Notes on semiarcs

Gy. Kiss

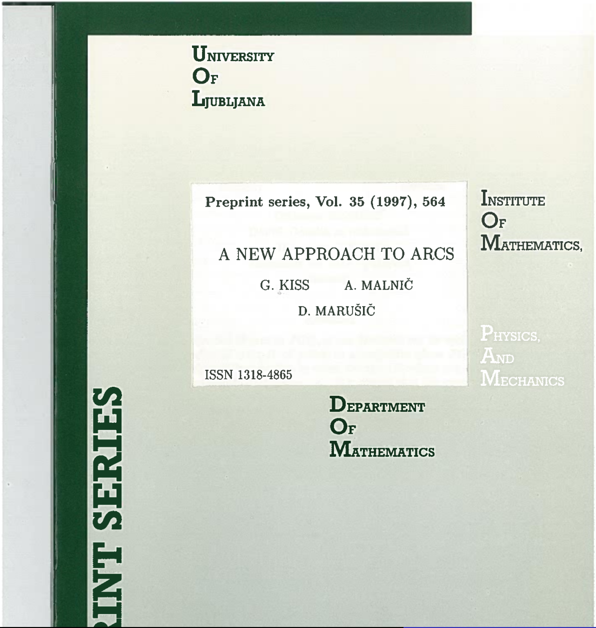
$$|\mathcal{DM}| = 60$$

May 3rd, 2013, Koper

1994

1995

Arcs from 1997



UNIVERSITY
OF
LJUBLJANA

INSTITUTE
OF
MATHEMATICS,
PHYSICS,
AND
MECHANICS

Preprint series, Vol. 35 (1997), 564

A NEW APPROACH TO ARCS

G. KISS A. MALNIČ
D. MARUŠIČ

ISSN 1318-4865

DEPARTMENT
OF
MATHEMATICS

RINT SERIES

Arcs in Projective Planes over Finite Fields

G. Kiss, A. Malnič, D. Marušič

In the past forty years there has been quite a lot of research regarding the existence and characterization of certain type of arcs in projective planes over finite fields. Here, an *arc* means a subset of points no three of which are colinear. Apart from being an interesting and difficult mathematical problem in its own due, some of the results are of particular importance to other fields and in particular to Coding theory.

Abstract

Some properties of arcs in $PG(2, q)$ are discussed via its cyclic model. An algorithm for checking whether a given set of points is an arc is given, and certain constructions of special type of arcs are presented

Nice arcs

It is of interest to consider certain special types of arcs. For example, a now classical result of Segre states that all $(q+1)$-arcs are conics if q is odd; however, no characterization of $(q+1)$-arcs in the even case is known. There are of course other ways to declare arcs as nice. We shall consider the case when arcs have certain nice properties with respect to the *inversion* (multiplication by -1 in $\mathbb{Z}_{q^2+q+1}$).

Proposition

If K is a k-segment then $-K$ is a k-arc. In particular, if L is a line then $-L$ is a $(q+1)$-arc.

Arcs from 1997

Proposition

Let a,b and c be arbitrary points where $a \neq b$. Then $-a, -b, -c$ are colinear if and only if $a + b - c \in L_{a,b}$. Consequently, $L_{-a,-b} = L_{a,b} - a - b$.

Let $L_{a,b} = S + i$. Then $a = s_a + i$ and $b = s_b + i$. We know that $-a, -b, -c$ are colinear if and only if $-b + a$ and $-c + a$ are in the same column of D_S. Since $-b + a = -s_b - i + s_a + i = s_a - s_b$ is in s_b-th column, we must have $-c + a = s - s_b$ for some $s \in S$. This can be rewritten as $a + b - c = s + i \in L_{a,b}$. Rewriting again we have $-c \in L_{a,b} - a - b$, that is, $L_{-a,-b} = L_{a,b} - a - b$.

SEMIOVALS CONTAINED IN THE UNION OF THREE CONCURRENT LINES

Aart Blokhuis,
György Kiss,
István Kovács
Aleksander Malnič,
Dragan Marušič
and János Ruff

Abstract

Semiovals which are contained in the union of three concurrent lines are studied. The notion of a *strong semioval* is introduced, and a complete classification of these objects in $\mathrm{PG}(2, p)$ and $\mathrm{PG}(2, p^2)$, p an odd prime, is given.

