On $(q+t,t)$-arcs of type $(0,2,t)$

András Gács* and Zsuzsa Weiner **

May 17, 2006

Abstract

In this paper we construct an infinite series of $(q+t,t)$-arcs of type $(0,2,t)$. We show that this construction includes the Korchmáros-Mazzocca arcs, and we gain new infinite series of examples, too.

1 Introduction

A $(q+t,t)$-*arc of type* $(0,2,t)$ is a set of $q+t$ points in $\mathrm{PG}(2,q)$ meeting every line in 0, 2 or t points. It can be considered as a generalization of hyperovals or as a small example for a set without tangents. We also suppose $t > 2$ (the $t = 2$ case is just the class of hyperovals).

In the next lemma we summarize some easy consequences of the definiton, for a proof see Korchmáros and Mazzocca [3].

Lemma 1.1 *Suppose that $\mathcal{K}$ is a $(q+t,t)$-arc of type $(0,2,t)$ in $\mathrm{PG}(2,q)$.*

(i) q is even;

(ii) the number of t-secants is $\frac{q}{t}+1$ (hence t divides q);

(iii) through any point of $\mathcal{K}$ there is one t-secant and q 2-secants.

In [3] the authors construct an infinite series of examples whenever the field $\mathrm{GF}(\frac{q}{t})$ is a subfield of $\mathrm{GF}(q)$. Before recalling it, we need a definition.

Definition 1.2 *For a function f over the finite field $\mathrm{GF}(q)$ we say that f determines the direction $c \in \mathrm{GF}(q)$, if $f(x) - c \cdot x$ is not a permutation of the field.*

*Research was partially supported by OTKA Grant F-030737, FKFP Grant 0063/2001 and the Magyary scholarship from "Alapítvány a Magyar Felsőoktatásért és Kutatásért"

**Research was partially supported by OTKA Grants F-030737, T-032455 and FKFP Grant 0063/2001

Construction 1.3 [Korchmáros-Mazzocca][3]

Assume that q is even. Suppose g is an o-polynomial over $\mathrm{GF}(q)$*, that is the point set* $\mathcal{H} = \{(g(x), x, 1) : x \in \mathrm{GF}(q)\} \cup \{(1, 0, 0), (0, 1, 0)\}$ *forms a hyperoval in* $\mathrm{PG}(2, q)$ *and let* T *be the following point set of* $\mathrm{AG}(2, q^h)$*,* $h > 1$*:*

$$T := \{(g(\mathrm{Tr}(a)), a, 1) : a \in \mathrm{GF}(q)\},$$

where $\mathrm{Tr}(a) = a + a^q + a^{q^2} + \ldots + a^{q^{h-1}}$.

Then T together with the q^{h-1} directions not determined by T forms a (q^h+q^{h-1}, q^{h-1})-arc of type $(0, 2, q^{h-1})$ in $\mathrm{PG}(2, q^h)$.

In Sections 3 and 4 we give a more general construction for $(q+t, t)$-arcs of type $(0, 2, t)$ including the previous ones. In some cases we will need the fact that such a set has a *t-nucleus* (that is the t-secants go through a common point). Korchmáros and Mazzocca, using algebraic geometry, prove this with a technical condition on q and t, though they conjecture that it should be true in general. In Section 2, using the Rédei polynomial instead of algebraic curves, we give a short proof for this fact.

Let us close this introduction with some remarks about the Rédei polynomial of a point set in $\mathrm{AG}(2, q)$. We use the usual Cartesian coordinate system in $\mathrm{AG}(2, q)$, that is points will be identified with ordered pairs (u, v) coming from $\mathrm{GF}(q)$, while lines of slope m have equation $v = mu + c$, finally vertical lines have equation $u = c$.

Let $U = \{(a_i, b_i) : i = 1, ..., n\}$ be a set of points in $\mathrm{AG}(2, q)$. The *Rédei polynomial of U* is the following polynomial in two variables:

$$H(X, Y) = \Pi_{i=1}^{n}(X + a_i Y - b_i).$$

In the next lemma we summarize the properties of the polynomial $H(X, Y)$. For a proof and for more about $H(X, Y)$, see Sziklai and Szőnyi [5].

