

# ARCS IN FINITE PROJECTIVE SPACES

SIMEON BALL

ABSTRACT. These notes are an outline of a course on arcs given at the Finite Geometry Summer School, University of Sussex, June 26-30, 2017.

## BASIC OBJECTS AND DEFINITIONS

Let  $\mathbb{K}$  denote an arbitrary field.

Let  $\mathbb{F}_q$  denote the finite field with  $q$  elements, where  $q$  is the power of a prime  $p$ .

Let  $V_k(\mathbb{K})$  denote the  $k$ -dimensional vector space over  $\mathbb{K}$ .

Let  $\text{PG}_{k-1}(\mathbb{K})$  denote the  $(k-1)$ -dimensional projective space over  $\mathbb{K}$ .

Let  $\text{AG}_k(\mathbb{K})$  denote the  $k$ -dimensional affine space over  $\mathbb{K}$ .

A projective point of  $\text{PG}_{k-1}(\mathbb{K})$  is a one-dimensional subspace of  $V_k(\mathbb{K})$  which, with respect to a basis, is denoted by  $(x_1, \dots, x_k)$ .

The *weight* of a vector is the number of non-zero coordinates it has with respect to a fixed canonical basis.

A  $k$ -dimensional *linear code* of length  $n$  and minimum distance  $d$  is a  $k$ -dimensional subspace of  $V_n(\mathbb{F}_q)$  in which every non-zero vector has weight at least  $d$ .

## 1. NORMAL RATIONAL CURVE

**Example 1.** A normal rational curve is a set of  $q+1$  points in  $\text{PG}_{k-1}(\mathbb{K})$  projectively equivalent to

$$S = \{(1, t, \dots, t^{k-1}) \mid t \in \mathbb{K} \cup \{(0, \dots, 0, 1)\}\}.$$

**Lemma 2.** Any  $k$ -subset of  $S$  spans  $\text{PG}_{k-1}(\mathbb{K})$ .

An *arc*  $S$  of  $\text{PG}_{k-1}(\mathbb{K})$  is a subset of points with the property that any  $k$ -subset of  $S$  spans  $\text{PG}_{k-1}(\mathbb{K})$ . Implicitly, we will assume that  $S$  has size at least  $k$ .

For  $k = 3$ , a normal rational curve is the zero-set of a quadratic form. In the example above,  $X_1X_3 - X_2^2$ .

A symmetric bilinear form  $b(X, Y)$  is *degenerate* if  $b(X, y) = 0$  for some point  $y$ .

A quadratic form  $f(X)$  is *degenerate* if  $f(y) = 0$  and  $b(X, y) = 0$  for some point  $y$ .

**Exercise 1.** Let  $f(X)$  be a non-degenerate quadratic form in three variables. There is a basis of the space with respect to which  $f(X) = X_1X_3 - X_2^2$ .

The zero-set of a non-degenerate quadratic form is a *conic*.

**Exercise 2.** There is a unique conic through any arc of 5 points of  $\text{PG}_2(\mathbb{K})$ .

There is a  $k \times k$  matrix  $M$  over  $\mathbb{K}$  such that

$$M \begin{pmatrix} 1 \\ t \\ \cdot \\ \cdot \\ \cdot \\ t^{k-1} \end{pmatrix} = \begin{pmatrix} (ct + d)^{k-1} \\ (ct + d)^{k-2}(at + d) \\ \cdot \\ \cdot \\ (ct + d)(at + d)^{k-2} \\ (at + d)^{k-1} \end{pmatrix}.$$

**Exercise 3.** The automorphism group of the normal rational curve is transitive on the points of the normal rational curve.

**Exercise 4.** The normal rational curve in  $\text{PG}_{k-1}(\mathbb{K})$  projects onto a normal rational curve in  $\text{PG}_{k-2}(\mathbb{K})$  from any point of the normal rational curve.

**Exercise 5.** There is a unique normal rational curve through any arc of  $k + 2$  points of  $\text{PG}_{k-1}(\mathbb{K})$ .

## 2. OTHER EXAMPLES OF LARGE ARCS

**Example 3.** Let  $\sigma$  be the automorphism of  $\mathbb{F}_q$ ,  $q = 2^h$ , which takes  $x$  to  $x^{2^e}$ . The set

$$S = \{(1, t, t^\sigma) \mid t \in \mathbb{F}_q \cup \{(0, 0, 1), (0, 1, 0)\}\}.$$

is called the *translation hyperoval*. It is an arc of  $q + 2$  points in  $\text{PG}_2(\mathbb{F}_q)$ , whenever  $(e, h) = 1$ .

