ARCS AND TENSORS

SIMEON BALL AND MICHEL LAVRAUW

ABSTRACT. To an arc $\mathcal{A}$ of $\mathrm{PG}(k-1,q)$ of size $q+k-1-t$ we associate a tensor in $\langle \nu_{k,t}(\mathcal{A})\rangle^{\otimes k-1}$, where $\nu_{k,t}$ denotes the Veronese map of degree t defined on $\mathrm{PG}(k-1,q)$. As a corollary we prove that for each arc $\mathcal{A}$ in $\mathrm{PG}(k-1,q)$ of size $q+k-1-t$, which is not contained in a hypersurface of degree t, there exists a polynomial $F(Y_1,\ldots,Y_{k-1})$ (in $k(k-1)$ variables) where $Y_j=(X_{j1},\ldots,X_{jk})$, which is homogeneous of degree t in each of the k-tuples of variables Y_j, which upon evaluation at any $(k-2)$-subset S of the arc $\mathcal{A}$ gives a form of degree t on $\mathrm{PG}(k-1,q)$ whose zero locus is the tangent hypersurface of $\mathcal{A}$ at S, i.e. the union of the tangent hyperplanes of $\mathcal{A}$ at S. This generalises the equivalent result for planar arcs ($k=3$), proven in [2], to arcs in projective spaces of arbitrary dimension. A slightly weaker result is obtained for arcs in $\mathrm{PG}(k-1,q)$ of size $q+k-1-t$ which are contained in a hypersurface of degree t. We also include a new proof of the Segre-Blokhuis-Bruen-Thas hypersurface associated to an arc of hyperplanes in $\mathrm{PG}(k-1,q)$.

1. Introduction and motivation

An *arc* of $\mathrm{PG}(k-1,q)$ is a set of points no k of which are contained in a hyperplane. Arcs are the subject of Segre's fundamental problems proposed in 1955 [10] and they play an important role in Galois geometry [11]. Segre's celebrated result from [9] which says that an arc of size $q+1$ in $\mathrm{PG}(2,q)$, q odd, is a conic, has inspired many mathematicians to work on problems related to arcs in projective spaces over finite fields. Normal rational curves are well known examples of arcs of size $q+1$. There are arcs of size $q+2$ in $\mathrm{PG}(2,q)$ when q is even called *hyperovals*. For a list of the collineation groups of these arcs, see [8].

Another driving force for the study of arcs is the fact that they are equivalent to linear Maximum Distance Separable codes (MDS codes), which according to [7] form "one of the most fascinating chapters in all of coding theory". These codes have been extensively studied and a well-known conjecture (called the *MDS conjecture*) claims that if $4\leq k\leq q-2$, then a k-dimensional linear MDS code over the finite field with q elements has length at most $q+1$. The MDS conjecture was proven for q prime in [1].

The most recent result from [2] verifies the MDS conjecture for $k\leq\sqrt{q}-\sqrt{q}/p+2$, in the case that $q=p^{2h}$ and p is an odd prime. Contrary to most previous results in this direction

Date: 3 December 2018.

2010 *Mathematics Subject Classification.* 51E21, 94B05, 05B25.

The first author acknowledges the support of the project MTM2017-82166-P of the Spanish *Ministerio de Economía y Competitividad.*

(for example, the bounds from [5], [6], [12], [13], [14] and [15]) the result from [2] does not rely on Segre's algebraic envelope associated to an arc, and deep results on the number of points on algebraic curves over finite fields, in particular the Hasse-Weil theorem and the Stöhr-Voloch theorem. Instead, the results in [2] are based on the existence of a certain bi-homogeneous polynomial which upon evaluation at a point of the arc splits into linear factors corresponding to the tangents of the arc through that point. In this paper, this is generalised to arcs in projective spaces of arbitrary dimension, resulting in Theorem 1.

In Section 7 we compare this result to the hypersurface associated to an arc of hyperplanes as obtained in the sequence of papers [11] for $k = 3$, in [3] for $k = 4, 5$, and [4] for arbitrary dimension $k \geq 3$.

2. The tangent hypersurfaces and the main theorem

Throughout, $\mathcal{A}$ will be an arc of $\mathrm{PG}(k-1,q)$ of size $q+k-1-t$, arbitrarily ordered, and we identify each point of $\mathcal{A}$ with a fixed vector representative. Let $V_r[X]$ denote the vector space of forms (homogeneous polynomials) of degree r in $\mathbb{F}_q[X_1,\ldots,X_k]$, and $\Phi_r[X]$ the subspace of $V_r[X]$ consisting of forms vanishing on $\mathcal{A}$. As in the previous sentence we will often write X instead of $X_1,\ldots,X_k$.

Each subset S of size $k-2$ of $\mathcal{A}$ is contained in precisely t hyperplanes of $\mathrm{PG}(k-1,q)$ meeting $\mathcal{A}$ exactly in S (called *tangent S-hyperplanes*). Their union forms the *tangent hypersurface of $\mathcal{A}$ at S*. Each such hypersurface has degree t and is the zero locus of

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

where $\alpha_i(X)$, $i = 1,\ldots,t$, are linear forms whose kernels are the t tangent S-hyperplanes. This defines $f_S(X)$ up to a nonzero scalar factor, which we will now determine based on the evaluation of f_S at carefully chosen points of $\mathcal{A}$.

Let E be the set of the first $k-2$ elements of $\mathcal{A}$. For each $(k-2)$-subset $S \subset \mathcal{A}$, scale the polynomial $f_S(X)$ so that

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

where e is the first element of $E\setminus S$, a is the last element of $S\setminus E$, and s is the parity of the permutation which orders $S\cup\{e\}$ as in the ordering of $\mathcal{A}$ (to determine the value of s we assume the ordering of $\mathcal{A}$ for the subset S). With this notation it should be understood that the order is respected when taking the union of ordered sets, i.e. with "union" we mean the concatenation of the ordered sets.

We are now in a position to state the main result of this article.

Theorem 1. *Let $\mathcal{A}$ be an arc in $\mathrm{PG}(k-1,q)$ of size $q+k-1-t$ and let $\Phi_t[X]$ denote the space of homogeneous polynomials of degree t in $X = (X_1,\ldots,X_k)$ which are zero on $\mathcal{A}$. There exists a homogeneous polynomial $F(Y_1,\ldots,Y_{k-1})$ (in $k(k-1)$ variables) where*

$Y_j = (X_{j1}, \ldots, X_{jk})$, 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*
$$F(a_1, \ldots, a_{k-2}, X) = (-1)^{s(t+1)} f_S(X) \text{ modulo } \Phi_t[X],$$
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 $\Phi_t[Y_1]$, …, $\Phi_t[Y_{k-1}]$.*

The following three sections are mainly dedicated to proving Theorem 1.