Lemma 1.4 *(i) Considering H as a polynomial of X, we have $H(X, Y) = X^n + h_1(Y)X^{n-1} + ... + h_n(Y)$, where for every $1 \leq i \leq n$, h_i is a polynomial in Y of degree at most i.*

(ii) Fixing a $Y = y_0$, $H(X, y_0)$ is a polynomial in one variable with the property, that $X = x_0$ is a root with multiplicity m if and only if the line with equation $v = y_0u + x$ meets U in m points.

Finally, $\mathrm{PG}(2, q)$ will be represented as $\mathrm{AG}(2, q)$ completed with the line at infinity. The infinite point corresponding to the lines with slope m will be denoted by (m), while (∞) will denote the improper point of vertical lines.

In one case we will use the representation of points of $\mathrm{AG}(2, q)$ as elements of $\mathrm{GF}(q^2)$, where directions correspond to $(q + 1)$-st roots of unity in the following way: the slope (direction) of the line joining x and y is $(x - y)^{q-1}$. For more about this representation see Hirschfeld [2].

2 The existence of the t-nucleus

In this section we prove that the t-secants of any $(q+t,t)$-arc $\mathcal{K}$ of type $(0,2,t)$ have a nucleus, that is they go through a common point. The key ingredient of the proof will be a lemma proving that the coordinates of points of $\mathcal{K}$ on a t-secant have as many zero power sums as possible. Since this property seems to be interesting on its own right, we give a general definition.

Definition 2.1 *Let q be a power of 2 and $1 < t|q$. We say that $T = \{y_1, ..., y_t\} \subseteq \mathrm{GF}(q)$ is a Vandermonde-set, if $\sum_i y_i^k = 0$ for all $1 \leq k \leq t-2$.*

Note that this property is invariant under the transformation $y \to ay + b$ $(a \neq 0)$. Also note that a t-set cannot have one more zero power sum. This is an easy consequence of the fact that a Vandermonde-determinant cannot be zero.

In the next proposition we characterize the Vandermonde-property.

Proposition 2.2 *Let $T = \{y_1, ..., y_t\} \subseteq \mathrm{GF}(q)$, where q is an even prime power and suppose $1 < t|q$. The following are equivalent*

(i) T is a Vandermonde set;

(ii) in the polynomial $f(Y) = \Pi_{i=1}^{t}(Y - y_i)$ all coefficients of odd degree are zero besides that of Y;

(iii) the polynomial $\chi(Y) = \sum_{i=1}^{t}(Y - y_i)^{q-1}$ has degree $q - t$.

Proof: The coefficients of χ are the power sums of the set T, so (i) and (iii) are clearly equivalent. The equivalence of (i) and (ii) is an easy consequence of the Newton formulas relating power sums and elementary symmetric polynomials. □

Note that the function χ in (iii) is the characteristic function of T, that is it is 1 on T and 0 everywhere else.

Now we give two examples for a Vandermonde set.

Example 2.3 *Let q be an even prime power.*

(i) Any additive subgroup of $\mathrm{GF}(q)$ is a Vandermonde set.

(ii) Consider the points of $\mathrm{AG}(2,q)$ as elements of $\mathrm{GF}(q^2)$. Any q-set corresponding to the affine part of a hyperoval with two infinite points is a Vandermonde set in $\mathrm{GF}(q^2)$.

Proof:

(i) Suppose T is an additive subgroup of size t in $\mathrm{GF}(q)$. We want to prove that Proposition 2.2 (ii) is satisfied, that is $f(Y) = \Pi_{y \in T}(Y - y)$ has only terms of even degree except for the term Y. By [2] Lemma 8.38 if we prove that f is additive, hence $\mathrm{GF}(2)$-linear, then this implies that f has only terms of degree a power of 2.

Consider the polynomial in two variables $F(X,Y) = f(X)+f(Y)-f(X+Y)$. First of all note that it has full degree at most t and that the coefficient of X^t and Y^t is zero. Considering F as a polynomial in X, we have

$$F(X,Y) = h_1(Y)X^{t-1} + h_2(Y)X^{t-2} + \ldots + h_t(Y),$$

where $h_i(Y)$ $(i = 1, \ldots t)$ is a polynomial in Y of degree at most i (and $\deg(h_t) \leq t-1$). Now $F(X,y) \equiv 0$ for any $y \in T$ (as a polynomial of X), so all h_i-s have at least t roots. Since their degree is smaller than this number, they are zero identically, so we have $F(X,Y) \equiv 0$, hence f is additive.