**Exercise 6.** Prove that Example 3 is an arc.

**Example 4.** Let  $\sigma$  be the automorphism of  $\mathbb{F}_q$ ,  $q = 2^h$ , which takes  $x$  to  $x^{2^e}$ . The set

$$S = \{(1, t, t^\sigma, t^{\sigma+1}) \mid t \in \mathbb{F}_q \cup \{(0, 0, 0, 1)\}\}.$$

is an arc of  $q + 1$  points in  $\text{PG}_3(\mathbb{F}_q)$ , whenever  $(e, h) = 1$ .

**Exercise 7.** Prove that the automorphism group of the arc is 2-transitive, by finding a matrix  $M$  such that

$$M \begin{pmatrix} 1 \\ t \\ t^\sigma \\ t^{\sigma+1} \end{pmatrix} = \begin{pmatrix} (ct + d)^{\sigma+1} \\ (ct + d)^\sigma(at + d) \\ (ct + d)(at + d)^\sigma \\ (at + d)^{\sigma+1} \end{pmatrix}.$$

Prove that Example 4 is an arc.

**Example 5.** Let  $\eta$  be an element of  $\mathbb{F}_9$ ,  $\eta^4 = -1$ . The set

$$S = \{(1, t, t^2 + \eta t^6, t^3, t^4) \mid t \in \mathbb{F}_9 \cup \{(0, 0, 0, 0, 1)\}\}.$$

is an arc of size  $q + 1$  in  $\text{PG}_4(\mathbb{F}_9)$ .

**Exercise 8.** Prove that Example 5 is an arc.

### 3. THE TRIVIAL UPPER BOUND AND THE MDS CONJECTURE

**Theorem 6.** Let  $S$  be an arc of  $\text{PG}_{k-1}(\mathbb{F}_q)$  of size  $q + k - 1 - t$  and let  $A$  be a subset of  $S$  of size  $k - 2$ . There are exactly  $t$  hyperplanes which meet  $S$  in precisely the points  $A$ .

*Proof.* The points of  $A$  span a  $(k - 3)$ -dimensional subspace  $\langle A \rangle$ . There are  $q + 1$  hyperplanes containing  $\langle A \rangle$  each containing at most one point of  $S \setminus A$ . Therefore there are  $q + 1 - (|S| - k - 2)$  hyperplanes which meet  $S$  in precisely the points  $A$ .  $\square$

**Corollary 7.** An arc of  $\text{PG}_{k-1}(\mathbb{F}_q)$  has at most  $q + k - 1$  points.

*Proof.* The follows from Theorem 6, since  $t \geq 0$ .  $\square$

**Theorem 8.** Let  $S$  be an arc of  $\text{PG}_{k-1}(\mathbb{F}_q)$ . If  $k \geq q$  then  $|S| \leq k + 1$ .

*Proof.* After choosing a suitable basis and scaling the points of  $S$  we can assume

$$S \supseteq \{e_1, \dots, e_k, e_1 + \dots + e_k\},$$

where  $e_i$  is the  $i$ -th coordinate vector.

Suppose  $u = (u_1, \dots, u_k) \in S \setminus \{e_1, \dots, e_k, e_1 + \dots + e_k\}$ .

If  $u_i = 0$  for some  $i$  then the hyperplane  $\ker X_i$  (the hyperplane with equation  $X_i = 0$ ) contains  $k$  points of  $S$ , contradicting the arc property.

If  $u_i \neq 0$  for all  $i$  then by the pigeon-hole principle there exists  $i$  and  $j$  such that  $u_i = u_j$ , since  $k \geq q$ . But then the hyperplane  $\ker(X_i - X_j)$  (the hyperplane with equation  $X_i = X_j$ ) contains  $k$  points of  $S$ , contradicting the arc property.  $\square$

Let  $G$  be a  $k \times |S|$  matrix with entries from  $\mathbb{F}_q$  whose columns are vector representatives of the points of  $S$ .

**Lemma 9.** *For all  $u \in \mathbb{F}_q^k$  the vector  $uG$  has at most  $k - 1$  zeros.*

*Proof.* Suppose that there are  $k$  coordinates where  $uG$  has zero coordinates. Then restricting  $G$  to these  $k$  coordinates we get a  $k \times k$  submatrix of  $G$  which has rank less than  $k$ . Hence, the  $k$  columns of this submatrix are linearly dependent, contradicting the arc property.  $\square$

Let  $C = \{uG \mid u \in \mathbb{F}_q^k\}$ . Then  $C$  is a  $k$ -dimensional subspace of  $\mathbb{F}_q^{|S|}$ .