3. The scaled coordinate-free lemma of tangents

In this section we prove what we call the *scaled coordinate-free lemma of tangents* for an arc in a projective space of arbitrary dimension. The original lemma of tangents is due to Segre [11]. A coordinate-free version was given in [1], and a scaled coordinate-free version for the planar case was introduced in [2].

As before, $\mathcal{A}$ is 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). Define the function g on ordered subsets of $\mathcal{A}$ of size $k-1$ by

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

where S is an ordered subset of $\mathcal{A}$ of size $k-2$ and s is the parity of the permutation which orders S as in the ordering of $\mathcal{A}$. Note that S is considered as an unordered set in the notation $f_S(a)$. Extend the definition of g by setting it equal to zero when evaluated at $(k-1)$-tuples with repeated elements. Recall that E consists of the first $k-2$ elements of $\mathcal{A}$.

Lemma 2. *If σ is a permutation in $\mathrm{Sym}(k-1)$ and T is an ordered $(k-1)$-subset of $\mathcal{A}$ containing E, then*
$$g(T^\sigma) = (-1)^{s(t+1)} g(T),$$
where s is the parity of the permutation σ.

Proof : If σ is a permutation in $\mathrm{Sym}(k-1)$ fixing $k-1$ then, by definition,

$$g(T^\sigma) = (-1)^{s(t+1)} g(T), \tag{4}$$

where s is the parity of the permutation σ.

So in order to prove the assertion is suffices to show that

$$g(a_1,\ldots,a_{k-3},a_{k-1},a_{k-2}) = (-1)^{t+1} g(a_1,\ldots,a_{k-1}),$$

for any distinct $a_1,\ldots,a_{k-1} \in \mathcal{A}$.

Pick any ordered subset $B = [a_1,\ldots,a_k] \subset \mathcal{A}$ of size k. Since $\mathcal{A}$ is an arc, it follows that B is a basis. Denote by $B_{l,i,j}$ the ordered set obtained from B by removing the l-th, the i-th and the j-th point from B and by $B_{l,i,j}(x,y)$ the ordered set of points obtained from B by removing the l-th point from B and replacing the i-th point by x and the j-th point by y.

Let $1 \le l < j < k$ be fixed. For $x, y \in \mathcal{A} \setminus B_{l,j,k}$ define

$$h(x,y) = g(B_{l,j,k}(x,y)).$$

Then for any point u, with coordinates $(u_1,\ldots,u_k)$ w.r.t. B, we have

$$h(a_l,u) = \prod_{i=1}^{t}(b_{ij}u_j + b_{ik}u_k), \quad h(a_j,u) = \prod_{i=1}^{t}(c_{il}u_l + c_{ik}u_k), \quad h(a_k,u) = \prod_{i=1}^{t}(d_{il}u_l + d_{ij}u_j),$$

for some $b_{ij}, c_{ij}, d_{ij} \in \mathbb{F}_q$.

Let $B_{l,j}$ denote the ordered set of points obtained from B by removing the l-th and the j-th point. With respect to the basis B, the hyperplane containing $\langle B_{l,j}\rangle$ and $s = (s_1, s_2, \ldots, s_k) \in \mathcal{A} \setminus B$ is the kernel of the linear form $X_l - (s_l/s_j)X_j$. Since these hyperplanes are distinct from the tangent $(B_{l,j})$-hyperplanes, together they constitute all hyperplanes containing $B_{l,j}$, except the kernels of the linear forms X_l and X_j. Hence,

$$\prod_{i=1}^{t}\frac{d_{ij}}{d_{il}} \prod_{s\in\mathcal{A}\setminus B}\frac{-s_l}{s_j} = \prod_{d\in\mathbb{F}_q\setminus\{0\}} d = -1.$$

Observing that $h(a_k,a_j) = \prod_{i=1}^{t} d_{ij}$ and $h(a_k,a_l) = \prod_{i=1}^{t} d_{il}$, this gives

$$h(a_k,a_j)\prod_{s\in\mathcal{A}\setminus B} s_l = (-1)^{|\mathcal{A}\setminus B|+1} h(a_k,a_l)\prod_{s\in\mathcal{A}\setminus B} s_j.$$

Similarly, by considering hyperplanes through $B_{l,k}$,

$$h(a_j,a_l)\prod_{s\in\mathcal{A}\setminus B} s_k = (-1)^{|\mathcal{A}\setminus B|+1} h(a_j,a_k)\prod_{s\in\mathcal{A}\setminus B} s_l.$$

and by considering hyperplanes through $B_{j,k}$,

$$h(a_l,a_k)\prod_{s\in\mathcal{A}\setminus B} s_j = (-1)^{|\mathcal{A}\setminus B|+1} h(a_l,a_j)\prod_{s\in\mathcal{A}\setminus B} s_k.$$

Combining these three equations, and observing that $(-1)^{|\mathcal{A}\setminus B|+1} = (-1)^{t+1}$, we obtain

$$h(a_j, a_l) = (-1)^{t+1} \quad h(a_l, a_j) \quad \frac{h(a_j, a_k)h(a_k, a_l)}{h(a_k, a_j)h(a_l, a_k)}.$$

We can rewrite this as

$$g(B_k^{(jl)}) = (-1)^{t+1} g(B_k) \frac{g(B_l)g(B_j^{(lk)})}{g(B_l^{(jk)})g(B_j)} \tag{5}$$

where B_l is obtained from B by removing the l-th vector, and with the understanding that B_l^σ denotes the result of removing the l-th vector from B after applying the permutation $\sigma \in Sym(k)$ to the k positions.

Consider any $k-1$ distinct points $a_1, \ldots, a_{k-1}$, and put $T = [a_1, \ldots, a_{k-1}]$. If $E = [e_1, \ldots, e_{k-2}] = [a_1, \ldots, a_{k-2}]$ then by the definition of g and the scaling (2) of the tangent forms $f_S(X)$ we have

$$g(a_1, \ldots, a_{k-1}) = g(e_1, \ldots, e_{k-2}, a_{k-1}) = f_E(a_{k-1}) = (-1)^{(k-2)(t+1)} f_{T_1}(e_1).$$

This is equal to

$$(-1)^{(k-2)(t+1)} g(e_2, \ldots, e_{k-2}, a_{k-1}, e_1) = (-1)^{(t+1)} g(a_{k-1}, e_2, \ldots, e_{k-2}, e_1)$$

where the last equality was obtained by applying (4).