(ii) Let $\{x_1, ..., x_q\} \subseteq \mathrm{GF}(q^2)$ correspond to the affine part of the hyperoval $\mathcal{H}$ and ϵ_1 and ϵ_2 be $(q+1)$-st roots of unity corresponding to the two infinite points. Consider the polynomial $\chi(x) = \sum_{i=1}^{q}(x-x_i)^{q-1}$. For any point x out of the hyperoval every line through x meets $\mathcal{H}$ in an even number of points, and since $(x-x_i)^{q-1}$ represents the slope of the line joining the affine points x and x_i, we have that $\chi(x) = \epsilon_1 + \epsilon_2$ for any $x \notin \{x_1, ..., x_q\}$. There are $q^2 - q$ different choices for such an x, while the degree of χ is at most $q-2$, so $\chi(x) \equiv \epsilon_1 + \epsilon_2$ identically (that is, all coefficients of χ are zero except for the constant term), so by Proposition 2.2 (iii), we are done. □

Now we are ready to state the key tool of our proof:

Proposition 2.4 *Suppose $\mathcal{K}$ is a $(q+t,t)$-arc of type $(0,2,t)$ having t points on the line at infinity, $\{(y_1),(y_2),...,(y_t)\}$, say. If the y-axis is also a t-secant, then the set $\{y_1,y_1,...,y_t\}$ is a Vandermonde-set.*

Proof: First of all note that (∞) cannot be in $\mathcal{K}$, since it would contradict Lemma 1.1.

Let $U = \{(a_i,b_i) : i = 1,...,q\}$ be the affine part of $\mathcal{K}$. Suppose $a_1 = ... = a_t = 0$ and consider the Rédei polynomial of U. According to Lemma 1.4 and to the properties of $\mathcal{K}$, for a fixed $Y \neq y_i$, the polynomial $H(X,y_i)$ is a square, while for $Y = y_i$ $(i = 1,..,t)$, $H(X,y_i) = X^q - X$. This means that the coefficient polynomial $h_{q-1}(Y)$ is 1 on the set $T = \{y_1,...,y_t\}$ and zero elsewhere (note that since the characteristic is two, we have $1 = -1$). This is also true about the polynomial $\chi(Y) = \sum_{i=1}^{t}(Y-y_i)^{q-1}$, so since these polynomials have degree at most $q-1$, they have to be the same. On the other hand (using that $a_1 = ... = a_t = 0$), the Y-degree of H and hence also of h_{q-1} is at most $q-t$, so using Proposition 2.2 (iii), we are done. □

Theorem 2.5 *The t-secants of a $(q+t,t)$-arc of type $(0,2,t)$ have a nucleus.*

Proof: Suppose to the contrary that (after transformation) the line at infinity and the two axes are t-secants.

Let $T = \{(y_1),...,(y_t)\}$ be the intersection of the arc and the line at infinity. According to Proposition 2.4, T is a Vandermonde-set. On the other hand the affine transformation switching the two affine coordinates (that is $(u,v) \to (v,u)$) (which extends to the ideal line as $(y) \to (1/y)$) replaces the two axes with each other, while the set T is replaced by $T' = \{1/y_1,...,1/y_t\}$ (note that (0) and (∞) cannot be in T). It follows that again

by Proposition 2.4, T' is also a Vandermonde set. So we have that $\sum_i y_i^k = 0$ for any $1 \leq k \leq t-2$ and for any $q-t+1 \leq k \leq q-2$.

Now consider the polynomial $\chi(Y) = \sum_{i=1}^{t}(Y - y_i)^{q-1}$. According to Propositions 2.4 and 2.2, it has degree $q-t$ and it has $q-t$ different roots (the complement of T). On the other hand, since $\sum_i y_i^k = 0$ for any $q-t+1 \leq k \leq q-2$, it is divisible by Y^t, which means that 0 is a root of multiplicity at least t. This is a contradiction. □

3 The construction

3.1 Geometric approach

In this subsection we give a geometric way of constructing $(q+t,t)$-arcs of type $(0,2,t)$. To do this first we need to extend the idea of projecting from a point to projecting from a subspace.