Strong semiovals

Theorem

If a semioval $\mathcal{S}$ in Π_q, $q > 3$, is contained in the union of three concurrent lines, then $|\mathcal{S}| \leq 3\lceil q - \sqrt{q}\rceil$.

Example

Let $q = s^2$ and let ℓ_1, ℓ_2, ℓ_3 be three concurrent lines in $\mathrm{PG}(2, q)$. Choose Baer sublines $\overline{\ell}_1 \subset \ell_1$, $\overline{\ell}_2 \subset \ell_2$, and $\overline{\ell}_3 \subset \ell_3$ in such a way that, for any triple of distinct $i, j, k \in \{1, 2, 3\}$, the Baer subplane $\mathcal{B}_{j,k} = \langle \overline{\ell_j}, \overline{\ell_k} \rangle$ meets the line ℓ_i only in the common point C. Then $\mathcal{S} = (\ell_1 \setminus \overline{\ell}_1) \cup (\ell_2 \setminus \overline{\ell}_2) \cup (\ell_3 \setminus \overline{\ell}_3)$ is a semioval which has $3(q - \sqrt{q})$ points.

Strong semiovals

A semioval $\mathcal{S}$ allows an algebraic description in terms of an ordered triple (R, S, T), where R, S, and T are certain subsets of $\mathrm{GF}(q)$. Namely, let us choose a system of reference for $\mathrm{PG}(2, q)$ in such a way that the lines ℓ_1, ℓ_2, and ℓ_3 have equations $X_1 = -X_3$, $X_1 = 0$, and $X_1 = X_3$, respectively. Then $C = (0, 1, 0) \notin \mathcal{S}$ because $q > 3$. Let

$$R = \{r \in GF(q) : (-1, r, 1) \in \mathcal{L}_1\},$$

$$S = \{s \in GF(q) : (0, s, -2) \in \mathcal{L}_2\},$$

$$T = \{t \in GF(q) : (1, t, 1) \in \mathcal{L}_3\}.$$

If we denote the size of $\mathcal{L}_i$ by a, then $|R| = |S| = |T| = a$. Consider the sets R, S and T as subsets of the additive group of $GF(q)$.

Now $r+s+t=0$ if and only if the points $(-1,r,1),(0,s,-2)$ and $(1,t,1)$ are collinear. Thus, $\mathcal{S}$ is a semioval if and only if

$$\begin{aligned} |S^c+u\cap -T^c| &= 1, \quad \text{if } u\in R,\\ |T^c+u\cap -R^c| &= 1, \quad \text{if } u\in S,\\ |R^c+u\cap -S^c| &= 1, \quad \text{if } u\in T. \end{aligned}$$

But for every $u\in E$,

$$|S+u\cap -T|+|S+u\cap(-T)^c|=|S+u|=a,$$

$$|S+u\cap -T^c|+|S^c+u\cap -T^c|=|-T^c|=q-a.$$

Further, if $u\in R$ then $|S+u\cap(-T)^c|=|S+u\cap -T^c|$, and so $|S^c+u\cap -T^c|=1$ amounts to $|S+u\cap -T|=2a-q+1$. Similarly, if $u\in S$ then $|T^c+u\cap -R^c|=1$ amounts to $|T+u\cap -R|=2a-q+1$ and if $u\in T$ then $|R^c+u\cap -S^c|=1$ amounts to $|R+u\cap -S|=2a-q+1$.

Therefore the above system of equations is equivalent to the following one:

$$\begin{aligned} |S+u\cap -T| &= 2a-q+1, \quad \text{if } u\in R,\\ |T+u\cap -R| &= 2a-q+1, \quad \text{if } u\in S,\\ |R+u\cap -S| &= 2a-q+1, \quad \text{if } u\in T. \end{aligned} \tag{1}$$

Let $\mathcal{S}$ be a strong semioval in $PG(2,q)$ and let S, R, T be subsets of E which are induced by $\mathcal{S}$ in the way described in the previous section. Let $a = |R| = |S| = |T|$. Since $\mathcal{S}$ is a strong semioval, there exists a natural number k such that the number of two-secants of $\mathcal{S}$ passing through each point in $\ell_i \setminus (\mathcal{L}_i \cup \{C\})$ is equal to k. (Example 4 gives a strong semioval with $k = (\sqrt{q}-1)^2$.) So instead of (1) we have the following refined system of equations

$$\begin{array}{rcl} |S+u\cap -T| & = & \begin{cases} 2a-q+1, & \text{if } u\in R,\\ k, & \text{if } u\notin R,\end{cases} \\ |T+u\cap -R| & = & \begin{cases} 2a-q+1, & \text{if } u\in S,\\ k, & \text{if } u\notin S,\end{cases} \\ |R+u\cap -S| & = & \begin{cases} 2a-q+1, & \text{if } u\in T,\\ k, & \text{if } u\notin T\end{cases} \end{array} \tag{2}$$

We call k the *parameter* of $\mathcal{S}$.