Likewise, for any $j \in \{2, \ldots, k-1\}$ we obtain

$$f_E(a_{k-1}) = (-1)^{(k-1-j)(t+1)} f_{T_j}(e_j)$$

which is equal to

$$(-1)^{(k-1-j)(t+1)} g(e_1, \ldots, e_{j-1}, e_{j+1}, \ldots, e_{k-2}, a_{k-1}, e_j),$$

and by applying (4) we obtain

$$g(e_1, \ldots, e_{k-2}, a_{k-1}) = (-1)^{(t+1)} g(e_1, \ldots, e_{j-1}, a_{k-1}, e_{j+1}, \ldots, e_{k-2}, e_j).$$

We have shown that for any $T = [e_1, \ldots, e_{k-2}, a_{k-1}]$,

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

for any transposition $\sigma = (j, k-1)$. In combination with (4) this proves the lemma. □

Next we formulate and prove the main result of this section.

Lemma 3. *[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.

Proof : We will prove this by induction on the size of $T \setminus E$ (as sets), where E consists of the first $k-2$ elements of $\mathcal{A}$.

If $|T \setminus E| = 1$ then the lemma follows from Lemma 2.

Suppose that for each ordered $(k-1)$-tuple T for which $T \setminus E$ has size at most $r \geq 1$, we have

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

for any transposition $\sigma \in \mathrm{Sym}(k-1)$.

Consider an ordered $(k-1)$-tuple $T = [a_1, \ldots, a_{k-1}]$ with $T \setminus E$ of size $r+1$. Let e_η denote the first point in $E \setminus T$ in the ordering of $\mathcal{A}$, and put $B = [a_1, \ldots, a_{k-1}, e_\eta]$.

Suppose that $a_{k-2}, a_{k-1} \notin E$. Then the left hand side of (5), with $j = k-2$ and $l = k-1$, becomes

$$g(B_k^{(jl)}) = g(a_1, \ldots, a_{k-3}, a_{k-1}, a_{k-2})$$

while the right hand side equals

$$(-1)^{t+1} g(B_k) \frac{g(a_1, \ldots, a_{k-3}, a_{k-2}, e_\eta) g(a_1, \ldots, a_{k-3}, e_\eta, a_{k-1})}{g(a_1, \ldots, a_{k-3}, e_\eta, a_{k-2}) g(a_1, \ldots, a_{k-3}, a_{k-1}, e_\eta)},$$

which by the induction hypothesis equals

$$(-1)^{t+1} g(B_k) = (-1)^{t+1} g(a_1, \ldots, a_{k-3}, a_{k-2}, a_{k-1}),$$

since $B_l \setminus E$ and $B_j \setminus E$ are of size r. This proves that if the points of T in position $k-2$ and $k-1$ do not belong to E then

$$g(T^\sigma) = (-1)^{t+1} g(T) \tag{6}$$

for the transposition $\sigma = (k-2, k-1)$.

Next, suppose $a_{k-2} \in E$ and $a_{k-1} \notin E$ is the last point of T in the ordering of $\mathcal{A}$. Let e_η denote the first point in $E \setminus (T \setminus \{a_{k-2}\})$, in the ordering of $\mathcal{A}$.

Let $S = \{a_1, \ldots, a_{k-3}, a_{k-1}\}$. By the scaling (2) of the tangent forms $f_S(X)$ we have

$$f_S(e_\eta) = (-1)^{s(t+1)} f_{S \setminus \{a_{k-1}\} \cup \{e_\eta\}}(a_{k-1}), \tag{7}$$

where s is the number of transpositions needed to reorder $S \cup \{e_\eta\}$ as in the ordering of $\mathcal{A}$. Moreover, by the definition of g, we have

$$f_S(e_\eta) = (-1)^{s_1(t+1)} g(a_1, \ldots, a_{k-3}, a_{k-1}, e_\eta),$$

where s_1 is the number of transpositions needed to reorder $[a_1, \ldots, a_{k-3}, a_{k-1}]$ as in the ordering of $\mathcal{A}$, and

$$f_{S \setminus \{a_{k-1}\} \cup \{e_\eta\}}(a_{k-1}) = (-1)^{s_2(t+1)} g(a_1, \ldots, a_{k-3}, e_\eta, a_{k-1})$$

where s_2 is the number of transpositions needed to reorder $[a_1, \ldots, a_{k-3}, e_\eta]$ as in the ordering of $\mathcal{A}$. Since a_{k-1} is the last point of T in the ordering of $\mathcal{A}$ we have

$$s_2 \equiv s_1 + s - 1 \mod 2$$

and therefore

$$(-1)^{s_1(t+1)}(-1)^{s(t+1)}(-1)^{s_2(t+1)} = (-1)^{(t+1)}.$$

Combining this with (7) we obtain

$$g(a_1, \ldots, a_{k-3}, a_{k-1}, e_\eta) = (-1)^{(t+1)} g(a_1, \ldots, a_{k-3}, e_\eta, a_{k-1}). \tag{8}$$

Let B denote the ordered k-tuple obtained from T by adding the point e_η. With $j = k-2$ and $l = k-1$, the induction hypothesis implies

$$g(B_l) = (-1)^{(t+1)} g(B_l^{(jk)})$$

since $B_l \setminus E$ has size r, and by (8)

$$g(B_j) = (-1)^{(t+1)} g(B_j^{(lk)}).$$

Therefore by (5), with $j = k-2$ and $l = k-1$ we obtain $g(B_k^{(jl)}) = (-1)^{(t+1)} g(B_k)$, i.e.

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

for the transposition $\sigma = (k-2, k-1)$.

Next suppose $a_{k-2} \in E$, $a_{k-1} \notin E$ and a_{k-1} is not the last point of T, in the ordering of $\mathcal{A}$. If a_j is the last point of T in the ordering of $\mathcal{A}$, then consider the transpositions $\tau = (j, k-2)$ and $\sigma = (k-2, k-1)$. Applying the permutation $\tau\sigma\tau\sigma\tau$ to T we get

$$T^{\tau\sigma\tau\sigma\tau} = [a_1, \ldots, a_j, \ldots, a_{k-1}, a_{k-2}]$$

which is T^σ. Moreover, the first time that σ is applied, the pair of points in the last two positions is (a_j, a_{k-1}), consisting of two points of $T \setminus E$, and therefore by (6) this gives a factor $(-1)^{(t+1)}$ to the evaluation of g. The second time σ is applied, the pair of points in the last two positions is (a_{k-2}, a_j) where $a_{k-2} \in E$ and a_j is the last point of T in the ordering of $\mathcal{A}$, and so, this time by (7), this gives a factor $(-1)^{(t+1)}$ to the evaluation of g.

Finally, by (5), each of the three applications of τ also gives a factor $(-1)^{(t+1)}$. This amounts to a total of five factors $(-1)^{(t+1)}$, and we may conclude that also in this case

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

for the transposition $\sigma = (k-2, k-1)$.

Thus, we have proved that if $a_{k-2} \in E$ and $a_{k-1} \notin E$ or if $a_{k-2} \notin E$ and $a_{k-1} \in E$ then

$$g(T^\sigma) = (-1)^{t+1} g(T) \tag{9}$$

for the transposition $\sigma = (k-2, k-1)$.