Definition 3.1 *Let π be an m-dimensional and P be an $(n-m-1)$-dimensional subspace in $\mathrm{PG}(n,q)$, $\pi \cap P = \emptyset$. Take a point S from $\mathrm{PG}(n,q) \setminus P$. The $(n-m)$-dimensional subspace $\langle P, S\rangle$ intersects π in a unique point S', that will be called the projection of S from P onto π.*

The crucial step in our construction is that we project a point set of a subgeometry from a subspace not intersecting the subgeometry. In general, it is very difficult to control the points that will project onto the same point. The next lemma shows, that in some special cases this can be done easily.

Lemma 3.2 *Let M be an $(h+1)$-dimensional subgeometry of order q in $\mathrm{PG}(h+1,q^h)$. Assume that R is an $(h-1)$-dimensional subspace of M and let R^* be the unique $(h-1)$-dimensional subspace of $\mathrm{PG}(h+1,q^h)$ that contains R.*

(i) There exists an $(h-2)$-dimensional subspace P in R^* such that P does not intersect the subgeometry M.

(ii) An $(h-1)$-dimensional subspace containing P different from R^* intersects the subgeometry M in 0 or 1 point.

(iii) Project the subgeometry M from P onto a plane π ($\pi \cap P = \emptyset$) of $\mathrm{PG}(h+1,q^h)$ to obtain M'. Then there is a one-to-one correspondence between the points of $M \setminus R$ and their projection. The subspace R projects onto the unique common point R' of R^* and π.

(iv) Let l be a line in π. Then the pre-image of $l \cap M'$ is a hyperplane (of the subgeometry M) containing R or a line (of M) skew to R, according as the point R' was on the line l or not.

Proof: Note that to block every hyperplane of R^* we need at least q^h+1 points. Now (i) is straightforward, since R has only $\frac{q^h-1}{q-1}$ points.

Let L be an $(h-1)$-dimensional subspace containing P and different from R^*. Assume to the contrary, that there are two different points, Q and S, lying in $L \cap M$. Since P, Q

and S are in L, the line $\langle Q, S\rangle$ intersects P and so S is in the hyperplane $H = \langle Q, R^*\rangle$. The hyperplane H intersects M in a hyperplane h of the subgeometry (since the intersection contains R and the point Q not in R). Considering h only, we get that the subline containing Q and S must intersect R. Hence $R^* \cap \langle Q, S\rangle$ contains a point of R and a point of P, too. This means that the line $\langle Q, S\rangle$ is in R^* and so $L \equiv R^*$, which contradicts our assumption.

Pick a point S' of M'. The pre-image of S' is the intersection of $\langle S', P\rangle$ and M; hence *(iii)* follows from *(ii)*.

The points of M that project onto a line l of π are the points of $\langle l, P\rangle \cap M$. Remark that this intersection always contains a line of M. To see this note that over $\mathrm{GF}(q)$, $\langle l, P\rangle$ is an $(h+1)h$-dimensional, M is an $(h+2)$- and $\mathrm{PG}(h+1, q^h)$ is an $(h+2)h$-dimensional vector space, hence the intersection of $\langle l, P\rangle$ and M is at least a 2-dimensional vector space over $\mathrm{GF}(q)$. To show *(iv)* note that if $\langle l, P\rangle \cap M$ contains a point of R^*, then it contains the entire R. □

In the next geometrical construction we start from a point set $\mathcal{D}$ of $\mathrm{PG}(2, q)$ and obtain a point set $\mathcal{D}'$ of $\mathrm{PG}(2, q^h)$, so that knowing the intersection numbers of $\mathcal{D}$ with respect to lines, we will be able to control the intersection of $\mathcal{D}'$ with lines. This construction is a generalization of a 3-dimensional one used in [4] for obtaining planar blocking sets.