Strong semiovals

Proposition

Let $\mathcal{S}$ be a strong semioval in $PG(2,q)$ with parameter k. If $\mathcal{S}$ consists of $3a$ points, then

$$k = a - \frac{a}{q-a}.$$

Theorem

If $\mathcal{S}$ is a strong semioval of cardinality $|\mathcal{S}| = 3(p^m - p^l)$, $m/2 < l < m$, in $PG(2,q)$, $q = p^m$ odd, then

$$(p-1)(p^{2l-m}-1)^2 \mid (p^{m-l}-1). \tag{3}$$

Corollary

There is no strong semioval in $PG(2,p)$ if p is an odd prime.

Corollary

If $\mathcal{S}$ is a strong semioval in $PG(2,p^m)$, where p is an odd prime, and

$$m \leq \begin{cases} (p-1)^2 & p \equiv -1 \pmod 4 \\ 2(p-1)^2 & p \equiv 1 \pmod 4, \end{cases}$$

then $|\mathcal{S}| = 3(q-\sqrt{q})$.

Definition

Let Π_q be a projective plane of order q. A non-empty pointset $\mathcal{S}_t \subset \Pi_q$ is called a t-semiarc if for every point $P \in \mathcal{S}_t$ there exist exatly t lines $\ell_1, \ell_2, \dots \ell_t$ such that $\mathcal{S}_t \cap \ell_i = \{P\}$ for $i = 1, 2, \dots, t$. These lines are called the tangents to $\mathcal{S}_t$ at P.

Definition

Let Π_q be a projective plane of order q. A non-empty pointset $\mathcal{S}_t \subset \Pi_q$ is called a t-semiarc if for every point $P \in \mathcal{S}_t$ there exist exatly t lines $\ell_1, \ell_2, \dots \ell_t$ such that $\mathcal{S}_t \cap \ell_i = \{P\}$ for $i = 1, 2, \dots, t$. These lines are called the tangents to $\mathcal{S}_t$ at P.

Some examples:

- Semiovals, $t = 1$.
- Subplanes, $t = q - m$, where m is the order of the subplane.

More examples

Proposition

Let $\mathcal{S}_t$ be a t-semiarc in Π_q. The followings hold:

- *if $t = q + 1$, then $\mathcal{S}_t$ is a single point,*
- *if $t = q$, then $\mathcal{S}_t$ is a subset of a line, and vice versa any subset of a line containing at least two points is a q-semiarc,*
- *if $t = q - 1$, then $\mathcal{S}_t$ is a set of three non-collinear points.*

More examples

Proposition

Let $\mathcal{S}_t$ be a t-semiarc in Π_q. The followings hold:

- *if $t = q + 1$, then $\mathcal{S}_t$ is a single point,*
- *if $t = q$, then $\mathcal{S}_t$ is a subset of a line, and vice versa any subset of a line containing at least two points is a q-semiarc,*
- *if $t = q - 1$, then $\mathcal{S}_t$ is a set of three non-collinear points.*

There exist t-semiarcs for each value of t satisfying $1 \leq t < q - 1$.

Example

Let ℓ_1 and ℓ_2 be two lines of Π_q, and let $1 \leq t < q - 1$ be an arbitrary integer. If we delete the point $\ell_1 \cap \ell_2$ and t other points from both lines, then the remaining $2(q - t)$ points obviously form a t-semiarc.