Finally suppose that both elements $a_{k-2}, a_{k-1} \in E$. Let a_j ($j \in \{1, \ldots, k-3\}$) be a point of $T \setminus E$ and consider the transpositions $\tau = (j, k-2)$, and $\sigma = (k-2, k-1)$. Then, similarly as above we have $T^{\tau\sigma\tau\sigma\tau} = T^\sigma$, which this time also making use of (9) implies

$$g(T^\sigma) = (-1)^{t+1} g(T). \tag{10}$$

This concludes the proof. □

4. A tensor associated with an arc

In this section we show how the coordinate-free lemma of tangents can be used to construct a particular tensor which will eventually lead to our main result Theorem 1. Let $\nu_{k,t}$ denote the *Veronese map of degree t*

$$\nu_{k,t} \ : \ \mathrm{PG}(k-1,q) \to \mathrm{PG}(N-1,q) \ : \ x=(x_1,\ldots,x_k) \mapsto (\ldots,x^I,\ldots),$$

where $N=\binom{k+t-1}{t}$. Under this map, the image of a point x is the point whose coordinate vector consists of all possible monomials x^I of degree t in $x_1,\ldots,x_k$. Thus, a coordinate of the image of x is of the form $x^I=x_1^{d_1}\cdots x_k^{d_k}$, where $d_1+\cdots+d_k=t$. The image of the Veronese map is an algebraic variety, called the *Veronese variety*, and is denoted by $\mathcal{V}_{k,t}(\mathbb{F}_q)$.

For each ordered $(k-2)$-subset $S\subset\mathcal{A}$ we consider the associated linear form $h_S\in\mathbb{F}_q[Z_1,\ldots,Z_N]$ defined by

$$h_S\circ\nu_{k,t}=f_S. \tag{11}$$

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

$$h(\nu_{k,t}(a_1),\nu_{k,t}(a_2),\ldots,\nu_{k,t}(a_{k-1})):=g(a_1,a_2,\ldots,a_{k-1}). \tag{12}$$

A *t-socle* for $\mathcal{A}$ is a set of points of $\mathcal{A}$ whose image under the Veronese map of degree t spans the subspace spanned by $\mathcal{A}$ under the Veronese map. So a t-socle is a set of points $e_1,\ldots,e_m\in\mathcal{A}$ for which

$$\langle\nu_{k,t}(e_1),\ldots,\nu_{k,t}(e_m)\rangle=\langle\nu_{k,t}(\mathcal{A})\rangle.$$

We define the function $\bar{h}$ from $\langle\nu_{k,t}(\mathcal{A})\rangle^{\otimes k-1}$ to $\mathbb{F}_q$ by

$$\bar{h}\left(\sum_{i_1}c_{1i_1}\nu_{k,t}(e_{i_1})\otimes\sum_{i_2}c_{2i_2}\nu_{k,t}(e_{i_2})\otimes\ldots\otimes\sum_{i_{k-1}}c_{1i_{k-1}}\nu_{k,t}(e_{i_{k-1}})\right)$$

$$:=\sum_{i_1}c_{1i_1}\sum_{i_2}c_{2i_2}\ldots\sum_{i_{k-1}}c_{1i_{k-1}}g(e_{i_1},\ldots,e_{i_{k-1}}),$$

where each sum is from $i_j=1,\ldots,m$.

We will show that for each $a_1,\ldots,a_{k-1}\in\mathcal{A}$,

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

Lemma 4. *The function $\bar{h}$ defines a multilinear form on $\langle \nu_{k,t}(\mathcal{A})\rangle^{\otimes k-1}$ whose restriction to*

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

equals h.

Proof : By definition, the function $\bar{h}$ is multilinear, and coincides with h when evaluated at arguments of the form

$$\mathbf{v} = \left(\nu_{k,t}(e_{i_1}), \nu_{k,t}(e_{i_2}), \ldots, \nu_{k,t}(e_{i_{k-1}})\right).$$

For each $x \in \mathcal{A}$ with $\nu_{k,t}(x) = \sum_i \lambda_i \nu_{k,t}(e_i)$, and for each $j \in \{1, \ldots, k-2\}$, we have

$$\begin{aligned} &h\left(\nu_{k,t}(e_{i_1}), \ldots, \nu_{k,t}(e_{i_{j-1}}), \nu_{k,t}(x), \nu_{k,t}(e_{i_{j+1}}), \ldots, \nu_{k,t}(e_{i_{k-1}})\right) \\ &= g(e_{i_1}, \ldots, e_{i_{j-1}}, x, e_{i_{j+1}}, \ldots, e_{i_{k-2}}, e_{i_{k-1}}) \\ &= (-1)^{t+1} g(e_{i_1}, \ldots, e_{i_{j-1}}, e_{i_{k-1}}, e_{i_{j+1}}, \ldots, e_{i_{k-2}}, x) \\ &= (-1)^{t+1} h_E(\nu_{k,t}(x)) \\ &= (-1)^{t+1} \sum_i \lambda_i h_E(\nu_{k,t}(e_i)) \end{aligned}$$

where $E = [e_{i_1}, \ldots, e_{i_{j-1}}, e_{i_{k-1}}, e_{i_{j+1}}, \ldots, e_{i_{k-2}}]$. This in turn equals

$$\begin{aligned} &\sum_i \lambda_i (-1)^{t+1} g(e_{i_1}, \ldots, e_{i_{j-1}}, e_{i_{k-1}}, e_{i_{j+1}}, \ldots, e_{i_{k-2}}, e_i) \\ &= \sum_i \lambda_i g(e_{i_1}, \ldots, e_{i_{j-1}}, e_i, e_{i_{j+1}}, \ldots, e_{i_{k-2}}, e_{i_{k-1}}) \\ &= \sum_i \lambda_i \bar{h}\left(\nu_{k,t}(e_{i_1}) \otimes \ldots \otimes \nu_{k,t}(e_{i_{j-1}}) \otimes \nu_{k,t}(e_i) \otimes \nu_{k,t}(e_{i_{j+1}}) \otimes \ldots \otimes \nu_{k,t}(e_{i_{k-1}})\right) \\ &= \bar{h}\left(\nu_{k,t}(e_{i_1}) \otimes \ldots \otimes \nu_{k,t}(e_{i_{j-1}}) \otimes \nu_{k,t}(x) \otimes \nu_{k,t}(e_{i_{j+1}}) \otimes \ldots \otimes \nu_{k,t}(e_{i_{k-1}})\right). \end{aligned}$$

This shows that $\bar{h}$ and h are equal when evaluated at arguments obtained from

$$\mathbf{v} = \left(\nu_{k,t}(e_{i_1}), \nu_{k,t}(e_{i_2}), \ldots, \nu_{k,t}(e_{i_{k-1}})\right),$$

by replacing the j-th argument in $\mathbf{v}$ by $\nu_{k,t}(x)$ ($x \in \mathcal{A}$).

