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 $\mathrm{V}_k(\mathbb{K})$ denote the k-dimensional vector space over $\mathbb{K}$.

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

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

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 $\mathrm{V}_n(\mathbb{F}_q)$ 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 $\mathrm{PG}_{k-1}(\mathbb{K})$ projectively equivalent to

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

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

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

Date: 30 June 2017.

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* is $b(X, y) = 0$ 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 an arc of 5 points of* $\mathrm{PG}_2(\mathbb{K})$.

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

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

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

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

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

2. Other examples of large arcs

Example 3. Let σ 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 $\mathrm{PG}_2(\mathbb{F}_q)$, whenever $(e, h) = 1$.

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

Example 4. Let σ 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 $\mathrm{PG}_3(\mathbb{F}_q)$, whenever $(e, h) = 1$.

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

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

Prove that Example 4 is an arc.

Example 5. Let η 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 $\mathrm{PG}_4(\mathbb{F}_9)$.

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 $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ 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. □

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

Proof. The follows from Theorem 6, since $t \geqslant 0$. □

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

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

$$S \supseteq \{e_1, \ldots, e_k, e_1 + \cdots + e_k\},$$

where e_i is the i-th coordinate vector.

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

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 and i and j such that $u_i = u_j$, since $k \geqslant q$. 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. □

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. □

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. □

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,

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

where $u \cdot v = u_1 v_1 + \cdots + u_k v_k$.

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. □

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

Proof. This follows from Lemma 11 and Lemma 12. □

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

4. The tangent functions and the lemma of tangents

Let S be an arc of $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ 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 $\mathrm{V}_k(\mathbb{F}_q)$ to $\mathbb{F}_q$ under evaluation. If we change the basis of $\mathrm{V}_k(\mathbb{F}_q)$ then although the polynomial f will change its evaluation function will not. Put another way, any function from $\mathrm{V}_k(\mathbb{F}_q)$ to $\mathbb{F}_q$ is the evaluation of a polynomial once we fix a basis of $\mathrm{V}_k(\mathbb{F}_q)$. Obviously, the polynomial we obtain depends on the basis we choose.

Lemma 15. *(Segre's lemma of tangents) Let S be an arc of $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ 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

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

Now permuting x, y and z, we get

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

and

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

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 $\mathrm{PG}_{k-1}(\mathbb{F}_q)$, the lemma follows. □

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

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* $\mathrm{PG}_2(\mathbb{F}_q)$. *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 $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ 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 σ 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 $\mathrm{PG}_2(\mathbb{F}_q)$.

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 $|S| \geqslant mt + 2$, 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 $G(X, y) = f_y(X)^m$. □

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 ϕ 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 $|S| \geqslant mt + 2$, 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 ϕ 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 $\phi(Z)$. □

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 $(q + 2 - t)t \leqslant (t - 1)(q + 1) + 1$. □

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

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

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

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

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

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

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 ℓ is a line incident with $r \geqslant 2$ points of S. Then ℓ intersects each Hermitian curve ($V(\mathrm{H} + \mu\mathrm{I})$ or $V(\mathrm{I})$) 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 ℓ 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 $2\sqrt{q} + 2$ points in common with a conic, so cannot be contained in a conic for $q - \sqrt{q} + 1 \geqslant 2\sqrt{q} + 2$. □

Exercise 9. *Prove that the arc constructed in Theorem 21 cannot be extended to a larger arc for* $q \geqslant 9$*.*

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

We denote by $\det_j(X_1, \ldots, X_{k-1})$ 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* $|S| \geqslant mt + k - 1$*, then there is a homogeneous polynomial in* *three variables* $\phi(Z)$*, of degree* mt*, which gives a polynomial* $G(X_1,\ldots,X_{k-1})$ *under the substitution* $Z_j = \det_j(X_1,\ldots,X_{k-1})$*, with the property that for all* $\{y_1,\ldots,y_{k-2}\} \subset S$