Proposition

If a t-semiarc $\mathcal{S}_t$ *is contained in the union of two lines* ℓ_1 *and* ℓ_2 *of* Π_q *and* $1 \leq t < q-1$*, then* $|\mathcal{S}_t \cap \ell_i| = q - t$ *for* $i = 1, 2$*, and* $\mathcal{S}_t$ *does not contain the point* $\ell_1 \cap \ell_2$*.*

Semiarcs contained in three lines

An algebraic description:
$\mathcal{S}_t \iff$ ordered triple (A, B, C),
where $A, B, C \subset \mathrm{GF}(q)$.
The lines ℓ_1, ℓ_2, and ℓ_3 have equations $X_1 = 0$, $X_1 = X_3$ and $X_3 = 0$, respectively. $V = (0, 1, 0)$.

$$A = \{a \in \mathrm{GF}(q) : (0, a, 1) \notin \mathcal{L}_1\},$$

$$B = \{b \in \mathrm{GF}(q) : (1, b, 1) \notin \mathcal{L}_2\},$$

$$C = \{c \in \mathrm{GF}(q) : (1, c, 0) \notin \mathcal{L}_3\}.$$

An algebraic description:
$\mathcal{S}_t \iff$ ordered triple (A, B, C),
where $A, B, C \subset \mathrm{GF}(q)$.
The lines ℓ_1, ℓ_2, and ℓ_3 have equations $X_1 = 0$, $X_1 = X_3$ and $X_3 = 0$, respectively. $V = (0, 1, 0)$.

$$A = \{a \in \mathrm{GF}(q) : (0, a, 1) \notin \mathcal{L}_1\},$$

$$B = \{b \in \mathrm{GF}(q) : (1, b, 1) \notin \mathcal{L}_2\},$$

$$C = \{c \in \mathrm{GF}(q) : (1, c, 0) \notin \mathcal{L}_3\}.$$

$$(0, a, 1),\ (1, b, 1),\ (1, c, 0)\ \text{collinear} \iff a + c = b.$$

Triangular case

The line ℓ_i has equation $X_i = 0$.

The line ℓ_i has equation $X_i = 0$.

$$(0, a, 1),\ (b, 0, 1),\ (1, c, 0)\,\text{collinear} \iff ac = -b.$$

Theorems from Additive Group Theory

Theorem (Exact inverse sumset theorem)

Suppose that A and B are finite nonempty subsets of the abelian group Z. Then the following are equivalent.

- $|A+B| = |A|$.
- $|A-B| = |A|$.
- *Let $G := stab(A)$. Then G is a finite subgroup of Z, B is contained in a coset of G, and A is the union of cosets of of G.*

Definition

Let A and B be finite, nonempty subsets of an abelian group $(Z, \odot)$, and let $i \geq 1$ an integer.
Let $N_i(A, B)$ all the elements c with at least i representations of the form $c = a \odot b$ with $a \in A$ and $b \in B$. Sometimes we use the shorthand notation N_i instead of $N_i(A, B)$.

Theorem (Pollard, 1974)

Let Z be an abelian group, $|Z| = p$ prime, $A, B \subseteq G$ nonempty subsets, and $1 \leq k \leq min\{|A|, |B|\}$. Then

$$|N_1| + |N_2| + \ldots + |N_k| \geq k \cdot min\{p, |A| + |B| - k\}.$$

Theorem (Grynkiewicz, 2010)

Let Z be an abelian group, $A, B \subseteq Z$ finite and nonempty subsets, and $k \geq 1$. If $|A|, |B| \geq k$, then either

$$\sum_{i=1}^{k} |N_i| \geq k(|A| + |B|) - 2k^2 + 1,$$

Theorem

or else there exist $A' \subseteq A$ and $B' \subseteq B$ with

$$l := \left|A \setminus A'\right| + \left|B \setminus B'\right| \leq k-1,$$

$$N_k(A', B') = N_1(A', B') = N_k(A, B),$$

$$\sum_{i=1}^{k} |N_k| \geq k(|A|+|B|) - (k-l)(|H|-\rho) - kl \geq k(|A|+|B|-|H|),$$

where H is the nontrivial stabilizer of $N_k(A, B)$ and $\rho = |A' \odot H| - |A'| + |B' \odot H| - |B'|$. In the case $k = 2$ instead of the first inequality $|N_1| + |N_2| \geq 2(|A|+|B|) - 4$ also holds.

Theorem ($V \notin \mathcal{S}_t$)

Let $\mathcal{S}_t$ be a t-semiarc in Π_q, suppose that $\mathcal{S}_t$ is contained in the union of three lines of $\mathcal{P}_V$, but does not contained in the union of any two lines of $\mathcal{P}_V$. If $V \notin \mathcal{S}_t$, then there are three possibilities.