Construction 3.3 *Choose a plane α in $\mathrm{PG}(h+1, q)$, where $h > 1$. Let $\mathcal{D}$ be a point set in α. Choose an $(h-2)$-dimensional subspace V in $\mathrm{PG}(h+1, q) \setminus \alpha$. Construct the cone $\mathcal{C}$ with vertex V and base $\mathcal{D}$. Now embed $\mathrm{PG}(h+1, q)$ into $\mathrm{PG}(h+1, q^h)$ as a subgeometry. Let Q be a point of α and let R be the $(h-1)$-dimensional subspace in $\mathrm{PG}(h+1, q)$ spanned by V and Q. Denote by R^* the unique $(h-1)$-dimensional subspace in $\mathrm{PG}(h+1, q^h)$ that contains R. Assume that P is an $(h-2)$-dimensional subspace in $R^* \setminus \mathrm{PG}(h+1, q)$. (For the existence of such a subspace, see 3.2 (i).) Project $\mathcal{C} \setminus R$ from P onto an arbitrary plane π of $\mathrm{PG}(h+1, q^h)$ to obtain $\mathcal{D}'$.* □

First of all note, that by Lemma 3.2 the size of $\mathcal{D}'$ is $|\mathcal{D}|q^{h-1}$, when $Q \notin \mathcal{D}$ and $(|\mathcal{D}|-1)q^{h-1}$, when $Q \in \mathcal{D}$. To find the intersection numbers of $\mathcal{D}'$ with lines (by Lemma 3.2) one has to find the intersection of $\mathcal{C} \setminus R$ with lines (of $\mathrm{PG}(h+1, q)$) skew to R and with hyperplanes (of $\mathrm{PG}(h+1, q)$) containing R. A line skew to R is skew to the vertex V, too, hence it can be projected from V onto the plane α. Note, that these projected lines are always skew to Q. So in this case the intersection numbers for $\mathcal{C} \setminus \mathcal{R}$ are the same as the intersection numbers of $\mathcal{D}$ with lines skew to Q. Now take a hyperplane H of $\mathrm{PG}(h+1, q)$, that contains R. Such a hyperplane intersects the plane α in a line (through Q). Suppose that this line intersects $\mathcal{D} \setminus Q$ in s points, then H intersects $\mathcal{C} \setminus R$ in sq^{h-1}. Hence, choosing $\mathcal{D}$ to be a hyperoval or a $(q+t, t)$-arc of $\mathrm{PG}(2, q)$, one may prove easily that the construction above gives $(q^h + t', t')$-arcs of type $(0, 2, t')$ in $\mathrm{PG}(2, q^h)$. More precisely:

Construction 3.4 *Let $q = 2^r$ and let the point set $\mathcal{D}$ in Construction 3.3 be a hyperoval of the plane α or a $(q+t, t)$-arc of type $(0, 2, t)$. Now use Construction 3.3 to obtain the point set $\mathcal{D}'$ of the plane $\pi \cong \mathrm{PG}(2, q^h)$.*

(1) When $\mathcal{D}$ is a hyperoval and Q (in Construction 3.3) is a point of the hyperoval, then the point set $\mathcal{D}'$ is a $(q^h + q^{h-1}, q^{h-1})$-arc of type $(0, 2, q^{h-1})$.

(2) When $\mathcal{D}$ is a hyperoval and Q is a point of $\alpha \setminus \mathcal{D}$, then the point set $\mathcal{D}'$ is a $(q^h + 2q^{h-1}, 2q^{h-1})$-arc of type $(0, 2, 2q^{h-1})$.

(3) When $\mathcal{D}$ is a $(q+t, t)$-arc of type $(0, 2, t)$ and Q is the t-nucleus of $\mathcal{D}$, then the point set $\mathcal{D}'$ is a $(q^h + tq^{h-1}, tq^{h-1})$-arc of type $(0, 2, tq^{h-1})$.

□

3.2 Algebraic approach

In this subsection our aim is to give an algebraic way of constructing the arcs of Construction 3.4. First we give the coordinates of the points of the arcs constructed above. By the next remark it is enough to determine the affine part of an arc.