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

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

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

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

The proof is then the same as the proof of Theorem 18. □

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* $|S| \geqslant mt + k - 1$*, then* S *has a unique completion to a complete arc.*

Proof. As in the proof of Theorem 19. □

6. A new form

For an arc S of $\mathrm{PG}_2(\mathbb{F}_q)$ 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.*

Proof. Let $V = \Psi[X] \oplus \Phi[X]$ be the vector space of all homogeneous polynomials of degree t in three variables, where $\Phi[X]$ is the subspace of polynomials vanishing on the arc S. Consider the subspace

$$\Omega = \{(g(a))_{a\in S} \mid g \in V\}$$

of $\mathbb{F}_q^{|S|}$.

Let λ_a denote the a coordinate of a vector $\lambda \in \mathbb{F}_q^{|S|}$.

For each $\lambda \in \Omega^{\perp}$ and each $x \in S$ we have

$$\sum_{a \in S} \lambda_a f_a(x) = 0,$$

since, by Lemma 17, $f_a(x) = (-1)^{t+1} f_x(a)$ for all $a, x \in S$, and $f_x(a)$ is a homogeneous polynomial in a of degree t, by definition.

Define the subspace Π to be

$$\Pi = \{\lambda \in \Omega^{\perp} \mid \sum_{a \in S} \lambda_a f_a(X) \equiv 0\}.$$

Let U and W be subspaces of $\mathbb{F}_q^{|S|}$ such that $\Omega^{\perp} = \Pi \oplus W$ and $\Pi^{\perp} = \Omega \oplus U$. Observe that $\dim U = \dim W$ and let $m = \dim U$.

For each $i, j \in \{0, \ldots, t\}$, with $i + j \leqslant t$, we define a function f_{ij} from S to $\mathbb{F}_q$, where for each $a \in S$ the value of $f_{ij}(a)$ is the coefficient of $X_1^i X_2^j X_3^{t-i-j}$ of the polynomial $f_a(X)$, i.e.

$$f_a(X) = \sum_{i+j=0}^{t} f_{ij}(a) X_1^i X_2^j X_3^{t-i-j}.$$

For each $\lambda \in \Pi$,

$$\sum_{a \in S} \lambda_a f_{ij}(a) = 0,$$

so the vector $(f_{ij}(a))_{a \in S} \in \Pi^{\perp}$. We can write

$$f_{ij} = p_{ij} + h_{ij},$$

for some functions p_{ij} and h_{ij}, where $(p_{ij}(a))_{a \in S} \in \Omega$ and $(h_{ij}(a))_{a \in S} \in U$. Observe that the function p_{ij} is the evaluation of a homogeneous polynomial $p_{ij}[Y] \in \Psi[Y]$ of degree t.

Let $u_1, \ldots, u_m$ be functions from S to $\mathbb{F}_q$ such that $\{((u_1(a))_{a \in S}, \ldots, ((u_m(a))_{a \in S}\}$ is a basis for U. Then

$$f_{ij} = p_{ij} + \sum_{k=1}^{m} q_{ijk} u_k,$$

for some $q_{ijk} \in \mathbb{F}_q$.

For $\lambda \in W \setminus \{0\}$,

$$\sum_{a \in S} \lambda_a f_a(X),$$

is a non-zero polynomial vanishing at the points of S, so is an element of $\Phi[X]$.

Since $(p_{ij}(a))_{a\in S} \in \Omega \subseteq W^{\perp}$, we have

$$\sum_{a\in S} \lambda_a f_a(X) = \sum_{k=1}^{m} \left(\sum_{a\in S} \lambda_a u_k(a) \right) v_k(X), \quad \text{where} \quad v_k(X) = \sum_{i+j=0}^{t} q_{ijk} X_1^i X_2^j X_3^{t-i-j}.$$

Suppose that $\lambda, \lambda' \in W$ and that

$$\sum_{a\in S} \lambda_a f_a(X) = \sum_{a\in S} \lambda'_a f_a(X).$$

Then $\lambda - \lambda' \in \Pi$ and so $\lambda = \lambda'$. This implies that as λ ranges over the q^m elements in W, we obtain q^m different polynomials $\sum_{a\in S} \lambda_a f_a(X)$ in the subspace spanned by the m polynomials $v_1, \ldots, v_m$. Hence,

$$\{\sum_{a\in S} \lambda_a f_a(X) \mid \lambda \in W\} = \langle v_1(X), \ldots, v_m(X) \rangle,$$

and in particular $v_1, \ldots, v_m \in \Phi[X]$.

