Seconda Università degli Studi di Napoli (a Caserta)
Dipartimento di Matematica e Fisica

Generalized Hyperfocused Arcs

Francesco Mazzocca
(jont work with Aart Blokhuis and Giuseppe Marino)

Finite Geometry Conference and Workshop
University of Szeged
10-14 June, 2013

Arcs and blocking sets

DEFINITION

A $k-$arc in $PG(2, q)$ is a set of k points with no 3 on a line.
A line containing 1 or 2 points of a $k-$arc is said to be a tangent or secant to the $k-$arc, respectively.

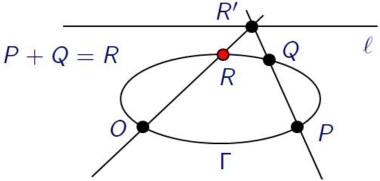
DEFINITION

A $k-$arc in $PG(2,q)$ is a set of k points with no 3 on a line.
A line containing 1 or 2 points of a $k-$arc is said to be a tangent or secant to the $k-$arc, respectively.

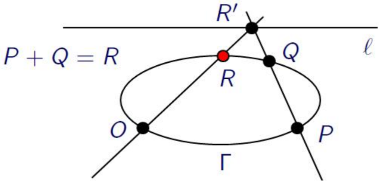
DEFINITION

Let $\mathcal{F}$ be a set of lines in $PG(2,q)$. A blocking set of $\mathcal{F}$ is a set of points $\mathcal{B} \subset PG(2,q)$ having non-empty intersection with each line in $\mathcal{F}$. If this is the case, we also say that the lines in $\mathcal{F}$ are blocked by $\mathcal{B}$.

Let ℓ and Γ be a line and a non singular conic in $PG(2, \mathbb{F})$, respectively. An abelian group G on $\Gamma \setminus \ell$ can be defined in the following way:

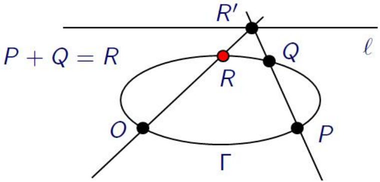


Let ℓ and Γ be a line and a non singular conic in $PG(2, \mathbb{F})$, respectively. An abelian group G on $\Gamma \setminus \ell$ can be defined in the following way:



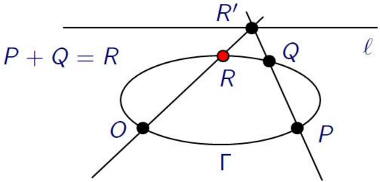
- choose a point $O \in \Gamma \setminus \ell$ as the identity of the group;

Let ℓ and Γ be a line and a non singular conic in $PG(2,\mathbb{F})$, respectively. An abelian group G on $\Gamma \setminus \ell$ can be defined in the following way:



- choose a point $O \in \Gamma \setminus \ell$ as the identity of the group;
- for any two points $P, Q \in \Gamma \setminus \ell$, let R' be the point that the line through P, Q has in common with ℓ;

Let ℓ and Γ be a line and a non singular conic in $PG(2, \mathbb{F})$, respectively. An abelian group G on $\Gamma \setminus \ell$ can be defined in the following way:



- choose a point $O \in \Gamma \setminus \ell$ as the identity of the group;
- for any two points $P, Q \in \Gamma \setminus \ell$, let R' be the point that the line through P, Q has in common with ℓ;
- the sum of P and Q is defined by $P + Q = R$, where R is the second of the two points (counted with multiplicity) common to the line OR' and $\Gamma \setminus \ell$.

DEFINITION

A dual 3-net embedded in $PG(2, \mathbb{F})$*, is a triple* $\{A, B, C\}$ *with* A, B, C *pairwise disjoint point-sets of size n, called* components, *such that every line meeting two distinct components meets each component in precisely one point.*

DEFINITION

A dual 3-net embedded in $PG(2, \mathbb{F})$, *is a triple* $\{A, B, C\}$ *with* A, B, C *pairwise disjoint point-sets of size* n, *called* components, *such that every line meeting two distinct components meets each component in precisely one point.*

EXAMPLE

Let ℓ *and* Γ *be a line and a non singular conic in* $PG(2, \mathbb{F})$, *respectively.*

DEFINITION

A dual 3-net embedded in $PG(2, \mathbb{F})$, is a triple $\{A, B, C\}$ with A, B, C pairwise disjoint point-sets of size n, called components*, such that every line meeting two distinct components meets each component in precisely one point.*

EXAMPLE

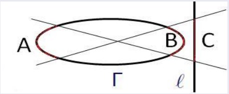
Let ℓ and Γ be a line and a non singular conic in $PG(2, \mathbb{F})$, respectively. Let G be the abelian group associated to Γ and ℓ.