Remark 3.5 *Assume that $\mathcal{K}$ is a $(q + t, t)$-arc of type $(0, 2, t)$ in $\mathrm{PG}(2, q)$. Delete the points of $\mathcal{K}$ on a line ℓ. First of all note that the maximum number of points of $\mathcal{K} \setminus \ell$ on a line is t. Remark also, that there is a unique way to extend $\mathcal{K} \setminus \ell$ to a $(q + t, t)$-arc of type $(0, 2, t)$.*

Assume that $\mathcal{K}$ is a $(q+t, t)$-arc of type $(0, 2, t)$ in $\mathrm{PG}(2, q^h)$ obtained by Construction 3.4 from the point set $\mathcal{D}$.

Without loss of generality we may assume that $\alpha \subset \pi$. We use the usual homogeneous coordinate representation of $\mathrm{PG}(2, q^h)$. With a suitable linear transformation we can achieve the following:
$M = \{(Z_0, \ldots, Z_{h+1}) : Z_i \in \mathrm{GF}(q)\}$;
$\pi = \{(X_0, X_1, X_2, 0, \ldots, 0) : X_i \in \mathrm{GF}(q^h)\}$;
$\alpha = \pi \cap M = \{(Z_0, Z_1, Z_2, 0, \ldots, 0) : Z_i \in \mathrm{GF}(q)\}$;
$V = \{(0, 0, 0, Z_3, \ldots, Z_{h+1}) : Z_i \in \mathrm{GF}(q)\}$;
$Q = (0, 1, 0, 0, \ldots, 0)$.

$X_2 = 0$ will be the hyperplane at infinity. Note, that since the affine part of an arc always determines the arc and since the hyperplane $X_2 = 0$ is mapped to the ideal line of π (that is $\pi \cap \{X_2 = 0\}$), we are allowed to consider only the affine part of $\mathcal{D}$.

Finally write $\{(x_k, y_k, 1, 0, \ldots, 0) : k\}$ for the affine part of $\mathcal{D}$ and let $\bar{\mathcal{C}}$ denote the affine part of the cone $\mathcal{C}$.

These conditions imply the following:
$\bar{\mathcal{C}} = \{(x_k, y_k, 1, z_1, \ldots, z_{h-1}) : (x_k, y_k, 1, 0, \ldots, 0) \in \mathcal{D}, z_i \in \mathrm{GF}(q)\}$.
$R = \{(0, Z_1, 0, Z_3, \ldots, Z_{h+1}) : Z_i \in \mathrm{GF}(q)\}$;
$R^* = \{(0, X_1, 0, X_3, \ldots, X_{h+1}) : X_i \in \mathrm{GF}(q^h)\}$.

One can choose a base for P of the following form:
$\{(0, b_1, 0, 1, 0, \ldots, 0), (0, b_2, 0, 0, 1, 0, \ldots, 0), \ldots, (0, b_{h-1}, 0, 0, \ldots, 0, 1)\}$. To see this, take an arbitrary generating point set of P that lies in $R^* \setminus V^*$, where V^* is the unique $(h-2)$-dimensional subspace of R^* that contains V. Any linear combination of the generating points is still in the subspace P, hence using Gauss elimination one gets the required form. Note, that $P \cap M = \emptyset$ implies $b_i \neq 0$.

An easy calculation shows that projecting $\bar{\mathcal{C}}$ from P onto π, we get

$\{(x_k, y_k+\sum_{i=1}^{h-1} \lambda_i b_i, 1, 0, \ldots, 0) : (x_k, y_k, 1, 0, \ldots, 0) \in \mathcal{D}, \lambda_i \in \mathrm{GF}(q)\}$. Let $I = \{\sum_{i=1}^{h-1} \lambda_i b_i : \lambda_i \in \mathrm{GF}(q)\}$. Hence the affine part of $\mathcal{K}$ is :

$$\{(x_k, y_k + i, 1, 0, \ldots, 0) : (x_k, y_k, 1, 0, \ldots, 0) \in \mathcal{D}, i \in I\}.$$

We show that I is a direct complement of $\mathrm{GF}(q)$ in the additive group of $\mathrm{GF}(q^h)$. One sees immediately, that I is a $\mathrm{GF}(q)$-linear additive subgroup in $\mathrm{GF}(q^h)$. To prove $|I| = q^{h-1}$ and $I \cap \mathrm{GF}(q) = 0$, suppose $\sum z_i b_i \in I \cap \mathrm{GF}(q)$. This means that the point $(0, \sum z_i b_i, 0, z_1, z_2, \ldots, z_{h-1})$ is in $P \cap M$, implying $z_1 = ... = z_{h-1} = 0$.