Let $g_{ij}(X) \in \Psi[X]$ be the polynomial such that $X_1^i X_2^j X_3^{t-i-j} = g_{ij}(X)$ modulo $\Phi[X]$.

Define a homogeneous polynomial of degree t in X and Y as

$$F(X,Y) = \sum_{i+j=0}^{t} p_{ij}(Y) g_{ij}(X),$$

Then, for all $a \in S$,

$$F(X,a) = \sum_{i+j=0}^{t} p_{ij}(a) g_{ij}(X) = \sum_{i+j=0}^{t} f_{ij}(a) g_{ij}(X) - \sum_{k=1}^{m} \sum_{i+j=0}^{t} q_{ijk} u_k(a) g_{ij}(X)$$

$$= \sum_{i+j=0}^{t} f_{ij}(a) X_1^i X_2^j X_3^{t-i-j} - \sum_{k=1}^{m} \sum_{i+j=0}^{t} q_{ijk} u_k(a) X_1^i X_2^j X_3^{t-i-j} \pmod{\Phi[X]}$$

$$= f_a(X) - \sum_{k=1}^{m} u_k(a) v_k(X) = f_a(X) \pmod{\Phi[X]}.$$

The proof of skew-symmetry and uniqueness are left as an exercise. □

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

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

$$(1,1,1), (1,-1,1), (-1,1,1), (-1,-1,1)\}$$

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

$$F(x,y) = 5(x_2^2x_3y_1^2y_3 + y_2^2y_3x_1^2x_3 + x_2x_3^2y_1^2y_2 + x_1^2x_2y_2y_3^2 + x_1x_3^2y_1y_2^2 + x_1x_2^2y_1y_3^2)$$
$$+6x_1x_2x_3y_1y_2y_3 + x_1^3y_1^3 + x_2^3y_2^3 + x_3^3y_3^3.$$

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 $i, j, k \in \{0, \ldots, t-1\}$ where $i+j+k \leqslant t-1$, define $\rho_{ijk}(Y)$ to be the coefficient of $X_1^iX_2^jX_3^k$ in

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

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

Proof. For all $a \in S$, the polynomial $f_a(X)$ is the product of t linear forms whose kernels contain the point a. Therefore, $f_a(X + a) = f_a(X)$. By Theorem 31, for each $a \in S$,

$$F(X + a, a) - F(X, a) = f_a(X + a) - f_a(X) = f_a(X) - f_a(X) = 0 \pmod{\Phi[X]}.$$

However, $F(X+a, a)-F(X, a)$ is a polynomial in X of degree at most $t-1$, so this is in fact zero. Hence, each coefficient of $F(X + Y, Y) - F(X, Y)$, written as a polynomial in X whose coefficients are polynomials in Y, is a (possibly zero) polynomial which vanishes 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 $x_3^4 = x_1^2x_2^2$, $x_2^4 = x_1^2x_3^2$ and $x_1^4 = x_3^2x_2^2$.

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

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 ϕ of degree at most $t + p^{\lfloor \log_p t\rfloor}$ which is hyperbolic on S.*

Proof. (for case $t < p$) Let

$$W = \{(w_1, w_2, w_3) \in \{0, \ldots, t-1\}^3 \mid w_1 + w_2 + w_3 = t - 1\}.$$

Let $\phi(Y)$ be the greatest common divisor of

$$\{\rho_w(Y) \mid w \in W\} \cup \Phi[Y].$$

Observe that the degree of ϕ is at most $t+1$. We do not yet discount the case that the first set and the second set contain only the zero polynomial. In this case, which we shall rule out, ϕ is the zero polynomial.