DEFINITION

A dual 3-net embedded in $PG(2, \mathbb{F})$, *is a triple* $\{A, B, C\}$ *with* A, B, C *pairwise disjoint point-sets of size* n, *called* components, *such that every line meeting two distinct components meets each component in precisely one point.*

EXAMPLE

Let ℓ *and* Γ *be a line and a non singular conic in* $PG(2, \mathbb{F})$, *respectively. Let* G *be the abelian group associated to* Γ *and* ℓ.



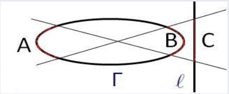
Now, given a proper subgroup A *of* G *of finite order* n *and one of its cosets* B $(\neq A)$, *the set* C *of the points of* ℓ *on some line intersecting both* A *and* B *has exactly* n *points.*

DEFINITION

A dual 3-net embedded in $PG(2,\mathbb{F})$, *is a triple* $\{A,B,C\}$ *with* A,B,C *pairwise disjoint point-sets of size* n, *called* components, *such that every line meeting two distinct components meets each component in precisely one point.*

EXAMPLE

Let ℓ *and* Γ *be a line and a non singular conic in* $PG(2,\mathbb{F})$, *respectively. Let* G *be the abelian group associated to* Γ *and* ℓ.



Now, given a proper subgroup A *of* G *of finite order* n *and one of its cosets* B $(\neq A)$, *the set* C *of the points of* ℓ *on some line intersecting both* A *and* B *has exactly* n *points. Then the triple* $\{A,B,C\}$ *is a dual* $3-$*net of order* n *embedded in* $PG(2,\mathbb{F})$.

The following theorem follows from the main result in the paper

Blokhuis A., Korchmáros G. & M.F. - 2011

On the structure of 3-nets embedded in a projective plane, Journal of Combinatorial Theory, Series A; 0097-3165; ; Vol.118 (2011); pp. 1228-1238.

The following theorem follows from the main result in the paper

Blokhuis A., Korchmáros G. & M.F. - 2011

On the structure of 3-nets embedded in a projective plane, Journal of Combinatorial Theory, Series A; 0097-3165; ; Vol.118 (2011); pp. 1228-1238.

Theorem

Let $\{A, B, C\}$ be a dual 3-net of order n in $PG(2,\mathbb{F})$. Then, if C is contained in a line and $\mathbb{F}$ has positive characteristic $p \geq n$, $A \cup B$ is contained in a conic. If this conic is irreducible then it is of type described in the previous example.

DEFINITION

A *generalized hyperfocused arc* $\mathcal{H}$ in $PG(2,q)$ (M.Giulietti - E.Montanucci, 2006) is a k-arc with the property that the $k(k-1)/2$ secants can be blocked by a set $\mathcal{B}$ of $k-1$ points not belonging to the arc.

DEFINITION

A *generalized hyperfocused arc* $\mathcal{H}$ in $PG(2, q)$ (M.Giulietti - E.Montanucci, 2006) is a k-arc with the property that the $k(k-1)/2$ secants can be blocked by a set $\mathcal{B}$ of $k-1$ points not belonging to the arc. When $\mathcal{B}$ is contained in a line, $\mathcal{H}$ is simply called a *hyperfoused arc* (W.Cherowitzo - L.Holder, 2005).

DEFINITION

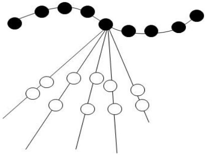
A *generalized hyperfocused arc* $\mathcal{H}$ in $PG(2,q)$ (M.Giulietti - E.Montanucci, 2006) is a k-arc with the property that the $k(k-1)/2$ secants can be blocked by a set $\mathcal{B}$ of $k-1$ points not belonging to the arc. When $\mathcal{B}$ is contained in a line, $\mathcal{H}$ is simply called a *hyperfoused arc* (W.Cherowitzo - L.Holder, 2005).

- Points of the arc $\mathcal{H}$ will be called *white points* and points of the blocking set $\mathcal{B}$ *black points*.

DEFINITION

A *generalized hyperfocused arc* $\mathcal{H}$ in $PG(2,q)$ (M.Giulietti - E.Montanucci, 2006) is a k-arc with the property that the $k(k-1)/2$ secants can be blocked by a set $\mathcal{B}$ of $k-1$ points not belonging to the arc. When $\mathcal{B}$ is contained in a line, $\mathcal{H}$ is simply called a *hyperfoused arc* (W.Cherowitzo - L.Holder, 2005).

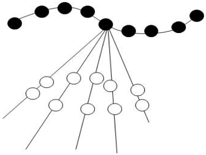
- Points of the arc $\mathcal{H}$ will be called *white points* and points of the blocking set $\mathcal{B}$ *black points*.
- In case $k > 1$, the secant lines to $\mathcal{H}$ trough a fixed black point induce a partition into 2-sets of $\mathcal{H}$; so k **must be even**.



