}$

Theorem

The linear code $C_{\mathcal{A}}$ generated by the matrix whose columns are the vectors of an arc $\mathcal{A}$ is a linear MDS code, and vice versa, the set of columns of a generator matrix of a linear MDS code is an arc.

The code $C_{\mathcal{A}}$ has parameters $[n, k, n-k+1]$ where $n = |\mathcal{A}|$.

Example:

NRC (size $q+1$) $\leftrightarrow$ Reed-Solomon code $[q+1, k, q-k+2]$

The main conjecture (MDS conjecture)

How large can an arc $\mathcal{A}$ in $\mathrm{PG}(k-1,q)$ be?

Exercise 3: Show that $|\mathcal{A}| = k+1$ is the best you can do if $q \leq k$.

From now on assume $q \geq k+1$.

MDS conjecture (B. Segre 1950's):

$\mathcal{A}$ cannot be larger than NRC (except if q even and $k \in \{3, q-2\}$)

(q even, $k=3$, allows planar arcs of size $q+2$: hyperovals)

The main conjecture (MDS conjecture)

The MDS conjecture is still open!

Most results rely on planar arcs (by projection methods) based on induction arguments from [Segre1955] and [Kaneta and Maruta 1989].

The results by Segre, Hirschfeld-Korchmáros, and Voloch rely on Segre's envelope associated to a planar arc in combination with the Hasse-Weil theorem or the Stöhr-Voloch theorem.

The MDS conjecture is known to be true for the following k. (bounds given only up to first order of magnitude, p is prime.)

$k < \sqrt{q}$, q even [Segre 1967]

$k < \sqrt{pq}$, $q = p^{2h+1}$ [Voloch 1991]

$k < q$, $q = p$ [Ball 2012]

$k < 2\sqrt{q}$, $q = p^2$ [Ball and De Beule 2012]

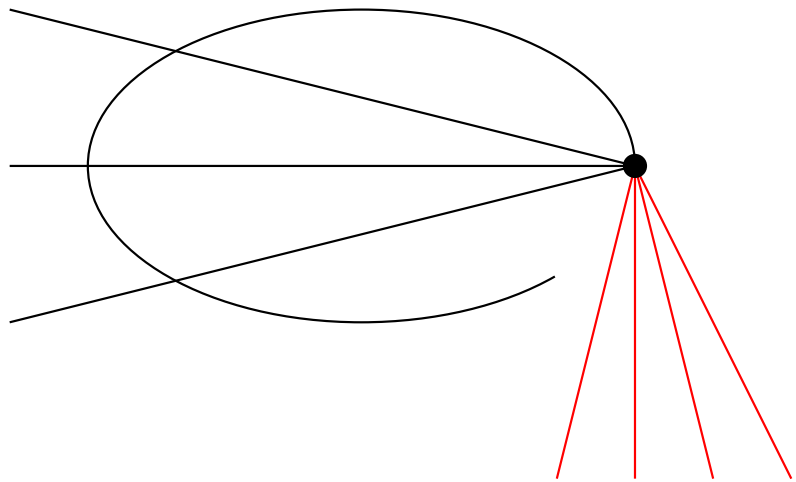
$k < \sqrt{q}$, $q = p^{2h}$ [Ball and Lavrauw 2018]

There are other bounds from Segre, Voloch and Hirschfeld and Korchmáros which are better for smaller q.

The algebraic envelope associated to a planar arc

Segre proved that the set of tangents to an arc $\mathcal{A}$ in $\mathrm{PG}(2, q)$ form an algebraic envelope $\mathcal{E}_{\mathcal{A}}$ of degree t for q even, and of degree $2t$ for q odd, where

$t =$ the number of tangents through a point of $\mathcal{A}$.



Combining $\mathcal{E}_{\mathcal{A}}$ with the Hasse-Weil theorem and the Stöhr-Voloch theorem lead to the bounds on the size of complete planar arcs.

The algebraic envelope $\mathcal{E}_{\mathcal{A}}$, q even

For q even, the algebraic envelope $\mathcal{E}_{\mathcal{A}}$ has degree t.

Combining $\mathcal{E}_{\mathcal{A}}$ with the Hasse-Weil theorem, Segre proved that

$$N(q) \leq q - \sqrt{q} + 1.$$

$N(q) =$ size of the second largest complete arc in $\mathrm{PG}(2, q)$.

The examples by Kestenband from 1981 (intersection of Hermitian curves) imply that this bound is tight if q is a square.