Let $F(X, Y)$ be a representative of the equivalence class of polynomials given by Theorem 31.

Let x and y be arbitrary points of S and let B be a basis, with respect to which, $x = (1, 0, 0)$ and $y = (0, 1, 0)$. Let $f_a^*(X)$ be the polynomial we obtain from $f_a(X)$ when we change the basis from the canonical basis to B, and likewise let $F^*(X, Y)$ be the polynomial we obtain from $F(X, Y)$, and let ϕ^* be the polynomial we get from ϕ.

Define homogeneous polynomials $b_{d_1 d_2 d_3}(Y)$ of degree t by writing

$$F^*(X, Y) = \sum_{d_1+d_2+d_3=t} b_{d_1 d_2 d_3}(Y) X_1^{d_1} X_2^{d_2} X_3^{d_3}.$$

Then

$$\begin{aligned} F^*(X+Y, Y) &= \sum_{d_1+d_2+d_3=t} b_{d_1 d_2 d_3}(Y)(X_1+Y_1)^{d_1}(X_2+Y_2)^{d_2}(X_3+Y_3)^{d_3}, \\ &= \sum_{d_1+d_2+d_3=t} b_{d_1 d_2 d_3}(Y) \binom{d_1}{i_1}\binom{d_2}{i_2}\binom{d_3}{i_3} X_1^{i_1} Y_1^{d_1-i_1} X_2^{i_2} Y_2^{d_2-i_2} X_3^{i_3} Y_3^{d_3-i_3}. \end{aligned}$$

Let $r_{ijk}(Y)$ be the coefficient of $X_1^i X_2^j X_3^k$ in $F^*(X+Y, Y) - F^*(X, Y)$. Then $r_{ijk}(Y)$ is a linear combination of the polynomials in the set $\{\rho_w^*(Y) \mid w_1 + w_2 + w_3 = i + j + k\}$, where $\rho_w^*(Y)$ is the polynomial we obtain from $\rho_w(Y)$, when we change the basis from the canonical basis to B.

Since $\phi(Y)$ is the greatest common divisor of

$$\{\rho_w(Y) \mid w \in W\} \cup \Phi[Y],$$

$\phi^*(Y)$ is a factor of all the polynomials in the set

$$\{r_w(Y) \mid w \in W\} \cup \Phi^*[Y],$$

where $\Phi^*[Y]$ is the subspace of homogeneous polynomials of degree t which are zero on S, with respect to the basis B.

Let $w=(i,t-i-1,0)$ and $i\in\{0,\ldots,t-1\}$. Then $w\in W$ and

$$r_w(Y)=\sum_{d_1+d_2+d_3=t}\binom{d_1}{t}\binom{d_2}{t-i-1}Y_1^{d_1-i}Y_2^{d_2-t+i+1}Y_3^{d_3}b_{d_1d_2d_3}(Y).$$

The polynomial ϕ^* is a factor of all these polynomials, so it is a factor of $Y_1^iY_2^{t-i-1}r_w(Y)$ and therefore,

$$\sum_{d=i}^{i+1}\binom{d}{i}\binom{t-d}{t-i-1}Y_1^dY_2^{t-d}b_{d,t-d,0}(Y)=0 \pmod{Y_3,\phi^*},$$

for alL $i\in\{0,\ldots,t-1\}$.

These equations imply, since $t<p$,

$$Y_1^tb_{t,0,0}(Y)+(-1)^{t+1}Y_2^tb_{0,t,0}(Y)=0 \pmod{Y_3,\phi^*}.$$

Note that if $\phi^*=0$ then $\rho_w=r_w=0$ for all $w\in W$, so the expression is also zero in this case.