DEFINITION

A *generalized hyperfocused arc* $\mathcal{H}$ in $PG(2,q)$ (M.Giulietti - E.Montanucci, 2006) is a k-arc with the property that the $k(k-1)/2$ secants can be blocked by a set $\mathcal{B}$ of $k-1$ points not belonging to the arc. When $\mathcal{B}$ is contained in a line, $\mathcal{H}$ is simply called a *hyperfoused arc* (W.Cherowitzo - L.Holder, 2005).

- Points of the arc $\mathcal{H}$ will be called *white points* and points of the blocking set $\mathcal{B}$ *black points*.
- In case $k>1$, the secant lines to $\mathcal{H}$ trough a fixed black point induce a partition into 2-sets of $\mathcal{H}$; so k **must be even**.



Moreover, the $k-1$ black points induce a factorization (i.e. a partition into matchings) of the white k-arc.

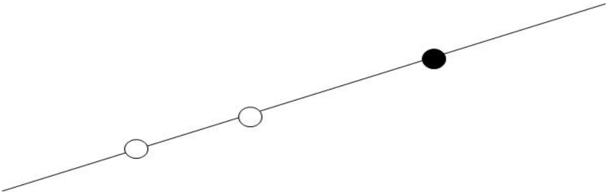
A trivial example of generalized hyperfocused arc

For $k = 2$, there is only a trivial example of generalized hyperfocused arc $\mathcal{H}$ (in fact it is a hyperfocused arc):

A trivial example of generalized hyperfocused arc

For $k = 2$, there is only a trivial example of generalized hyperfocused arc $\mathcal{H}$ (in fact it is a hyperfocused arc):

$\mathcal{B}$ consists of a unique black point out of $\mathcal{H}$ on the line through the two white points of $\mathcal{H}$.



- Hyperfocused arcs only exist if q is even (Bichara - Korchmáros, 1980).

- Hyperfocused arcs only exist if q is even (Bichara - Korchmáros, 1980).
- Although many results are known about hyperfocused arcs and their generalizations (Cherowitzo, Holder, Giulietti, Korchmáros, Lanzone, Montanucci, Parrettini, Pasticci, Siciliano, Sonnino,...), there are still many open problems concerning them.

- Hyperfocused arcs only exist if q is even (Bichara - Korchmáros, 1980).
- Although many results are known about hyperfocused arcs and their generalizations (Cherowitzo, Holder, Giulietti, Korchmáros, Lanzone, Montanucci, Parrettini, Pasticci, Siciliano, Sonnino,...), there are still many open problems concerning them.
- It is known that there exist examples of generalized hyperfocused arcs which are not hyperfocused, provided q is even (M.Giulietti - E.Montanucci, 2006).

- Hyperfocused arcs only exist if q is even (Bichara - Korchmáros, 1980).
- Although many results are known about hyperfocused arcs and their generalizations (Cherowitzo, Holder, Giulietti, Korchmáros, Lanzone, Montanucci, Parrettini, Pasticci, Siciliano, Sonnino,...), there are still many open problems concerning them.
- It is known that there exist examples of generalized hyperfocused arcs which are not hyperfocused, provided q is even (M.Giulietti - E.Montanucci, 2006).
- The study of hyperfocused arcs is motivated by a relevant application to cryptography in connection with constructions of efficient secret sharing schemes (G.Simmons, 1990; L.Holder, 1997).

A bank president problem

In a bank there are a president, n first level and m second level employees. The president knows the combination to the vault and does not want to share this combination with any individual other than himself.

A bank president problem

In a bank there are a president, n first level and m second level employees. The president knows the combination to the vault and does not want to share this combination with any individual other than himself.

The problem is to find a way to give out parts (shares) of the combination (the secret) to any employees so that, combining their information, the vault can be open by

A bank president problem

In a bank there are a president, n first level and m second level employees. The president knows the combination to the vault and does not want to share this combination with any individual other than himself.

The problem is to find a way to give out parts (shares) of the combination (the secret) to any employees so that, combining their information, the vault can be open by

- any two of the first level employees, or

A bank president problem

In a bank there are a president, n first level and m second level employees. The president knows the combination to the vault and does not want to share this combination with any individual other than himself.

The problem is to find a way to give out parts (shares) of the combination (the secret) to any employees so that, combining their information, the vault can be open by

- any two of the first level employees, or
- any one of the first level together with any two of the second level employees, or

A bank president problem

In a bank there are a president, n first level and m second level employees. The president knows the combination to the vault and does not want to share this combination with any individual other than himself.