**Lemma 10.** *The minimum weight of a non-zero vector in  $C$  is  $|S| - k + 1$ .*

*Proof.* This follows immediately from Lemma 9.  $\square$

A  $k$ -dimensional *linear maximum distance separable* (MDS) code  $C$  of length  $n$  is a  $k$ -dimensional subspace of  $\mathbb{F}_q^n$  in which every non-zero vector has weight at least  $n - k + 1$ .

We have already established the following lemma.

**Lemma 11.** *The linear code generated by the matrix  $G$ , whose columns are vector representatives of the points of an arc is a linear MDS code, and vice-verse, the set of columns of a generator matrix of a linear code, considered as a set of points of the projective space, is an arc.*

The *dual* of a linear code  $C$  is,

$$C^\perp = \{v \in \mathbb{F}_q^{|S|} \mid u \cdot v = 0 \text{ for all } u \in C\},$$

where  $u \cdot v = u_1v_1 + \cdots + u_kv_k$ .

**Lemma 12.** *The linear code  $C$  is MDS if and only if  $C^\perp$  is MDS.*

*Proof.* Suppose  $C$  is MDS and that  $C^\perp$  is not MDS. Then  $C^\perp$  contains a non-zero vector  $v$  with of weight less than  $n - (n - k) = k$ . Consider the columns of  $G$  which correspond to these non-zero coordinates of  $v$ . Then these columns are linearly dependent, contradicting the arc property implied by Lemma 11.  $\square$

**Corollary 13.** *There is an arc of size  $n$  in  $\text{PG}_{k-1}(\mathbb{F}_q)$  if and only if there is an arc of size  $n$  in  $\text{PG}_{n-k-1}(\mathbb{F}_q)$ .*

*Proof.* This follows from Lemma 11 and Lemma 12.  $\square$

**Conjecture 14.** *(The MDS conjecture) If  $4 \leq k \leq q - 3$  then an arc of  $\text{PG}_{k-1}(\mathbb{F}_q)$  has size at most  $q + 1$ .*

#### 4. THE TANGENT FUNCTIONS AND THE LEMMA OF TANGENTS

Let  $S$  be an arc of  $\text{PG}_{k-1}(\mathbb{F}_q)$  of size  $q + k - 1 - t$  and let  $A$  be a subset of  $S$  of size  $k - 2$ .

Let  $\alpha_1, \dots, \alpha_t$  be  $t$  linear forms whose kernels are the  $t$  hyperplanes which meet  $S$  in precisely the points  $A$ , see Theorem 6.

Define (up to scalar factor) a homogeneous polynomial of degree  $t$ ,

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

where  $X = (X_1, \dots, X_k)$ .

A homogeneous polynomial  $f$  in  $k$  variables defines a function from  $V_k(\mathbb{F}_q)$  to  $\mathbb{F}_q$  under evaluation. If we change the basis of  $V_k(\mathbb{F}_q)$  then although the polynomial  $f$  will change its evaluation function will not. Put another way, any function from  $V_k(\mathbb{F}_q)$  to  $\mathbb{F}_q$  is the evaluation of a polynomial once we fix a basis of  $V_k(\mathbb{F}_q)$ . Obviously, the polynomial we obtain depends on the basis we choose.

**Lemma 15.** *(Segre's lemma of tangents) Let  $S$  be an arc of  $\text{PG}_{k-1}(\mathbb{F}_q)$  and let  $D$  be a subset of  $S$  of size  $k - 3$ . For all  $x, y, z \in S \setminus D$ ,*

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

*Proof.* ( $k = 3$ ). Let  $f_a^*(X)$  be the homogeneous polynomial we obtain from  $f_a(X)$  when we change the basis from the canonical basis to  $B = \{x, y, z\}$ .

The polynomial  $f_x^*(X) = \prod_{i=1}^t (a_{i2}X_2 + a_{i3}X_3)$ , for some  $a_{ij} \in \mathbb{F}_q$ .

The polynomial  $f_y^*(X) = \prod_{i=1}^t (b_{i1}X_1 + b_{i3}X_3)$ , for some  $b_{ij} \in \mathbb{F}_q$ .

The polynomial  $f_z^*(X) = \prod_{i=1}^t (c_{i1}X_1 + c_{i2}X_2)$ , for some  $c_{ij} \in \mathbb{F}_q$ .

Let  $s \in S \setminus B$ . The line joining  $x$  and  $s$  is  $\ker(s_3X_2 - s_2X_3)$  where  $(s_1, \dots, s_k)$  are the coordinates of  $s$  with respect to the basis  $B$ .