By Theorem 31,

$$F(Y,x)=f_x(Y) \pmod{\Phi[Y]}.$$

With respect to the basis B this gives,

$$F^*(Y,x)=f_x^*(Y) \pmod{\Phi^*[Y]}.$$

Since $f_x^*(Y)$ is a polynomial in Y_2 and Y_3,

$$f_x^*(Y)=f_x^*(y)Y_2^t \pmod{Y_3}.$$

By Theorem 31,

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

so with respect to the basis B this gives,

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

This implies that

$$b_{t,0,0}(Y)=F^*(x,Y)=(-1)^{t+1}F^*(Y,x)=(-1)^{t+1}f_x^*(y)Y_2^t \pmod{\Phi^*[Y],Y_3}.$$

Similarly

$$b_{0,t,0}(Y)=(-1)^{t+1}f_y^*(x)Y_1^t \pmod{\Phi^*[Y],Y_3}.$$

Hence, we have that

$$Y_1^tY_2^t(f_x^*(y)+(-1)^{t+1}f_y^*(x))=0 \pmod{Y_3,\phi^*}.$$

By Lemma 16 and the fact that f_a and f_a^* define the same functions, this implies

$$2Y_1^tY_2^tf_x(y) = 0 \pmod{Y_3, \phi^*}.$$

By hypothesis q is odd, so the left-hand side is non-zero. Hence, this equation rules out the possibility that ϕ^* (and hence ϕ) is zero and we have proved that there is a curve of degree at most $t+1$ which contains S.

If the degree of ϕ is zero then there must be at least two co-prime polynomials of degree at most $t+1$ both of which are zero on S.

If the degree of ϕ is not zero then the above equation implies that

$$\phi^*(Y) = cY_1^iY_2^j \pmod{Y_3},$$

for some integers i, j such that $i + j = \deg\phi^* = \deg\phi$ and some $c \in \mathbb{F}_q$. With respect to the canonical basis this gives

$$\phi(Y) = \alpha(Y)^i\beta(Y)^j \pmod{\gamma(Y)},$$

where the kernel of the linear form γ is the line joining x and y and α and β are linear forms with the property that $\alpha(y) = 0$ and $\beta(x) = 0$. Thus, we have proved that if the kernel of a linear form γ is a bisecant to S then ϕ modulo γ factorises into two linear factors whose multiplicities sum to the degree of ϕ, i.e. ϕ is hyperbolic on S. □

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

Proof. Let r be the degree of ϕ. Observe that $r \geqslant 2$, since S is not a line. Also, we can assume that ϕ is not a p-th power, since we can replace ϕ by its p-th root and all the properties are preserved.

Choose a suitable basis so that $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$ are points of S.

Suppose every term of $\phi(X)$ is of the form $c_{ijk}X_1^iX_2^{jp}X_3^{kp}$. Since $\phi(X)$ is hyperbolic on S, $\phi(0,X_2,X_3) = c_{0jk}X_2^{jp}X_3^{kp}$, for some j and k. Hence $r = (j+k)p$. Considering any term with $i > 0$, it follows that p divides i. So ϕ is a p-th power, which it is not. Hence we can assume, without loss of generality, that some exponent of X_1 is not a multiple of p, some exponent of X_3 is not a multiple of p and that the degree of ϕ in X_3 is at most the degree of ϕ in X_1.

Let n be the degree of ϕ in X_1.

Write

$$\phi(X) = \sum_{j=0}^{n} X_1^{n-j} c_j(X_2, X_3),$$

where c_j is either zero or a homogeneous polynomial of degree $r-n+j$ and by assumption $c_0(X_2, X_3) \neq 0$.