1. $u_1 = u_2 = u_3 = u$, *and*
$$3 \cdot \frac{q-t}{2} \leq |\mathcal{S}_t| \leq 3 \cdot \left(q + \frac{t}{2} - \sqrt{qt + \frac{t^2}{4}} \right).$$
2. $u_i = u_j = q - t$ *and* $2 \leq u_k \leq t$ *holds for* $\{i, j, k\} = \{1, 2, 3\}$. *The inequalities*
$$2q - 2t + 2 \leq |\mathcal{S}_t| \leq 2q - t \tag{4}$$
also hold in this case.
3. $\mathcal{S}_t$ *is a 5-arc and* $t = q - 3$.

Application of thms from additive group theory

Theorem (B. Csajbók, Gy. K, 2012)

Suppose that the t-semiarc $\mathcal{S}_t$ in $PG(2,p^r)$, p odd prime, belongs to the family of Case 2 of Theorem $V \notin \mathcal{S}_t$. Then there exists a subgroup G of E such that both A and C are union of cosets of G, and $\overline{B}$ is contained in a coset of G.
If ϕ is the natural homomorphism from E to E/G, $|G| = g$ and $|\phi(C)| = h$, then $t = gh$ and $|\mathcal{S}_t| = 2p^r - 2gh + |\overline{B}|$.

Corollary (B. Csajbók, Gy. K, 2012)

Let p be an odd prime. Then the followings hold.

1. *In $PG(2,p)$ there is no semiarc belonging to the family of Case 2 of Theorem $V \notin \mathcal{S}_t$.*
2. *Let $1 \le e < r$ be integers and let $t = p^e s$, where $(p,s) = 1$ and $t < p^r$. Then $PG(2,p^r)$ contains t-semiarcs with cardinality $2p^r - 2t + k$ for all t and k satisfying the conditions $2 \le k \le p^e$.*

Theorem (B. Csajbók, Gy. K, 2012)

Let $\mathcal{S}_1$ be a semioval in the plane $PG(2, q)$, $q = p^r$, p odd prime. Suppose that $\mathcal{S}_1$ is contained in the union of three lines of $\mathcal{P}_V$, but does not contained in the union of any two lines of $\mathcal{P}_V$. Then $|\mathcal{S}_1| \geq 3q - 3f_r(q)$, where

$$f_r(q) = \begin{cases} 2\lceil\sqrt{p+1}\rceil - 2 & \text{if } r = 1, \\ 4\left\lceil\sqrt{\frac{q+1}{2}}\right\rceil - 4 & \text{if } r = 2, \\ q^{\frac{r-1}{r}} + q^{\frac{1}{r}} - 1 & \text{if } r \geq 3. \end{cases}$$

Theorem (B. Csajbók, Gy. K, 2012)

Let $\mathcal{S}_1$ be a strong semioval in $PG(2, p^r)$, p an odd prime. Then the followings hold.

1. *If $r = 2l$, then $\mathcal{S}_1$ contains $3(p^{2l} - p^l)$ points.*
2. *If $r = 2l + 1$ and $p > 7$, then there is no strong semioval in $PG(2, p^r)$.*
3. *If $r = 2l + 1$ and $p = 3, 5$ or 7, then $\mathcal{S}_1$ contains $3(p^{2l+1} - p^{l+1})$ points.*

2-semiarcs

Theorem (B. Csajbók, Gy. K, 2012)

Let $\mathcal{S}_2$ be a 2-semiarc in $PG(2, q)$, $q = p^r$, p odd prime. Suppose that $\mathcal{S}_2$ belongs to the family of Case 1 of Theorem $V \notin \mathcal{S}_t$. Then $|\mathcal{S}_2| \geq 3q - 3f_r(p)$, where

$$f_r(p) = \begin{cases} 2\lceil\sqrt{2p+4}\rceil - 4 & \textit{if } r = 1, \\ 4\left\lceil\sqrt{p^2 + \frac{7}{2}}\right\rceil - 8 & \textit{if } r = 2, \\ 14, 37, 66 & \textit{if } r = 3 \textit{ and } p = 3,\ 5,\ 7, \\ p^2 + 2p + 2 & \textit{if } r = 3 \textit{ and } p \geq 11, \\ p^{r-1} + 2p - 2 & \textit{if } r \geq 4. \end{cases}$$

THANK YOU FOR YOUR ATTENTION!