As  $s$  runs through the elements of  $S \setminus B$ , the element  $-s_2/s_3$  runs through the elements of  $\mathbb{F}_q \setminus \{a_{i3}/a_{i2} \mid i = 1, \dots, t\}$ . Since the product of all the non-zero elements of  $\mathbb{F}_q$  is  $-1$ ,

$$\prod_{s \in S \setminus B} \frac{-s_2}{s_3} \prod_{i=1}^t \frac{a_{i3}}{a_{i2}} = -1,$$

and since  $\prod_{i=1}^t a_{i3} = f_x^*(z)$  and  $\prod_{i=1}^t a_{i2} = f_x^*(y)$ , we have

$$f_x^*(z) \prod_{s \in S \setminus B} (-s_2) = \prod_{s \in S \setminus B} (-s_2) s_3 f_x^*(y).$$

Now permuting  $x$ ,  $y$  and  $z$ , we get

$$f_y^*(x) \prod_{s \in S \setminus B} (-s_3) = \prod_{s \in S \setminus B} s_1 f_y^*(z)$$

and

$$f_z^*(y) \prod_{s \in S \setminus B} (-s_1) = \prod_{s \in S \setminus B} s_2 f_z^*(x),$$

from which

$$f_x^*(z) f_y^*(x) f_z^*(y) = (-1)^{t+1} f_x^*(y) f_y^*(z) f_z^*(x).$$

Now, since  $f^*$  and  $f$  define the same functions on the points of  $\text{PG}_{k-1}(\mathbb{F}_q)$ , the lemma follows.  $\square$

Order the elements of  $S$  arbitrarily and let  $F$  be the first  $k-2$  points of  $S$ .

Let  $A$  be a subset of  $S$  of size  $k-2$ , where  $A \neq F$ . Let  $e$  be the first element of  $F \setminus A$  and  $a$  be the last element of  $A \setminus F$ . We scale  $f_A(X)$  so that

$$f_A(e) = (-1)^{s(\sigma)(t+1)} f_{(A \cup \{e\}) \setminus \{a\}}(a),$$

where  $\sigma$  is the permutation that orders  $(A, e)$  as in the ordering of  $S$  and  $s(\sigma)$  is the sign of the permutation  $\sigma$ .

Note that this scaling only makes sense if we fix a representative for each point of  $S$ .

**Lemma 16.** (*Segre's lemma of tangents scaled and planar*) Let  $S$  be an arc of  $\text{PG}_2(\mathbb{F}_q)$ . For all  $x, y \in S$ ,

$$f_{\{x\}}(y) = (-1)^{t+1} f_{\{y\}}(x).$$

*Proof.* This follows from Lemma 15 and the fact that we have scaled  $f_a(X)$  so that  $f_e(x) = (-1)^{t+1} f_x(e)$ .  $\square$

**Lemma 17.** (*Segre's lemma of tangents scaled*) Let  $S$  be an arc of  $\text{PG}_{k-1}(\mathbb{F}_q)$  and let  $D$  be a subset of  $S$  of size  $k - 3$ . For any  $x, y \in S \setminus D$ ,

$$f_{D \cup \{x\}}(y) = (-1)^{s(\sigma)(t+1)} f_{D \cup \{y\}}(x),$$

where  $\sigma$  is the permutation that orders  $(D \cup \{x\}, y)$  as  $(D \cup \{y\}, x)$

Lemma 17 can be proved by induction on the number of elements that  $D$  intersects  $F$  in and using Lemma 15.

## 5. THE SEGRE-BLOKHUIS-BRUEN-THAS FORM

A *planar arc* is an arc of  $\text{PG}_2(\mathbb{F}_q)$ .

The Segre form associated to a planar arc is the polynomial  $G(X, Y)$  whose existence is proved in the following theorem.

**Theorem 18.** Let  $m \in \{1, 2\}$  such that  $m - 1 = q$  modulo 2. If  $S$  is a planar arc of size  $q + 2 - t$ , where  $|S| \geq mt + 2$ , then there is a homogeneous polynomial in three variables  $\phi(Z)$ , of degree  $mt$ , which gives a polynomial  $G(X, Y)$  under the substitution  $Z_1 = X_2Y_3 - Y_2X_3$ ,  $Z_2 = X_1Y_3 - Y_1X_3$ ,  $Z_3 = X_2Y_1 - Y_2X_1$ , with the property that for all  $y \in S$

$$G(X, y) = f_y(X)^m.$$

*Proof.* Order the set  $S$  arbitrarily and let  $E$  be a subset of  $S$  of size  $mt + 2$ . Define

$$G(X, Y) = \sum_{a < b} f_a(b)^m \prod_{u \in E \setminus \{a, b\}} \frac{\det(X, Y, u)}{\det(a, b, u)}.$$

where the sum runs over subsets  $\{a, b\}$  of  $E$ .