The algebraic envelope $\mathcal{E}_{\mathcal{A}}$, q odd

For q odd, the algebraic envelope $\mathcal{E}_{\mathcal{A}}$ has degree $2t$. The Hasse-Weil theorem and the Stöhr-Voloch theorem lead to the following results.

For q prime, Voloch (1990) proved $N(q) \leq \frac{44}{45}q + \frac{8}{9}$.

For q non-square, Voloch (1991) proved
$N(q) \leq q - \frac{1}{4}\sqrt{pq} + \frac{29}{16}p - 1$.

Hirschfeld and Korchmáros (1996) proved that
$N(q) \leq q - \frac{1}{2}\sqrt{q} + 5$ (provided that the characteristic is at least 5)
improved to
$N(q) \leq q - \frac{1}{2}\sqrt{q} + 3$ (provided that $q \geqslant 529$ and $q \neq 3^6, 5^5$)
by same authors in 1998.

Algebraic hypersurface associated to an arc in $\mathrm{PG}(k-1,q)$

Several generalisations were proven of Segre's envelope.

Blokhuis-Bruen-Thas: On M.D.S. codes, arcs in $\mathrm{PG}(n,q)$ with q even, and a solution of three fundamental problems of B. Segre. *Invent. Math.* (1988).

Blokhuis-Bruen-Thas: Arcs in PG(n,q), MDS-codes and three fundamental problems of B. Segre : some extensions. *Geometriae Dedicata* (1990)

Blokhuis-Cameron-Thas: On a generalization of a theorem of B. Segre. *Geometriae Dedicata* (1992).

Crucial ingredient: Lemma of tangents

All of the previous results fall back on the Lemma of tangents, which describes the relation between the set of (combinatorial) tangent lines at three different points of an arc in terms of an algebraic formula.

For a planar arc of size $q+1$ this says that the triangles Δabc and ΔABC are in perspective.

Tensors

Lemma (Scaled coordinate-free lemma of tangents)

Let $\mathcal{A}$ be an arc in $\mathrm{PG}(k-1,q)$, with tangent hypersurfaces given as the zero loci of the forms $f_S(X)$ as defined in (1) and scaled as in (2), and let g be the function as defined in (3). If σ is a permutation in $\mathrm{Sym}(k-1)$ and T is a $(k-1)$-subset of $\mathcal{A}$ then

$$g(T^\sigma) = (-1)^{s(t+1)} g(T),$$

where s is the parity of the permutation σ.

$$f_S(X) = \prod_{i=1}^{t} \alpha_i(X), \tag{1}$$

$$f_S(e) = (-1)^{s(t+1)} f_{S\cup\{e\}\setminus\{a\}}(a), \tag{2}$$

$$g(S \cup \{a\}) = (-1)^{s(t+1)} f_S(a), \tag{3}$$

A tensor associated to an arc

Let $\nu_{k,t}$ denote the degree t Veronese map on $\mathrm{PG}(k-1,q)$.

We define a function h from

$$\nu_{k,t}(\mathcal{A}) \times \nu_{k,t}(\mathcal{A}) \times \ldots \times \nu_{k,t}(\mathcal{A}) \quad (k-1 \text{ factors})$$

to $\mathbb{F}_q$ by

$$h(\nu_{k,t}(a_1), \nu_{k,t}(a_2), \ldots, \nu_{k,t}(a_{k-1})) := g(a_1, a_2, \ldots, a_{k-1}). \quad (4)$$

and show that h extends to a multilinear form on $\langle \nu_{k,t}(\mathcal{A}) \rangle^{\otimes k-1}$.

Theorem (Ball-Lavrauw 2019)

There exists a homogeneous polynomial $F(Y_1, \ldots, Y_{k-1})$ (in $k(k-1)$ variables) where $Y_j = (Y_{j1}, \ldots, Y_{jk})$, and F is homogeneous of degree t in each of the k-tuples of variables Y_j, with the following properties.

(i) *For every $(k-2)$-subset $S = [a_1, \ldots, a_{k-2}]$ of the arc $\mathcal{A}$ we have $F(a_1, \ldots, a_{k-2}, X) = (-1)^{s(t+1)} f_S(X)$ modulo $\Phi_t[X]$, where s is the parity of the permutation which orders S as in the ordering of $\mathcal{A}$.*

(ii) *For every sequence $a_1, \ldots, a_{k-1}$ of elements of $\mathcal{A}$ in which points are repeated, $F(a_1, \ldots, a_{k-1}) = 0$.*

(iii) *For every permutation $\sigma \in \mathrm{Sym}(k-1)$,*

$$F(Y_{\sigma(1)}, \ldots, Y_{\sigma(k-1)}) = (-1)^{s(t+1)} F(Y_1, \ldots, Y_{k-1}),$$

modulo $\Phi_t[Y_1], \ldots, \Phi_t[Y_{k-1}]$, where s is the parity of σ.