The next construction shows that I can be an arbitrary direct complement of $\mathrm{GF}(q)$ in the additive group of $\mathrm{GF}(q^h)$.

Construction 3.6 *Let I be a direct complement of $\mathrm{GF}(q)$ in the additive group of $\mathrm{GF}(q^h)$, $h > 1$. Let $\mathcal{H} = \{(x_k, y_k, 1) : x_k, y_k \in \mathrm{GF}(q)\} \subseteq \mathrm{PG}(2, q)$ be the affine part of a hyperoval or of a $(q + t, t)$-arc of type $(0, 2, t)$. Construct the following point set of $\mathrm{AG}(2, q^h)$:*

$$\mathcal{J} := \{(x_k, y_k + i, 1) : (x_k, y_k, 1) \in \mathcal{H}, i \in I\}.$$

(A) When $\mathcal{H}$ is a hyperoval and $(0, 1, 0) \in \mathcal{H}$, then $\mathcal{J}$ can be uniquely extended to a $(q^h + q^{h-1}, q^{h-1})$-arc of type $(0, 2, q^{h-1})$ in $\mathrm{PG}(2, q^h)$.

(B) When $\mathcal{H}$ is a hyperoval and $(0, 1, 0) \notin \mathcal{H}$, then $\mathcal{J}$ can be uniquely extended to a $(q^h + 2q^{h-1}, 2q^{h-1})$-arc of type $(0, 2, 2q^{h-1})$ in $\mathrm{PG}(2, q^h)$.

(C) When $\mathcal{H}$ is a $(q + t, t)$-arc of type $(0, 2, t)$ and $(0, 1, 0)$ is the t-nucleus of $\mathcal{H}$, then $\mathcal{J}$ can be uniquely extended to a $(q^h + tq^{h-1}, tq^{h-1})$-arc of type $(0, 2, tq^{h-1})$ in $\mathrm{PG}(2, q^h)$.

Proof: (Sketch) We show that $\mathcal{J}$ can be obtained from the point set $\mathcal{H}$ by using Construction 3.4 and deleting the points of a line, hence Remark 3.5 yields the result.

It is easy to show that I must be $\mathrm{GF}(q)$-linear, hence there are elements $b_1, \ldots, b_{h-1} \in \mathrm{GF}(q^h)$ such that every element of I can be written as $\sum_{i=1}^{h-1} z_i b_i$, where $z_i \in \mathrm{GF}(q)$. Now we coordinatize $\mathrm{PG}(h+1, q^h)$ as we did after Remark 3.5, we build the 'same' cone $\mathcal{C}$ on $\mathcal{H}$ in order to get back the same setting as we had there. Choosing P to be the subspace generated by the points $(0, b_1, 0, 1, 0, \ldots, 0), (0, b_2, 0, 0, 1, 0, \ldots, 0), \ldots, (0, b_{h-1}, 0, 0, \ldots, 0, 1)$ we are done. □

The proof above and the note after Remark 3.5 yields the following corollary.

Corollary 3.7 *The classes of arcs obtained by Construction 3.4 (1), (2) and (3) are exactly the classes of arcs of Construction 3.6 (1), (2) and (3), respectively.* □

This algebraic description shows that Construction 3.4 is the generalization of the Korchmáros-Mazzocca arcs: among new examples, *(1)* contains the arcs in question, while the arcs coming from *(2)* are all new examples. (3) only gives new examples if we start with an arc not arising from our construction, see the first remark of the next section.

4 Remarks

Remark 1. Construction 3.4 *(3)* enables us to 'iterate' our construction method. From the previous section it follows that if we start from an arc obtained by Construction 3.4 *(1)* then the resulting arc is again of that type, similarly starting from Construction 3.4 *(2)* we obtain an arc of type *(2)*.