The proof can now be finished by induction. As induction hypothesis we assume that the values of $\bar{h}$ and h are equal when evaluated at $(k-1)$-tuples obtained from $\mathbf{v}$ by replacing $s \geq 1$ of the arguments of $\mathbf{v}$ by $\nu_{k,t}(x_1), \ldots, \nu_{k,t}(x_s)$ for any s points $x_1, \ldots, x_s \in \mathcal{A}$.

Let $\mathbf{w}$ be obtained from $\mathbf{v}$, by replacing $s+1$ of the arguments of $\mathbf{v}$ by expressions of the form $\nu_{k,t}(x_1), \ldots, \nu_{k,t}(x_{s+1})$ where $x_1, \ldots, x_{s+1} \in \mathcal{A}$.

If $\nu_{k,t}(x_{s+1})$ is not in the last position of $\mathbf{w}$, then define $\mathbf{w}'$ as the $(k-1)$-tuple obtained from $\mathbf{w}$ by interchanging the argument where x_{s+1} appears with the argument in the last position. Then, by Lemma 3,

$$h(\mathbf{w}) = (-1)^{t+1} h(\mathbf{w}').$$

If $\nu_{k,t}(x_{s+1})$ is in the last position of $\mathbf{w}$ then put $\mathbf{w}' = \mathbf{w}$.

Then $h(\mathbf{w}') = h_E(\nu_{k,t}(x_{s+1}))$ for a suitable E, and since h_E is a linear form, we can rewrite $h(\mathbf{w}')$ as a linear combination of evaluations of h at $(k-1)$-tuples obtained from $\mathbf{v}$ by replacing s arguments of $\mathbf{v}$ by expressions of the form $\nu_{k,t}(x_1), \ldots, \nu_{k,t}(x_s)$ with $x_1, \ldots, x_s \in \mathcal{A}$. By induction the values of $\bar{h}$ and h are equal when evaluated at such $(k-1)$-tuples. □

5. Proof of Theorem 1

The previous sections contain the necessary lemma's to prove the main theorem. We restate the theorem for the convenience of the reader.

Theorem 1 *Let $\mathcal{A}$ be an arc in $\mathrm{PG}(k-1,q)$ of size $q+k-1-t$ and let $\Phi_t[X]$ denote the space of homogeneous polynomials of degree t in $X = (X_1, \ldots, X_k)$ which are zero on $\mathcal{A}$. 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*

$$F(a_1, \ldots, a_{k-2}, X) = (-1)^{s(t+1)} f_S(X) \text{ modulo } \Phi_t[X],$$

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 $\Phi_t[Y_1]$, …, $\Phi_t[Y_{k-1}]$.*

Proof :

Let $\mathcal{A}$ be an arc of size $q+k-1-t$ in $\mathrm{PG}(k-1,q)$. By Lemma 4, there exists a multilinear form $\bar{h}$ on $\langle \nu_{k,t}(\mathcal{A}) \rangle^{\otimes k-1}$, such that for all $a_1, \ldots, a_{k-1} \in \nu_{k,t}(\mathcal{A})$

$$\bar{h}(\nu_{k,t}(a_1), \ldots, \nu_{k,t}(a_{k-1})) = g(a_1, \ldots, a_{k-1}) = (-1)^{s(t+1)} f_S(a_{k-1}),$$

where $S = [a_1, \ldots, a_{k-2}]$ is an ordered subset of $\mathcal{A}$ and s is the parity of the permutation which orders S as in the ordering of $\mathcal{A}$.

The multi-linear form $\bar{h}$ corresponds to a hyperplane $\bar{\mathcal{H}}$ in $\langle \nu_{k,t}(\mathcal{A}) \rangle^{\otimes k-1}$. Let $\mathcal{H}$ be a hyperplane of $\langle \mathcal{V}_{k,t}(\mathbb{F}_q) \rangle^{\otimes k-1}$ intersecting $\langle \nu_{k,t}(\mathcal{A}) \rangle^{\otimes k-1}$ in $\bar{\mathcal{H}}$.

The hyperplane $\mathcal{H}$ is the zero locus of a linear form α on $\langle \mathcal{V}_{k,t}(\mathbb{F}_q)\rangle^{\otimes k-1}$. This defines α up to a nonzero scalar factor. Now scale α such that the restriction of α to $\langle \nu_{k,t}(\mathcal{A})\rangle^{\otimes k-1}$ coincides with $\overline{h}$ (which is possible since $\mathcal{H} \cap \langle \nu_{k,t}(\mathcal{A})\rangle^{\otimes k-1} = \bar{\mathcal{H}}$).

Denote by φ the polynomial map from

$$\mathrm{PG}(k-1,q) \times \ldots \times \mathrm{PG}(k-1,q) \longrightarrow \mathrm{PG}(N^{k-1}-1,q),$$

where $N = \binom{k+t-1}{t}$, obtained as the composition of first applying the Veronese map

$$\nu_{k,t} \ : \ \mathrm{PG}(k-1,q) \longrightarrow \mathrm{PG}(N-1,q),$$

in each of the $k-1$ factors, and then applying the Segre embedding

$$\sigma \ : \ \mathrm{PG}(N-1,q) \times \ldots \times \mathrm{PG}(N-1,q) \longrightarrow \mathrm{PG}(N^{k-1}-1,q).$$

Define F as the polynomial map $\alpha \circ \varphi$. It follows that F is a homogeneous polynomial $F(Y_1,\ldots,Y_{k-1})$ where $Y_j = (Y_{j1},\ldots,Y_{jk})$, which is homogeneous (of degree t) in each of the Y_j's. Moreover,

$$F(a_1,\ldots,a_{k-1}) = (\alpha \circ \varphi)(a_1,\ldots,a_{k-1}) = g(a_1,\ldots,a_{k-1})$$

For an ordered subset $S = [a_1,\ldots,a_{k-2}]$ of $\mathcal{A}$, consider

$$H(X) := F(a_1,\ldots,a_{k-2},X) - (-1)^{s(t+1)} f_S(X),$$

a homogeneous polynomial of degree t.

The polynomial $H(X)$ vanishes at the points of $\mathcal{A}$ and therefore belongs to $\Phi_t[X]$, which proves (i).

For $S = [a_1,\ldots,a_{k-2}]$, where $a_i \in \mathcal{A}$ and for which one of the a_i's is repeated,

$$F(a_1,\ldots,a_{k-2},a_{k-1}) = g(a_1,\ldots,a_{k-2},a_{k-1}) = 0,$$

which proves (ii).

