When is an arc contained in a conic?

Michel Lavrauw

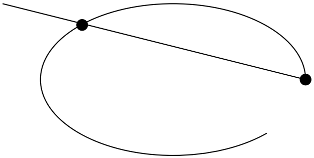
Sabancı University

joint work with Simeon Ball

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

- planar arcs ($k = 3$)
  - a basis of $\mathbb{F}_q^k$
  - a frame (basis + all 1 vector)
  - a conic
    $$\{(1, t, t^2) \ : \ t \in \mathbb{F}_q \cup \{\infty\}\}$$
  - a hyperoval (q even)
    $$\{(1, t, t^2) \ : \ t \in \mathbb{F}_q \cup \{\infty\}\} \cup \{(0, 1, 0)\}$$
- $k > 3$
  - a normal rational curve (NRC)
    $$\{(1, t, t^2, \dots, t^{k-1}) \ : \ t \in \mathbb{F}_q \cup \{\infty\}\}$$
  - Glynn arc ($q = 9,\ k = 5$)
    $$\{(1, t, t^2 + \eta t^6, t^3, t^4) \ : \ t \in \mathbb{F}_q\} \cup \{(0, 0, 0, 0, 1)\}$$
    where $\eta^4 = -1$.

Classification of large complete planar arcs

- Hyperovals (size $q+2$) are not classified
- An oval (size $q+1$) in $\mathrm{PG}(2,q)$, q odd, is a conic [Segre 1955]
- An arc of size q is incomplete [Segre 1955] [Tallini 1957]
- In combination with computational results from [Coolsaet and Sticker 2009, 2011] and [Coolsaet 2015], the results from [BL2018] complete the classification of complete planar arcs of size $q-1$ and $q-2$.

[BL2018] S. Ball and M. L. *Planar arcs*. J. Combin. Theory A. (2018)

Classification of large complete planar arcs

"Il primo nuovo quesito":

Are there more arcs of size $q-3$ which are not contained in a conic?

In combination with previous computational results, [BL2018] implies that the only possibility is an arc $\mathcal{A}$ in $\mathrm{PG}(2,37)$ such that $\mathcal{A}$ is contained in the intersection of two sextic curves not sharing a common component.

The main conjecture (MDS conjecture)

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

MDS conjecture (B. Segre 1950's):

$\mathcal{A}$ cannot be larger than NRC

(except if $q \leq k$, or q even and $k \in \{3, q-2\}$)

Many results, but the MDS conjecture is still open!

A lot of results rely on planar arcs (by projection).

Projection

Most results on the MDS conjecture are based on induction arguments from [Segre1955] and [Kaneta and Maruta 1989].

This further motivates the study of planar arcs, in particular the size of the second largest complete planar arc.

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

(So if $|\mathcal{A}| > N(q)$ and q is odd, then $\mathcal{A}$ is contained in a conic.)

Results from [BL2018]

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

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

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 $q+1$.

About the proof - Bounds on $N(q)$

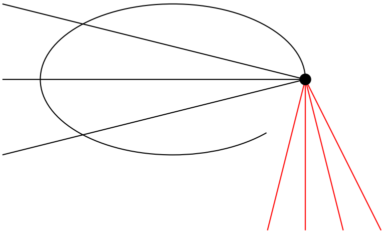
$N(q) =$ size of the second largest complete arc in $\mathrm{PG}(2, q)$.

1. Segre's algebraic envelope
2. Sketch of the proof of Theorem (A)

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 results mentioned in the previous talk by James Hirschfeld (bounds on $m'(2,q)$).

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 $\mathcal{A} \not\subseteq$ 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.

If $\mathcal{A}$ is contained in a curve of degree t (part (ii)), then the proof is not as streamlined, and we refer to the paper for further details.[1]

We continue with 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.

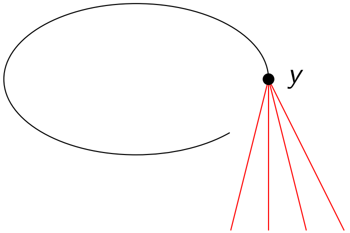
The crucial part is the existence of a certain (t, t)-form which relies on a scaled coordinate-free version of Segre's lemma of tangents.

[1] This part is fundamentally different from the 2017 version

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:

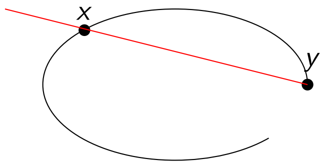
Lemma (2)

(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

- Theorem (B) gives the best results for q a square.
- In the case that q is a non-square and non-prime, our results do not improve upon the bound of Voloch.
- We do not rely on Hasse-Weil or Stöhr-Voloch.
- In the case that q is prime, it does improve on Voloch's bound for primes less than 1783.
- $F(X, Y)$ for higher dimensions $F(Y_1, \ldots, Y_{k-1})$

Thank you for your attention!