Remark 2. Using the cone $\mathcal{C}$ we construct $(q+t,t)$-arcs of type $(0,2,t)$ in translation planes (in fact this construction works for Desarguesian planes, as well). As before, let us construct the cone $\mathcal{C}$ in $\mathrm{PG}(h+1,q)$. Embed $\mathrm{PG}(h+1,q)$ into $\mathrm{PG}(2h,q)$ as a subspace. Let H be the hyperplane at infinity in $\mathrm{PG}(2h,q)$. Choose an $(h-1)$-spread $\mathcal{S}$ of H. By the Andrè/Bruck-Bose representation we obtain the translation plane $\pi^{\mathcal{S}}$ corresponding to the spread $\mathcal{S}$ (for more details see [1]). Let Q be a point in $\mathrm{PG}(h+1,q)\setminus V$ and assume that we chose the hyperplane H and the spread $\mathcal{S}$ so that $\langle Q,V\rangle$ is an element of the spread $\mathcal{S}$. The h-dimensional subspaces intersecting the hyperplane H in an element of the $(h-1)$-spread correspond to lines on $\pi^{\mathcal{S}}$. An h-dimensional subspace that intersects H in $\langle Q,V\rangle$ intersects $\mathcal{C}\setminus\langle Q,V\rangle$ in 0 or in q^{h-1} points when $Q\in\mathcal{C}$, and in 0 or in $2q^{h-1}$ points when $Q\notin\mathcal{C}$. An h-dimensional subspace intersecting H in an element of $\mathcal{S}$ different from $\langle Q,V\rangle$ intersects $\mathrm{PG}(h+1,q)$ in a line skew to $\langle Q,V\rangle$, so it intersects $\mathcal{C}\setminus\langle Q,V\rangle$ in 0 or in 2 points (see the remark after Construction 3.3).

Hence when Q was in $\mathcal{C}$ then the point set $\mathcal{C}^{\mathcal{S}}\subset\pi^{\mathcal{S}}$, correspondig to $\mathcal{C}\setminus\langle Q,V\rangle$, is a (q^h+q^{h-1},q^{h-1})-arc of type $(0,2,q^{h-1})$; when $Q\notin\mathcal{C}$, then it is a $(q^h+2q^{h-1},2q^{h-1})$-arc of type $(0,2,2q^{h-1})$.

Remark 3. Now change the base of the cone $\mathcal{C}$ to a $(q+t,t)$-arc $\mathcal{B}$ of type $(0,2,t)$. Choose the nucleus of $\mathcal{B}$ for the point Q. Similarly as before, the construction above gives a (q^h+tq^{h-1},tq^{h-1})-arc of type $(0,2,tq^{h-1})$ on the translation plane $\pi^{\mathcal{S}}$.

Remark 4. Let $\mathcal{H}$ be a maximal arc in $\mathrm{PG}(2,q)$ of size (2^sq+2^s-q). Similarly to Construction 3.4 we obtain

(1) $((2^sq+2^s-q-1)q^{h-1},(2^s-1)q^{h-1}))$-arcs of type $(0,2^s,(2^s-1)q^{h-1})$;

(2) $((2^sq+2^s-q)q^{h-1},(2^s)q^{h-1})$-arcs of type $(0,2^s,(2^s)q^{h-1})$.

References

[1] R. H. Bruck and R. C. Bose, The construction of translation planes from projective spaces, *J. Algebra* **1** (1964), 85–102.

[2] J. W. P. Hirschfeld, Projective geometries over finite fields, *Clarendon Press, Oxford*, 1979, 2nd edition, 1998.

[3] G. Korchmáros and F. Mazzocca, On $(q+t)$-arcs of type $(0,2,t)$ in a desarguesian plane of order q. *Math. Proc. Camb. Phil. Soc.* **108** (1990), 445-459.

[4] O. Polverino, T. Szőnyi and Zs. Weiner, Blocking sets in Galois planes of square order, *Acta Sci. Math. (Szeged)* **65** (1999), 773-784.

[5] P. Sziklai, T. Szőnyi, Blocking sets and algebraic curves, *Rend. Circ. Mat. Palermo* **51** (1998), 71–86.