Then, for  $y \in E$ , the only non-zero terms in  $G(X, y)$  are obtained for  $a = y$  and  $b = y$ . Lemma 16 implies

$$G(X, y) = \sum_{a \in E \setminus y} f_a(y)^m \prod_{u \in E \setminus \{a, y\}} \frac{\det(X, y, u)}{\det(a, y, u)}.$$

With respect to a basis containing  $y$ , the polynomials  $G(X, y)$  and  $f_y(X)^m$  are homogeneous polynomials in two variables of degree  $mt$ . Their values at the  $mt + 1$  points  $x \in E \setminus \{y\}$  are the same, so we conclude that  $G(X, y) = f_y(X)^m$ .

If  $y \notin E$  then we still have that with respect to a basis containing  $y$ , the polynomial  $G(X, y)$  is a homogeneous polynomial in two variables of degree  $mt$ . For  $x \in E$ ,

$$G(x, y) = G(y, x) = f_x(y)^m = f_y(x)^m,$$

the last equality following from Lemma 16, and so again we conclude that  $G(X, y) = f_y(X)^m$ .  $\square$

If  $y \in S$  and  $x$  is a point on a tangent to  $S$  incident with  $y$  then  $G(x, y) = f_y(x)^m = 0$ . This implies that, changing the coordinates to  $z_1 = x_2y_3 - y_2x_3$ , etc, the point  $z$  is a zero of the polynomial  $\phi(Z)$ . Therefore, the set of zeros of  $\phi$  contains the points in the dual plane, dual to the tangents of  $S$ .

**Theorem 19.** *Let  $m \in \{1, 2\}$  such that  $m - 1 = q$  modulo 2. If  $S$  is a planar arc of size  $q + 2 - t$ , where  $|S| \geq mt + 2$ , then  $S$  has a unique completion to a complete arc.*

*Proof.* Suppose that  $S$  is incomplete, i.e. there is a point  $u$  such that  $S \cup \{u\}$  is an arc. Then the polynomial we obtain from  $G(u, Y)$ , when we change the basis to a basis containing  $u$ , is a homogenous polynomial in two variables of degree  $mt$  which is zero at all points  $y$  of  $S$ , since the line joining  $y$  and  $u$  is a tangent and so  $G(u, y) = f_y(u)^m = 0$ . Therefore  $G(X, u)$  is identically zero. This implies

$$\phi(u_3X_2 - u_2X_3, u_3X_1 - u_1X_3, u_1X_2 - u_2X_1) = 0,$$

so  $\phi$  is zero at all points of the line  $u_1Z_1 + u_2Z_2 + u_3Z_3 = 0$ , so  $u_1Z_1 + u_2Z_2 + u_3Z_3$  is a factor of  $\phi(Z)$ . Therefore, if  $S$  is incomplete, we can find the points which extend  $S$  to a larger arc by looking at the factors of  $\phi(Z)$ .  $\square$

**Theorem 20.** *If  $S$  is a planar arc of size at least  $q - \sqrt{q} + 2$  and  $q$  is even then  $S$  is extendable to an arc of size  $q + 2$ .*

*Proof.* The tangents to  $S$  are a set of  $(q + 2 - t)t$  points in the dual plane which are all zeros of  $\phi(Z)$ , the polynomial of degree  $t$  given by Theorem 18. If  $\phi(Z)$  has a linear factor then  $G(X, Y)$  has a factor  $\det(X, Y, u)$  for some point  $u$ , so  $u$  is joined to each point of  $S$  by a tangent. Therefore  $u$  extends  $S$  to a larger arc.



If not then each line meets the zero-set of  $\phi(Z)$  in at most  $t$  points. Fixing a zero  $x$  of  $\phi(Z)$  and considering the lines incident with  $x$ , each of these lines is incident with at most  $t - 1$  other points of the zero-set of  $\phi(Z)$ . Therefore the zero-set of  $\phi(Z)$  has at most  $(t - 1)(q + 1) + 1$  points. Hence, if  $S$  is complete then  $(q + 2 - t)t \leq (t - 1)(q + 1) + 1$ .  $\square$

**Theorem 21.** *Let  $q \geq 9$  be a square. Let  $I$  be the  $3 \times 3$  identity matrix and let  $H$  be a  $3 \times 3$  matrix with the property that  $H^{\sqrt{q}} = H^t$ . For any  $3 \times 3$  matrix  $M$ , let*

$$V(M) = \{x \in \text{PG}_2(\mathbb{F}_q) \mid x^t M x^{\sqrt{q}} = 0\}$$

*If the characteristic polynomial of  $H$  is irreducible over  $\mathbb{F}_q$  then the set of points  $S = V(I) \cap V(H)$  is an arc of  $\text{PG}_2(\mathbb{F}_q)$  of size  $q - \sqrt{q} + 1$  not contained in a conic.*

*Proof.* Consider the Hermitian curves  $V(H + \mu I)$ , where  $\mu \in \mathbb{F}_{\sqrt{q}}$  and  $V(I)$ .