(iv) *Any form $F(Y_1, \ldots, Y_{k-1})$ satisfying (i), (ii) and (iii) is unique modulo $\Phi_t[Y_1]$, $\ldots$, $\Phi_t[Y_{k-1}]$.*

This extends the planar arc result:

Theorem (Ball-Lavrauw 2018)

Let $\mathcal{A}$ be an arc of size $q+2-t$ of $\mathrm{PG}(2,q)$. If $\mathcal{A}$ is not contained in a curve of degree t, then there is a (t,t)-form $F(X,Y) \in \mathbb{F}_q[X,Y]$ such that

$$F(X,y) = f_y(X),$$

for all $y \in \mathcal{A}$.

Theorem (Segre 1955)

An arc in $\mathrm{PG}(2,q)$, q odd, of size $q+1$ is a conic.

Proof $|\mathcal{A}| = q+1 \Rightarrow t = 1 \Rightarrow F(X,Y)$ is a bilinear form with $F(y,y) = 0$, $\forall y \in \mathcal{A} \Rightarrow \mathcal{A}$ is a conic. □

Results from [Ball-Lavrauw 2018]

$N(q) =$ size of the second largest complete arc in $\mathrm{PG}(2, q)$.

Theorem (A)

If q is odd and a square then $N(q) < q - \sqrt{q} + \sqrt{q}/p + 3$, and if q is prime then $N(q) < q - \sqrt{q} + 7/2$.

Corollary (MDS conjecture for $k \leq \sqrt{q} - \sqrt{q}/p + 2$)

If $k \leqslant \sqrt{q} - \sqrt{q}/p + 2$ and $q = p^{2h}$, p odd, then an arc of $\mathrm{PG}(k-1, q)$ has size at most $q + 1$.

Sketch of the proof of Theorem (A)

Theorem (A) is a corollary of our main result:

Theorem (B)

Let $\mathcal{A}$ be a planar arc of size $q+2-t$, q odd, not $\mathcal{A} \subseteq$ conic.

(i) If $\mathcal{A}$ is not contained in a curve of degree t then $\mathcal{A}$ is contained in the intersection of two curves of degree at most $t + p^{\lfloor \log_p t \rfloor}$ which do not share a common component.

(ii) If $\mathcal{A}$ is contained in a curve ϕ of degree t and

$$p^{\lfloor \log_p t \rfloor}(t + \tfrac{1}{2}p^{\lfloor \log_p t \rfloor} + \tfrac{3}{2}) \leqslant \tfrac{1}{2}(t+2)(t+1)$$

then there is another curve of degree at most $t + p^{\lfloor \log_p t \rfloor}$ which contains $\mathcal{A}$ and shares no common component with ϕ.

The existence of a curve of degree t containing $\mathcal{A}$ (part (ii)) complicates the proof. We restrict ourselves to part (i):

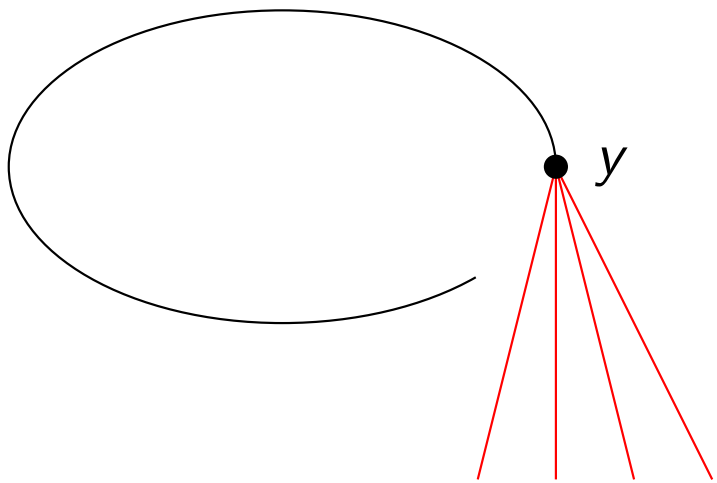
If $\mathcal{A}$ is not contained in a curve of degree t then it is contained in the intersection of two curves of degree at most $t + p^{\lfloor \log_p t \rfloor}$ which do not share a common component.