Let $E = \{e \in \mathbb{F}_q \mid X_3 - eX_2$ is a bisecant and $c_0(X_2, eX_2) \neq 0\}$. Since the degree of c_0 is $r - n$ we have that $|E| \geqslant q - t - r + n$. Since $\phi(X)$ is hyperbolic on S, for all $e \in E$, there exists a d such that

$$\phi(X_1, X_2, eX_2) = (X_1 + dX_2)^n c_0(X_2, eX_2).$$

The coefficient of X_1^{n-j} implies that for $j = 1, \ldots, n$,

$$c_j(X_2, eX_2) = \binom{n}{j} d^j X_2^j c_0(X_2, eX_2).$$

If p divides n and j is not a multiple of p then $c_j(X_2, eX_2) = 0$ for all $e \in E$. Since the degree of c_j is at most r and $r \leqslant |E| - n + 1$, by hypothesis, $c_j(X_2, X_3) = 0$. But then this implies that each exponent of X_1 in a term of $\phi(X)$ is a multiple of p, a contradiction. Therefore, n is not a multiple of p.

For $e \in E$ and $j = 1$ we have that

$$c_1(X_2, eX_2) = ndX_2 c_0(X_2, eX_2).$$

Thus, for $j = 1, \ldots, n$, substituting for d we obtain

$$c_0(X_2, eX_2)^{j-1} c_j(X_2, eX_2) n^j = \binom{n}{j} c_1(X_2, eX_2)^j.$$

Hence, $h_j(e) = 0$, for all $e \in E$, where $h_j(Y)$ is a polynomial in $(\mathbb{F}_q[X_2])[Y]$ defined by

$$h_j(Y) = c_0(X_2, YX_2)^{j-1} c_j(X_2, YX_2) n^j - \binom{n}{j} c_1(X_2, YX_2)^j.$$

Suppose $n \geqslant 2$. Let m be the degree of the polynomial $h_2(Y)$. Then $m \leqslant 2(r - n + 1)$ since the degree of c_j is $r - n + j$, and $m \leqslant 2n$ since the degree of $c_j(X_2, X_3)$ in X_3 is at most n. To be able to conclude that h_2 is identically zero, we need $m \leqslant |E| - 1$, which is equivalent to $\min(3(r-n)+2, r+n) \leqslant q-t-1$. If $n \leqslant r-2$ then $r+n \leqslant 2r-2 \leqslant q-t-1$ by hypothesis. If $n = r - 1$ then $3(r - n) + 2 = 5 \leqslant q - t - 1$, since $|S| = q + 2 - t \geqslant 8$.

Therefore, $h_2(Y)$ is identically zero. This implies that the polynomial $c_0(X_2, YX_2)$ divides $c_1(X_2, YX_2)$ and so

$$c_1(X_2, YX_2) = (aX_2 + bYX_2)c_0(X_2, YX_2),$$

for some $a, b \in \mathbb{F}_q$. Hence,

$$h_j(Y) = c_0(X_2, YX_2)^{j-1}(c_j(X_2, YX_2)n^j - \binom{n}{j} c_0(X_2, YX_2)(aX_2 + bYX_2)^j).$$

But for each $e \in E$, the polynomial

$$c_j(X_2, YX_2)n^j - \binom{n}{j} c_0(X_2, YX_2)(aX_2 + bYX_2)^j,$$

is zero at $Y = e$. It has degree at most $r - n + j \leqslant r \leqslant |E| + 1 - n$ in Y, so we conclude that it is identically zero.

Substituting $Y = X_3/X_2$, we have that

$$c_j(X_2, X_3)n^j = \binom{n}{j} c_0(X_2, X_3)(aX_2 + bX_3)^j,$$

for $j = 1, \ldots, n$.

Hence,

$$\phi(X) = \sum_{j=0}^{n} \binom{n}{j} X_1^{n-j} c_0(X_2, X_3)(\frac{a}{n}X_2 + \frac{b}{n}X_3)^j,$$

and therefore

$$\phi(X) = c_0(X_2, X_3)(X_1 + \frac{a}{n}X_2 + \frac{b}{n}X_3)^n.$$

Suppose that there is a point $x \in S$ which is not in the zero-set of ϕ. Then when we consider any bisecant incident with x, since ϕ is hyperbolic on S, we have that ϕ is zero at all other points of S.