If  $x$  is a point on two of these curves then  $x \in S$ .

If  $x \notin S$  and  $x \notin V(I)$  then  $x$  is a point of  $V(H + (a/b)I)$ , where  $x^t H x^{\sqrt{q}} = a$  and  $x^t I x^{\sqrt{q}} = -b$ .

Hence, each point is either in  $S$  or on exactly one of the  $\sqrt{q} + 1$  Hermitian curves.

Therefore,

$$(\sqrt{q} + 1)(q\sqrt{q} + 1) = |S|(\sqrt{q} + 1) + q^2 + q + 1 - |S|,$$

which gives  $|S| = q - \sqrt{q} + 1$ .

Suppose that  $\ell$  is a line incident with  $r \geq 2$  points of  $S$ . Then  $\ell$  intersects each Hermitian curve ( $V(H + \mu I)$  or  $V(I)$ ) in  $\sqrt{q} + 1$  points,  $r$  of which are in  $S$  and  $\sqrt{q} + 1 - r$  of which are not in  $S$ .

Counting points of  $\ell$  not in  $S$  we have  $(\sqrt{q} + 1 - r)(\sqrt{q} + 1) = q + 1 - r$ , since each point not in  $S$  is on exactly one of the  $\sqrt{q} + 1$  Hermitian curves. This gives  $r = 2$  and so  $S$  is an arc.

It follows from Bezout's theorem that  $S$  has at most  $2\sqrt{q}$  points in common with a conic, so cannot be contained in a conic for  $q - \sqrt{q} \geq 2\sqrt{q}$ .  $\square$

**Exercise 9.** *Prove that the arc constructed in Theorem 21 cannot be extended to a larger arc.*

The Segre-Blokhuis-Bruen-Thas form associated to an arc is the polynomial  $G(X_1, \dots, X_{k-1})$  whose existence is proved in the following theorem.

We denote by  $\det_j(X_1, \dots, X_{k-1})$  the determinant in which the  $j$ -coordinate has been deleted.

**Theorem 22.** *Let  $m \in \{1, 2\}$  such that  $m - 1 = q$  modulo 2. If  $S$  is a planar arc of size  $q + k - 1 - t$ , where  $|S| \geq mt + k - 1$ , then there is a homogeneous polynomial in three variables  $\phi(Z)$ , of degree  $mt$ , which gives a polynomial  $G(X_1, \dots, X_{k-1})$  under the substitution  $Z_j = \det_j(X_1, \dots, X_{k-1})$ , with the property that for all  $\{y_1, \dots, y_{k-2}\} \subset S$*

$$G(X, y_1, \dots, y_{k-2}) = f_{\{y_1, \dots, y_{k-2}\}}(X)^m.$$

*Proof.* Order the set  $S$  arbitrarily and let  $E$  be a subset of  $S$  of size  $mt + k - 1$ . Define

$$G(X_1, \dots, X_{k-1}) = \sum_{\{a_1, \dots, a_{k-1}\}} f_{a_1, \dots, a_{k-2}}(a_{k-1})^m \prod_{u \in E \setminus \{a_1, \dots, a_{k-1}\}} \frac{\det(X_1, \dots, X_{k-1}, u)}{\det(a_1, \dots, a_{k-1}, u)}.$$

where the sum runs over subsets  $\{a_1, \dots, a_{k-1}\}$  of  $E$ .

The proof is then the same as the proof of Theorem 18.  $\square$

**Theorem 23.** *Let  $m \in \{1, 2\}$  such that  $m - 1 = q$  modulo 2. If  $S$  is a planar arc of size  $q + k - 1 - t$ , where  $|S| \geq mt + k - 1$ , then  $S$  has a unique completion to a complete arc.*

## 6. A NEW FORM

For an arc  $S$  of  $\text{PG}_2(\mathbb{F}_q)$  of size  $q + 2 - t$ , let  $\Phi[X]$  denote the subspace of the vector space of homogeneous polynomials of degree  $t$  in  $X = (X_1, X_2, X_3)$  which are zero on  $S$ .