To prove (iii) it suffices to prove that

$$F(X_2,X_1,X_3,\ldots,X_{k-1}) = (-1)^{t+1} F(X_1,X_2,X_3,\ldots,X_{k-1}) \pmod{\Phi_t[X_1],\ldots,\Phi_t[X_{k-1}]},$$

the other transpositions following by the same argument.

By induction on r we will prove that

$$F(a_1,a_2,a_3,\ldots,a_r,X_{r+1},\ldots,X_{k-1}) = (-1)^{t+1} F(a_2,a_1,a_3,\ldots,a_r,X_{r+1},\ldots,X_{k-1})$$

modulo $(\Phi_t[X_{r+1}],\ldots,\Phi_t[X_{k-1}])$.

This holds for $r = k-1$ (in which case there are no X_i's) by Lemma 3.

By induction, whenever we evaluate at $X_r = a_r \in \mathcal{A}$, the polynomial

$$F(a_1,a_2,a_3,\ldots,a_{r-1},X_r,X_{r+1},\ldots,X_{k-1}) - (-1)^{t+1} F(a_2,a_1,a_3,\ldots,a_{r-1},X_r,X_{r+1},\ldots,X_{k-1})$$

is zero modulo $(\Phi_t[X_{r+1}],\ldots,\Phi_t[X_{k-1}])$. Hence, it is zero modulo $(\Phi_t[X_r],\ldots,\Phi_t[X_{k-1}])$, which proves (iii).

To prove (iv), suppose that both F and G are polynomials satisfying (i), (ii) and (iii). Then

$$F(a_1,\ldots,a_{k-2},Y_{k-1}) = G(a_1,\ldots,a_{k-2},Y_{k-1}) \pmod{\Phi_t[Y_{k-1}]}.$$

for any $[a_1,\ldots,a_{k-2}]$, where $a_j \in \mathcal{A}$ are possibly repeated.

We proceed by induction. Suppose that for all $[a_1,\ldots,a_r]$, where $a_j \in \mathcal{A}$ are possibly repeated,

$$F(a_1,\ldots,a_r,Y_{r+1},\ldots,Y_{k-1}) = G(a_1,\ldots,a_r,Y_{r+1},\ldots,Y_{k-1}) \pmod{\Phi_t[Y_{r+1}],\ldots,\Phi_t[Y_{k-1}]}.$$

Then, evaluating Y_r at any point of $\mathcal{A}$, the polynomial

$$F(a_1,\ldots,a_{r-1},Y_r,\ldots,Y_{k-1}) - G(a_1,\ldots,a_{r-1},Y_r,\ldots,Y_{k-1}),$$

is zero $\pmod{\Phi_t[Y_{r+1}],\ldots,\Phi_t[Y_{k-1}]}$, which implies that

$$F(a_1,\ldots,a_{r-1},Y_r,\ldots,Y_{k-1}) = G(a_1,\ldots,a_{r-1},Y_r,\ldots,Y_{k-1}) \pmod{\Phi_t[Y_r],\ldots,\Phi_t[Y_{k-1}]}.$$

This complete the proof. □

Definition 1. *The multi-homogeneous polynomial $F(Y_1,\ldots,Y_{k-1})$ where $Y_j = (Y_{j1},\ldots,Y_{jk})$, which is homogeneous (of degree t) in each of the Y_j's, is called a* tensor form of $\mathcal{A}$. *Note that a tensor form of an arc is unique modulo the ideals of forms of degree t vanishing on $\mathcal{A}$ in each of the k-tuples of variables $Y_1,\ldots,Y_{k-1}$.*

6. Hypersurfaces containing an arc

Suppose $q = p^h$, where p is an odd prime. Let $\mathcal{A}$ be an arc in $\mathrm{PG}(k-1,q)$ of size $q+k-1-t$ and let S be a subset of $\mathcal{A}$ of size $k-3$. Projecting $\mathcal{A}$ from S one obtains a planar arc and the results from [2] apply. These results imply that $\mathcal{A}$ is contained in a hypersurface of degree $t+p^{\lfloor \log_p t\rfloor}$, which is the cone of a planar curve of degree $t+p^{\lfloor \log_p t\rfloor}$ and the subspace $\langle S\rangle$.

The following theorem implies that there may be more hypersurfaces containing $\mathcal{A}$. Indeed, we will consider a specific example in which Theorem 5 tells us more than what we obtain from simply projecting.

In the following, $X^{(i_1,\ldots,i_k)} = X_1^{i_1}\cdots X_k^{i_k}$.

Theorem 5. *Let $\mathcal{A}$ be an arc in $\mathrm{PG}(k-1,q)$ of size $q+k-1-t$ and let $F(Y_1,\ldots,Y_{k-1})$ be the $(t,t,\ldots,t)$-form whose existence is given by Theorem 1. If $\mathcal{A}$ is not contained in a hypersurface of degree t then the coefficient of $Y_1^{i_1}\cdots Y_{k-2}^{i_{k-2}}$, where $i_m = (i_{m1},\ldots,i_{mk})$, in*

$$F(Y_1+X,\ldots,Y_{k-2}+X,X) - F(Y_1,\ldots,Y_{k-2},X)$$

is a homogeneous polynomial in X of degree at most

$$(k-1)t - \sum_{m=1}^{k-2}\sum_{j=1}^{k} i_{mj},$$

which is zero on $\mathcal{A}$.

Proof. Let $x \in \mathcal{A}$ and define $F_x(Y_1, \ldots, Y_{k-2})$ as the F we obtain by applying Theorem 1 to the arc $\overline{\mathcal{A}}$ obtained by projecting $\mathcal{A}$ from x. Explicitly, this can be done in the following way.

Choose a coordinate j such that $x_j \neq 0$. For each $a = (a_1, \ldots, a_k) \in \mathcal{A}$, define a point $\overline{a}$ of $\mathrm{PG}(k-2, q)$, whose i-th coordinate is $a_i x_j - a_j x_i$, for $i \neq j$. So $\overline{a}$ has no j-th coordinate.

Let

$$\overline{\mathcal{A}} = \{\overline{a} \mid a \in \mathcal{A} \setminus \{x\}\}.$$

Theorem 1 implies the existence of a form $G(Z_1, \ldots, Z_{k-2})$ for $\overline{\mathcal{A}}$. Note that each Z_{mi} has not j-th coordinate. Then define F_x as the polynomial obtained from G by substituting $Z_{mi} = x_j Y_{mi} - x_i Y_{mj}$ for $i \neq j$.