The above equation for ϕ implies that all but $r - n$ points of $S \setminus \{x\}$ are contained in a line, which gives $|S| - 1 \leqslant r - n + 2 \leqslant r$ and hence $q + 1 - t \leqslant \frac{1}{2}(q - t + 1)$, an inequality which is not valid.

Hence, $n = 1$. Since the degree of ϕ in X_3 is at most the degree of ϕ in X_1, this implies that the degree of ϕ in X_3 is one. Since ϕ is hyperbolic on S, $\phi(X_1, 0, X_3)$ is a constant times X_1X_3. Therefore, $r = 2$ and we have proved that ϕ is a quadratic form and that S is contained in a conic. $\square$

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 $t+p^{\lfloor \log_p t \rfloor}$.*

Proof. (of Theorem 30) Let $d = t + p^{\lfloor \log_p t \rfloor}$.

Suppose that $|S| \leqslant 2d$. Let $a_1, \ldots, a_d$ be linear forms whose kernels give a set L of lines which cover the points of S. Let $b_1, \ldots, b_d$ be another d linear forms whose kernels give a set of lines, disjoint from L, but which also cover the points of S. Let $a(X) = \prod_{i=1}^{d} a_i(X)$ and $b(X) = \prod_{i=1}^{d} b_i(X)$. Then the zero sets of $a(X)$ and $b(X)$ both contain S and $a(X)$ and $b(X)$ have no common factor, so we are done.

If $|S| \leqslant 7$ then the theorem holds almost trivially, since we can cover the points with a conic and a line in two ways (i.e. using different conics and different lines) and deduce that S is in the intersection of two cubics, which do not share a common component. Note that $t \geqslant 2$, since we are assuming that S is not contained in a conic.

Suppose that $|S| \geqslant 2d+1$ and $|S| \geqslant 8$. Then $q+2-t \geqslant 2(t+p^{\lfloor \log_p t \rfloor})+1$ which implies $\frac{1}{2}(q-t+1) \geqslant t + p^{\lfloor \log_p t \rfloor}$ and Lemma 28 applies.

If there is a non-zero homogeneous polynomial ϕ of degree at most $t+p^{\lfloor \log_p t \rfloor}$ which is hyperbolic on S then, by Lemma 29, S is contained in a conic. This is ruled out by hypothesis. Therefore, we have the other possibility given by Lemma 28, that there are two co-prime polynomials of degree at most $t+p^{\lfloor \log_p t \rfloor}$ which are zero on S, i.e. there are two curves of degree at most $t+p^{\lfloor \log_p t \rfloor}$, which do not share a common component, both containing S. $\square$

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

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

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

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

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

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

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

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

7. Proof of the MDS conjecture for prime fields

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

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

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

Observe that $\alpha_{C,E} \neq 0$.

Lemma 32. *Let* S *be an arc of* $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ *of size* $q+k-1-t \geqslant k+t$ *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* $\mathrm{PG}_{k-1}(\mathbb{F}_q)$*. If* $k \leqslant p$ *then* $|S| \leqslant q+1$*.*

Proof. Suppose that $|S| = q+2$. Let E be a subset of S of size $k+t = 2k-3$. Note that if $|S| < |E|$ then we can apply Corollary 13 and obtain an arc S of the same size with $|S| > |E|$.

Let F be a set of $k-2$ elements of E. For each $(k-2)$-subset A of E, let $r = |A \cap F|$. Then, by Lemma 32

$$\sum_{A \subset E} r!(k-2-r)!(-1)^r \sum_{C \supset A} \alpha_{C,E} = 0,$$

where the second sum runs over the $(k-1)$-subsets C of E. Changing the order of the summations,

$$\sum_{C \subset E} \alpha_{C,E} \sum_{A \subset C} r!(k-2-r)!(-1)^r = 0.$$

If $|C \cap F| = s \neq 0$ then

$$\sum_{A \subset C} s(s-1)!(k-1-s)!(-1)^{s-1} + (k-1-s)s!(k-2-s)!(-1)^s = 0.$$

Hence the only term left after summing the second sum if the term with $|C \cap F| = 0$, which gives

$$(k-1)!\alpha_{E \setminus F, E} = 0.$$

Since $\alpha_{E\setminus F,E} \neq 0$, we have a contradiction for $k \leqslant p$. $\square$