**Theorem 24.** *Let  $S$  be a planar arc of size  $q + 2 - t$ . There is a polynomial  $F(X, Y)$ , which is a homogeneous polynomial of degree  $t$  in both  $X$  and  $Y$ , such that*

$$F(X, Y) = (-1)^{t+1} F(Y, X)$$

*and with the property that for all  $a \in S$ ,*

$$F(X, a) = f_a(X) \pmod{\Phi[X]}.$$

*Moreover, modulo  $(\Phi[X], \Phi[Y])$  the polynomial  $F$  is unique.*

**Example 25.** The planar arc of 12 points in  $\text{PG}_2(\mathbb{F}_{13})$ ,

$$S = \{(3, 4, 1), (-3, 4, 1), (3, -4, 1), (-3, -4, 1), (4, 3, 1), (4, -3, 1), (-4, 3, 1), (-4, -3, 1), \\ (1, 1, 1), (1, -1, 1), (-1, 1, 1), (-1, -1, 1)\}$$

is an arc with  $t = 3$  and it is not contained in a curve of degree 3. Consequently, Theorem 31 implies that there is a unique polynomial  $F(X, Y)$  of degree three in both  $X$  and  $Y$  with the property that  $F(X, a) = f_a(X)$  for all  $a \in S$ . It is given by

$$\begin{aligned} F(x, y) = & 5(x_2^2 x_3 y_1^2 y_3 + y_2^2 y_3 x_1^2 x_3 + x_2 x_3^2 y_1^2 y_2 + x_1^2 x_2 y_2 y_3^2 + x_1 x_3^2 y_1 y_2^2 + x_1 x_2^2 y_1 y_3^2) \\ & + 6x_1 x_2 x_3 y_1 y_2 y_3 + x_1^3 y_1^3 + x_2^3 y_2^3 + x_3^3 y_3^3. \end{aligned}$$

Let  $S$  be a planar arc of size  $q+2-t$  and let  $F(X, Y)$  be a polynomial given by Theorem 31, i.e. a representative from the equivalence class modulo  $(\Phi[X], \Phi[Y])$ .

For each  $i, j, k \in \{0, \dots, t-1\}$  where  $i+j+k \leq t-1$ , define  $\rho_{ijk}(Y)$  to be the coefficient of  $X_1^i X_2^j X_3^k$  in

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

**Lemma 26.** *For all  $i, j, k \in \{0, \dots, t-1\}$  where  $i+j+k \leq t-1$ , the polynomial  $\rho_{ijk}(Y)$  is either zero or a homogeneous polynomial of degree  $2t-i-j-k$  which is zero on  $S$ .*

**Example 27.** Applying Lemma 26 to the arc of size 12 in Example 25, we see that  $S$  lies on the intersection of the three quartic curves  $x_3^4 = x_1^2 x_2^2$ ,  $x_2^4 = x_1^2 x_3^2$  and  $x_1^4 = x_3^2 x_2^2$ .

We say that a polynomial  $\phi(X)$  is *hyperbolic on an arc  $S$*  if  $\phi$  has the property that if the kernel of a linear form  $\gamma$  is a bisecant  $\ell$  to  $S$  then  $\phi$  modulo  $\gamma$  factorises into at most two linear factors, which are zero at the points of  $S$  on  $\ell$ , and whose multiplicities sum to the degree of  $\phi$ .

**Lemma 28.** *Let  $S$  be a planar arc of size  $q+2-t$ . If  $q$  is odd then one of the following holds: (i) there are two co-prime polynomials of degree at most  $t+p^{\lfloor \log_p t \rfloor}$  which are zero on  $S$ ; (ii) there is a non-zero homogeneous polynomial  $\phi$  of degree at most  $t+p^{\lfloor \log_p t \rfloor}$  which is hyperbolic on  $S$ .*

**Lemma 29.** *Let  $S$  be a planar arc of size  $q+2-t \geq 8$ . If there is a homogeneous polynomial  $\phi$  of degree at most  $\frac{1}{2}(q-t+1)$  which is hyperbolic on  $S$ , then  $S$  is contained in a conic.*

**Theorem 30.** *Let  $S$  be a planar arc of size  $q+2-t$  not contained in a conic. If  $q$  is odd then  $S$  is contained in the intersection of two curves, sharing no common component, each of degree at most  $t+p^{\lfloor \log_p t \rfloor}$ .*

**Theorem 31.** *Let  $S$  be a arc of  $\text{PG}_{k-1}(\mathbb{F}_q)$  of size  $q+k-1-t$  arbitrarily ordered. There is a function  $F = F(X_1, \dots, X_{k-1})$ , which is homogeneous polynomial of degree  $t$  in  $X_i = (X_{i1}, \dots, X_{ik})$  for each  $i = 1, \dots, k-1$ , with the following properties*