The crucial part is the existence of the (t, t)-form obtained from the scaled coordinate-free version of Segre's lemma of tangents.

A polynomial in $\mathbb{F}_q[X, Y]$ is called a (t, t)-form if it is simultaneously homogeneous of degree t in both sets of variables $X = (X_1, X_2, X_3)$ and $Y = (Y_1, Y_2, Y_3)$.

Lemma (1)

There exists a (t, t)-form $F(X, Y) \in \mathbb{F}_q[X, Y]$ such that for each $y \in \mathcal{A}$, the curve defined by $F(X, y)$ is the union of the t tangent lines of $\mathcal{A}$ at y.



For each $w = (i, j, k) \in \{0, \ldots, t-1\}^3$ where $i + j + k \leqslant t - 1$, define $\rho_w(Y)$ to be the coefficient of $X_1^i X_2^j X_3^k$ in

$$F(X + Y, Y) - F(X, Y).$$

Observe that the degree of $\rho_w(Y)$ is $2t - i - j - k$.

Since

$$F(X, y) = F(X + y, y)$$

for all $y \in \mathcal{A}$, we have that $\rho_w(y) = 0$ for all $y \in \mathcal{A}$.

The curves defined by the $\rho_w(Y)$'s are then used to prove that one of the following conditions holds:

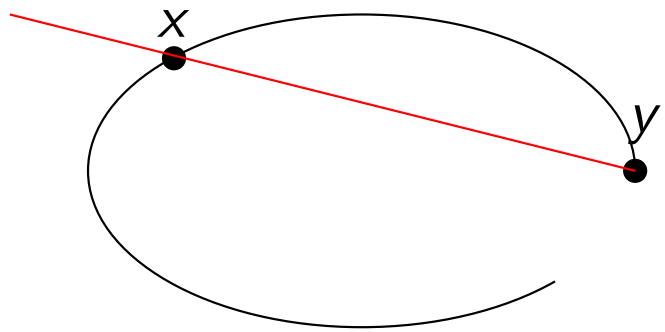
Lemma (2)

(i) there are two co-prime forms of degree at most $t + p^{\lfloor \log_p t \rfloor}$ *which vanish on* $\mathcal{A}$ (=Theorem (B) (i));
or
(ii) there exists a form of degree at most $t + p^{\lfloor \log_p t \rfloor}$ *which is hyperbolic on* $\mathcal{A}$.

Proof (sketch) Consider the gcd ϕ of the space spanned by the $\rho_w(Y)'s$ of degree between $t+1$ and $t + p^{\lfloor \log_p t \rfloor}$.

- ϕ cannot be zero.
- If $\deg \phi = 0$ then we get case (i).
- If $\deg \phi > 0$, then ϕ must be hyperbolic on $\mathcal{A}$.

A form ϕ on $\mathrm{PG}(2, q)$ is hyperbolic on $\mathcal{A}$, if it has the property that ϕ modulo any bisecant factorises into at most two linear factors whose multiplicities sum to the degree of ϕ and which are zero at the points of $\mathcal{A}$ on the bisecant.



$$\phi(X) = \alpha(X)^a \beta(X)^b \text{ modulo bisecant}$$

with $\alpha(x) = 0$, $\beta(y) = 0$, and $a + b = \deg \phi$.

In order to finish the proof we need to exclude case (ii) of Lemma (2), i.e. we need to show that the existence of a hyperbolic form on $\mathcal{A}$ implies that $\mathcal{A}$ is contained in a conic.

Lemma (3)

If there is a form ϕ which is hyperbolic on an arc $\mathcal{A}$, where $|\mathcal{A}| \geqslant 2 \deg \phi + 2$, then all but at most one point of $\mathcal{A}$ are contained in a conic and if q is odd then $\mathcal{A}$ is contained in a conic.

Combining the Lemma's (1) (2) and (3) with Theorem (B) completes the proof of Theorem (A).

Final comments

- We do not rely on Hasse-Weil or Stöhr-Voloch.
- [Ball-Lavrauw 2019] $F(X, Y) \to$ tensor T: $F(Y_1, \ldots, Y_{k-1})$
- The tensor approach simplifies the proof of the MDS conjecture for q prime.
- We expect/hope this approach will allow further progress.

Thank you for your attention!

Sabancı University Graduate Admissions

Application deadline for graduate school:
10th of May 2019

https://www.sabanciuniv.edu/en/admission-to-graduate-programs