8. Classification of the largest arcs for $k \leqslant p$

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

Proof. Since S has size $q+1$, we have $k+t = 2k-2$. Let E be a subset of S of size $2k-2$ and F be a subset of E of size $k-2$ and sum together the equation in Lemma 32 as in the proof Theorem 33. This gives,

$$(k-1)! \sum_{C \subset E\setminus F} \alpha_{C,E} = 0.$$

Let $\{x\}$, K and L be disjoint subsets of S of size 1, k and $k-2$ respectively.

For each $w \in L$ consider the above equation with $E = K \cup \{x\} \cup (L \setminus \{w\})$ and $F = L \cup \{x\} \setminus W$. This gives

$$0 = (k-1)! \sum_{C \subset K} \alpha_{C,K\cup L} \frac{\det(w,C)}{\det(x,C)} = 0.$$

As w varies in L we get $k-2$ equations with variables $x_1^{-1}, \ldots, x_k^{-1}$, where $x = (x_1, \ldots, x_k)$ with respect to the basis K.

Since the element of L form an arc, these $k-2$ equation span a system of rank $k-2$ and we get equations of the form

$$c_i x_i^{-1} + c_j x_j^{-1} + c_m x_m^{-1} = 0,$$

for all $x \in S \setminus (K \cup L)$.

Since $|S \setminus (K \cup L)| \geqslant 3$, for each i, j, m the coefficients c_i, c_j, c_m are fixed by two points $x \in S \setminus (K \cup L)$. Now switching an element of L with a third point of $S \setminus (K \cup L)$ we conclude that the above equation is also zero for the elements of L and so

$$c_i x_j x_m + c_j x_i x_m + c_m x_i x_j = 0,$$

for all $x \in S$. Therefore the projection of S to the plane from any $k-3$ points of S is contained in a conic. It's an exercise to then prove that S is then a normal rational curve. $\square$

9. Extending small arcs to large arcs

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

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

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

Proof. Let $|G| = k+t+n$ and suppose that G extends to an arc S of size $q+k-1-t$.

Let U be a subset of G of size n. Then $E = G \setminus U$ is a subset of G of size $k+t$. By Lemma 32, for each subset A of E of size $k-2$,

$$\sum_{C \supset A} \alpha_{C,E} = 0,$$

where the sum runs over all $(k-2)$-subsets C of E containing A.

Then

$$\sum_{C \supset A} \alpha_{C,G} \prod_{u \in U} \det(u,C) = 0.$$

This system of equations is given by the matrix P_n and a solution v is a vector with C coordinate $\alpha_{C,G}$, which are all non-zero. □

Suppose that we do find a solution v to the system of equation. Then we know the value of $\alpha_{C,G}$ and therefore $f_A(x)$, where $C = A \cup \{x\}$. This would allow one to calcuate the polynomials $f_A(X)$ for each subset A of G of size $k-2$. Therefore, if G does extend to an arc S then each solution tells us precisely the tangents to S at each point of G.

By starting with a generic arc G of size $2k-2$ one can compute the rank of the matrix P_n and conclude the following theorem, which verifies the MDS conjecture for $k \leqslant 2p-2$.

Theorem 36. *Let S be an arc of $\mathrm{PG}_{k-1}(\mathbb{F}_q)$. If $k \leqslant 2p-2$ then $|S| \leqslant q+1$.*

By starting with a sub-arc G of size $3k-6$ of the normal rational curve one can again compute the rank of the matrix P_n and conclude the following theorem.

Theorem 37. *If G is a subset of the normal rational curve of $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ of size $3k-6$ and q is odd, then G cannot be extended to an arc of size $q+2$.*