(i) For all ordered subsets  $A = \{a_1, \dots, a_{k-2}\} \subseteq S$ ,

$$F(X, a_1, \dots, a_{k-2}) = f_A(X) \pmod{\Phi[X]}.$$

(ii) For all non-distinct  $a_1, \dots, a_{k-1} \in S$ ,

$$F(a_1, \dots, a_{k-1}) = 0.$$

(iii) For any permutation  $\sigma \in \text{Sym}(k-1)$ ,

$$F(X_1, X_2, \dots, X_{k-1}) = (-1)^{s(\sigma)(t+1)} F(X_{\sigma(1)}, X_{\sigma(2)}, \dots, X_{\sigma(k-1)}).$$

(iv) Modulo  $\Phi[X_1], \dots, \Phi[X_{k-1}]$  the polynomial  $F$  is unique.

## 7. PROOF OF THE MDS CONJECTURE FOR PRIME FIELDS

Let  $S$  be an arc of  $\text{PG}_{k-1}(\mathbb{F}_q)$  of size  $q + k - 1 - t \geq k + t$  arbitrarily ordered.

For each subset  $E$  of  $S$  of size at least  $k + t$ , and subset  $C = \{a_1, \dots, a_{k-2}\}$  of  $E$ , define

$$\alpha_{C,E} = f_{a_1, \dots, a_{k-2}}(a_{k-1}) \prod_{u \in E \setminus C} \det(u, a_1, \dots, a_{k-1}).$$

**Lemma 32.** *Let  $S$  be an arc of  $\text{PG}_{k-1}(\mathbb{F}_q)$  of size  $q + k - 1 - t \geq k + t$  arbitrarily ordered and let  $E$  be a subset of  $S$  of size  $k + t$ . For every subset  $A$  of  $E$  of size  $k - 2$ ,*

$$\sum_C \alpha_{C,E} = 0,$$

where the sum runs over the  $(k-1)$ -subsets of  $E$  containing  $A$ .

The following theorem proves the MDS conjecture for  $q$  prime.

**Theorem 33.** *Let  $S$  be an arc of  $\text{PG}_{k-1}(\mathbb{F}_q)$ . If  $k \leq p$  then  $|S| \leq q + 1$ .*

## 8. CLASSIFICATION OF THE LARGEST ARCS FOR $k \leq p$

**Theorem 34.** *Let  $S$  be an arc of  $\text{PG}_{k-1}(\mathbb{F}_q)$  of size  $q + 1$ . If  $k \leq p$  and  $k \neq \frac{1}{2}(q + 1)$  then  $S$  is a normal rational curve.*

## 9. EXTENDING SMALL ARCS TO LARGE ARCS

Let  $G$  be an arc of  $\text{PG}_{k-1}(\mathbb{F}_q)$  arbitrarily ordered.

Suppose that  $G$  can be extended to an arc  $S$  of  $\text{PG}_{k-1}(\mathbb{F}_q)$  of size  $q + k - 1 - t \geq k + t$ .

Let  $n = |G| - k - t$  be a non-negative integer.

For each subset  $A$  of  $G$  of size  $k - 2$  and  $U$  of  $G \setminus A$  of size  $n$ , Lemma 32 implies

$$\sum_C \alpha_{C,G} \prod_{u \in U} \det(u, C) = 0,$$

where the sum runs over the  $(k - 1)$ -subsets of  $G$  containing  $A$ .

This system of equations can be expressed in matrix form by the matrix  $P_n$ , whose columns are indexed by the  $(k - 1)$ -subsets  $C$  of  $G$  and whose rows are indexed by pairs  $(A, U)$ , where  $A$  is a  $(k - 2)$ -subset of  $G$  and  $U$  is a  $n$ -subset of  $G \setminus A$ . The  $((A, U), C)$  entry of  $P_n$  is zero unless  $C$  contains  $A$  in which case it is  $\prod_{u \in U} \det(u, C)$ .

**Theorem 35.** *If an arc  $G$  of  $\text{PG}_{k-1}(\mathbb{F}_q)$  can be extended to an arc of size  $q + 2k - 1 - |G| + n$  then the system of equations  $P_n v = 0$  has a solution in which all the coordinates of  $v$  are non-zero.*

**Theorem 36.** *If  $G$  is a subset of the normal rational curve of  $\text{PG}_{k-1}(\mathbb{F}_q)$  of size  $3k - 6$  and  $q$  is odd, then  $G$  cannot be extended to an arc of size  $q + 2$ .*