Since Z_{mi} is unaffected by the substitution $Y_{mi} \mapsto Y_{mi} + x_i$

$$F_x(Y_1 + x, \ldots, Y_{k-2} + x) = F_x(Y_1, \ldots, Y_{k-2}).$$

Both $F_x(Y_1, \ldots, Y_{k-2})$ and $F(Y_1, \ldots, Y_{k-2}, x)$ satisfy all the properties of the F-form obtained by applying Theorem 1 to the arc $\overline{\mathcal{A}}$, apart from the fact that each Y_j is a k-tuple and not a $(k-1)$-tuple. However, the same uniqueness argument used in part (iv) of the proof of Theorem 1 applies, so they are the same.

Therefore, for all $x \in \mathcal{A}$,

$$F(Y_1 + x, \ldots, Y_{k-2} + x, x) = F(Y_1, \ldots, Y_{k-2}, x),$$

from which the theorem follows. □

We now consider an example which illustrates that Theorem 5 can prove the existence of hypersurfaces containing $\mathcal{A}$ which are not obtained simply by projection.

Theorem 6. *If q is odd then an arc of size $q+1$ in $\mathrm{PG}(3, q)$ is contained in a quadric.*

Proof. Suppose that $\mathcal{A}$ is an arc of $\mathrm{PG}(3, q)$ of size $q+1$ not contained in a quadric. Then $k = 4$, $t = 2$ and $\Phi_t = \{0\}$.

By Theorem 1, there is a $(2, 2, 2)$-form

$$F(Y_1, Y_2, Y_3) = \sum_{j_1, j_2, j_3} b_{j_1, j_2, j_3} Y_1^{j_1} Y_2^{j_2} Y_3^{j_3},$$

where the sum goes over all $j_m = (j_{m1}, j_{m2}, j_{m3}, j_{m4})$ such that $j_{m1} + j_{m2} + j_{m3} + j_{m4} = 2$, with the properties therein stated.

Since $t+1$ is odd, and $\Phi_t = \{0\}$, Theorem 1 (iii) implies

$$b_{j_1, j_2, j_3} = -b_{j_1, j_3, j_2}.$$

Since $F_{e_1}(Y_1, Y_2)$ has no Y_{11} or Y_{21} terms

$$b_{(2,0,0,0), j_2, j_3} = 0,$$

if $j_{11} \neq 0$ or $j_{21} \neq 0$.

Applying Theorem 5 to the coefficient $Y_1^{(2,0,0,0)}Y_2^{(0,1,0,0)}$, we have that the polynomial

$$2X_2 f_{e_1e_2}(X_3,X_4) + (b_{(2,0,0,0),(0,1,1,0),(0,0,1,1)} + b_{(2,0,0,0),(0,1,0,1),(0,0,2,0)})X_3^2X_4 \\ +(b_{(2,0,0,0),(0,1,0,1),(0,0,1,1)} + b_{(2,0,0,0),(0,1,1,0),(0,0,0,2)})X_3X_4^2 \tag{13}$$

defines a hypersurface containing $\mathcal{A}$.

Note that it is not zero, since q is odd and $f_{e_1e_2}(X_3,X_4) \neq 0$.

Applying Theorem 5 to the coefficient $Y_1^{(0,2,0,0)}Y_2^{(1,0,0,0)}$, we have that the polynomial

$$2X_1 f_{e_1e_2}(X_3,X_4) + (b_{(0,2,0,0),(1,0,1,0),(0,0,1,1)} + b_{(0,2,0,0),(1,0,0,1),(0,0,2,0)})X_3^2X_4 \\ +(b_{(0,2,0,0),(1,0,0,1),(0,0,1,1)} + b_{(0,2,0,0),(1,0,1,0),(0,0,0,2)})X_3X_4^2 \tag{14}$$

defines a hypersurface containing $\mathcal{A}$.

Then dividing $X_1(13) - X_2(14)$ by X_3X_4 we have that there is a polynomial

$$c_{13}X_1X_3 + c_{14}X_1X_4 + c_{23}X_2X_3 + c_{24}X_2X_4,$$

which is zero on $\mathcal{A}$. Again, this polynomial is not zero since this would imply that $2X_2 f_{e_1e_2}(X_3,X_4)$ is zero on $\mathcal{A}$, which it is not.

Hence, $\mathcal{A}$ is contained in a quadric. □

7. The Segre-Blokhuis-Bruen-Thas hypersurface

In this section we elaborate on the hypersurface associated to an arc of hyperplanes in $\mathrm{PG}(k-1,q)$ obtained in [11] for $k=3$, in [3] for $k=4,5$, and [4] for arbitrary dimension $k \geq 3$. We will give a new proof for its existence and compare this result with Theorem 1.

For $j = 1,\ldots,k-1$ consider $X_j = (X_{j1},\ldots,X_{jk})$ as a k-tuple of indeterminates. We denote by

$$\det_i(X_1,\ldots,X_{k-1})$$

the determinant of the matrix which is obtained from the matrix with the X_j's as rows and the i-th column deleted.

The main theorem of [4] implies that there is a homogeneous polynomial $\phi(Z_1,\ldots,Z_k)$ of degree t for q even and of degree $2t$ for q odd, which vanishes at the points of the dual space which are dual to the hyperplanes containing exactly $k-2$ points of an arc $\mathcal{A}$. We paraphrase the main result of [4] as follows.

Theorem 7. *Let $m \in \{1,2\}$ be such that $m-1 \equiv q$ modulo 2. If $\mathcal{A}$ is an arc in $\mathrm{PG}(k-1,q)$ of size $q+k-1-t$, where $|\mathcal{A}| \geq mt+k-1$, then there is a homogeneous polynomial in k variables $\phi(Z_1,\ldots,Z_k)$, of degree mt, which gives a polynomial $G(X_1,\ldots,X_{k-1})$ in $k(k-1)$ indeterminates under the substitution $Z_j = \det_j(X_1,\ldots,X_{k-1})$, with the property that for each $(k-2)$-subset $S = \{y_1,\ldots,y_{k-2}\}$ of $\mathcal{A}$*

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

Proof. Order the arc $\mathcal{A}$ arbitrarily and let E be a subset of $\mathcal{A}$ of size $mt+k-1$. Define

$$G(X_1,\dots,X_{k-1}) = \sum_T \left(f_{T\setminus\{a_{k-1}\}}(a_{k-1})\right)^m \prod_{u\in E\setminus T} \frac{\det(X_1,\dots,X_{k-1},u)}{\det(a_1,\dots,a_{k-1},u)}. \tag{15}$$

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

Observe that G can be obtained from a homogeneous polynomial of degree mt in $Z_1,\dots,Z_k$ under the change of variables $Z_j=\det_j(X_1,\dots,X_{k-1})$.

For $S=\{y_1,\dots,y_{k-2}\}$ define

$$h_S(X) := G(y_1,\dots,y_{k-2},X).$$

Note that $h_S(X)$ is well-defined since any reordering of S can only ever multiply $h_S(X)$ by $(-1)^{mt}=1$.

For $S\subset E$, the only nonzero terms in $h_S(X)$ are obtained for subsets T of E containing S. Therefore

$$h_S(X) = \sum_{a\in E\setminus S} (f_S(a))^m \prod_{u\in E\setminus(S\cup\{a\})} \frac{\det(y_1\dots,y_{k-2},X,u)}{\det(y_1,\dots,y_{k-2},a,u)}.$$

The evaluation of $h_S(X)$ at $x\in E$ is equal to zero if $x\in S$ and equal to $(f_S(x))^m\neq 0$ otherwise. Since, with respect to a basis containing S both f_S^m and h_S are homogeneous polynomials in two variables of degree mt, we conclude that $h_S=f_S^m$.

If S is not contained in E then we proceed by induction on the size of $S\setminus E$. As induction hypothesis we assume that for each subset S with $S\setminus E$ of size r the polynomials h_S and f_S^m are equal. Let $S=\{y_1,\dots,y_{k-2}\}$ be such that $S\setminus E$ is of size $r+1$. W.l.o.g. assume $y_{k-1}\notin E$. Then for $x\in E$ we have

$$h_S(x) = (-1)^{mt} h_{S'}(y_{k-1}) = h_{S'}(y_{k-1}),$$

where S' is the set obtained from S by replacing the $(k-1)$-th element y_{k-1} of S by x. On the other hand, by the definition (3) of g and the scaled coordinate-free lemma of tangents, we have

$$(f_S(x))^m = (g(y_1,\dots,y_{k-1},x))^m = (g(y_1,\dots,y_{k-2},x,y_{k-1}))^m = (f_{S'}(y_{k-1}))^m.$$

By induction $h_{S'}(y_{k-1}) = (f_{S'}(y_{k-1}))^m$, and therefore the polynomials h_S and f_S^m have the same evaluation at points in E. Applying the same argument as in the case where $S\subset E$ we obtain $h_S=f_S^m$. □

We now compare Theorem 7 to Theorem 1. First, observe that the polynomial G as defined in (15) is homogeneous of degree mt in each of its k-tuples of variables, and G takes the value zero when evaluated at an argument which contains repeated points. Next, by Theorem 7, for any subset $S=\{a_1,\dots,a_{k-2}\}$ of $\mathcal{A}$ we have $G(a_1,\dots,a_{k-1},X) = (f_S(X))^m$. Also, as we already explained in the proof of Theorem 7, it follows from the

scaled coordinate-free lemma of tangents that the polynomial G it is not affected by reordering of the points in its arguments. We obtain the following theorem.

Theorem 8. *Let $m \in \{1, 2\}$ be such that $m - 1 \equiv q$ modulo 2. If $\mathcal{A}$ is an arc in $\mathrm{PG}(k-1, q)$ of size $q + k - 1 - t$, where $|\mathcal{A}| \geq mt + k - 1$, then there exists a polynomial $G(Y_1, \ldots, Y_{k-1})$ (in $k(k-1)$ variables) which is homogeneous of degree mt in each of the k-tuples of variables Y_j, with the following properties.*

(i) *$G(a_1, \ldots, a_{k-2}, X) = (f_S(X))^m$ for every $(k-2)$-subset $S = \{a_1, \ldots, a_{k-2}\}$ of $\mathcal{A}$;*
(ii) *$G(a_1, \ldots, a_{k-1}) = 0$ if $a_i = a_j$ for some $i \neq j$;*
(iii) *G is symmetric in its $k-1$ arguments $Y_1, \ldots, Y_{k-1}$;*

Note that for q even, Theorem 8 is an improvement of Theorem 1. It proves that the modulo $\Phi_t[X]$ is not necessary in Theorem 1 for q even, although the uniqueness would not be valid without the modulo $\Phi_t[X]$. For q odd, Theorem 8 has the advantage that its properties hold true without the modulo $\Phi_t[X]$; the disadvantage is that the degree of G in each of its k-tuples of arguments is $2t$ whereas for the form F from Theorem 1 it is only t. We do not believe that the modulo $\Phi_t[X]$ is necessary in Theorem 1 for q odd although, as in the q even case, the uniqueness would not be valid without the modulo $\Phi_t[X]$.

References

[1] S. Ball, On sets of vectors of a finite vector space in which every subset of basis size is a basis, *J. Eur. Math. Soc.*, **14** (2012) 733–748.
[2] S. Ball and M. Lavrauw, Planar arcs, *J. Combin. Theory Ser. A.*, **160** (2018) 261–287.
[3] A. Blokhuis, A. A. Bruen and J. A. 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.* **92** (1988) 441–459.
[4] A. Blokhuis, A. A. Bruen and J. A. Thas, Arcs in $PG(n, q)$, MDS-codes and three fundamental problems of B. Segre - some extensions, *Geom. Dedicata*, **35** (1990) 1–11.
[5] J. W. P. Hirschfeld and G. Korchmáros, On the embedding of an arc into a conic in a finite plane, *Finite Fields Appl.*, **2** (1996) 274–292.
[6] J. W. P. Hirschfeld and G. Korchmáros, On the number of rational points on an algebraic curve over a finite field, *Bull. Belg. Math. Soc. Simon Stevin*, **5** (1998) 313–340.
[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.
[8] T. Penttila and I. Pinneri, Hyperovals, *Australasian J. Combin*, **19** (1999) 101–114.
[9] B. Segre, Ovals in a finite projective plane, *Canad. J. Math.*, **7** (1955) 414–416.
[10] B. Segre, Curve razionali normali e k-archi negli spazi finiti, *Ann. Mat. Pura Appl.*, **39** (1955) 357–379.
[11] B. Segre, Introduction to Galois geometries, *Atti Accad. Naz. Lincei Mem.*, **8** (1967) 133–236.
[12] J. F. Voloch, On the completeness of certain plane arcs, *European J. Combin.*, **8** (1987) 453–456.
[13] J. F. Voloch, On the completeness of certain plane arcs II, *European J. Combin.*, **11** (1990) 491–496.
[14] J. F. Voloch, Arcs in projective planes over prime fields, *J. Geom.*, **38** (1990) 198–200.
[15] J. F. Voloch, Complete arcs in Galois planes of non-square order, in: *Advances in Finite Geometries and Designs*, Oxford University Press, Oxford, 1991, pp. 401–406.

Simeon Ball,
Departament de Matemàtiques,
Universitat Politècnica de Catalunya,
Mòdul C3, Campus Nord,
c/ Jordi Girona 1-3,
08034 Barcelona, Spain
simeon@ma4.upc.edu

Michel Lavrauw,
Faculty of Engineering and Natural Sciences,
Sabancı University,
Istanbul, Turkey
mlavrauw@sabanciuniv.edu