The problem is to find a way to give out parts (shares) of the combination (the secret) to any employees so that, combining their information, the vault can be open by

- any two of the first level employees, or
- any one of the first level together with any two of the second level employees, or
- any three second level employees;

A bank president problem

In a bank there are a president, n first level and m second level employees. The president knows the combination to the vault and does not want to share this combination with any individual other than himself.

The problem is to find a way to give out parts (shares) of the combination (the secret) to any employees so that, combining their information, the vault can be open by

- any two of the first level employees, or
- any one of the first level together with any two of the second level employees, or
- any three second level employees;

and the previous ones are the only minimal combinations of employees able to open the vault.

A bank president problem

In a bank there are a president, n first level and m second level employees. The president knows the combination to the vault and does not want to share this combination with any individual other than himself.

The problem is to find a way to give out parts (shares) of the combination (the secret) to any employees so that, combining their information, the vault can be open by

- any two of the first level employees, or
- any one of the first level together with any two of the second level employees, or
- any three second level employees;

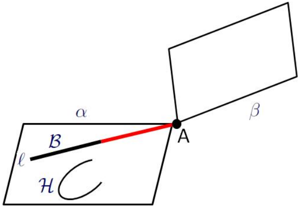
and the previous ones are the only minimal combinations of employees able to open the vault.
These set of combinations is called an access structure and a solution to the problem is an example of a secret sharing scheme.

A geometric solution
to our bank president problem

A geometric solution
to our bank president problem

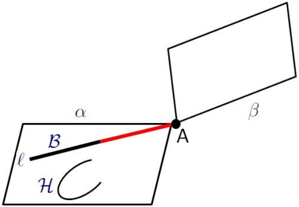
Let α, β be two planes in $PG(4, q)$ meeting in exactly one point A. Assume that α contains a hyperfocused $k-$arc $\mathcal{H}$ with a set $\mathcal{B}$ of $k-1$ black points on a line ℓ.

Let α, β be two planes in $PG(4, q)$ meeting in exactly one point A. Assume that α contains a hyperfocused k−arc $\mathcal{H}$ with a set $\mathcal{B}$ of $k - 1$ black points on a line ℓ. Set



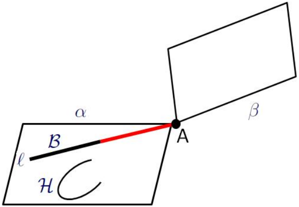
- A = the secret;

Let α, β be two planes in $PG(4, q)$ meeting in exactly one point A. Assume that α contains a hyperfocused $k-$arc $\mathcal{H}$ with a set $\mathcal{B}$ of $k-1$ black points on a line ℓ. Set



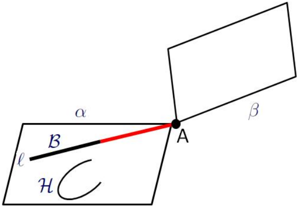
- $A =$ the secret;
- points of $\ell \setminus (\mathcal{B} \cup A) =$ $q-k+1$ first level employees;

Let α, β be two planes in $PG(4, q)$ meeting in exactly one point A. Assume that α contains a hyperfocused $k-$arc $\mathcal{H}$ with a set $\mathcal{B}$ of $k-1$ black points on a line ℓ. Set



- $A =$ the secret;
- points of $\ell \setminus (\mathcal{B} \cup A) =$ $q-k+1$ first level employees;
- $\mathcal{H} = k$ second level employees.

Let α, β be two planes in $PG(4, q)$ meeting in exactly one point A. Assume that α contains a hyperfocused $k-$arc $\mathcal{H}$ with a set $\mathcal{B}$ of $k-1$ black points on a line ℓ. Set

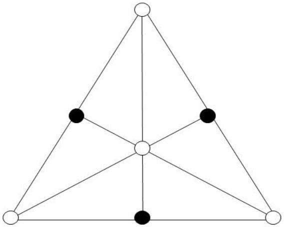


- $A =$ the secret;
- points of $\ell \setminus (\mathcal{B} \cup A) =$ $q-k+1$ first level employees;
- $\mathcal{H} = k$ second level employees.

Then any team in the access structure can get the secret.

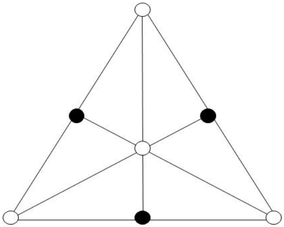
EXAMPLE

Any 4-arc $\mathcal{Q}$ of white points, with its three black diagonal points, is a non trivial example of generalized hyperfocused arc.



EXAMPLE

Any 4-arc $\mathcal{Q}$ of white points, with its three black diagonal points, is a non trivial example of generalized hyperfocused arc.



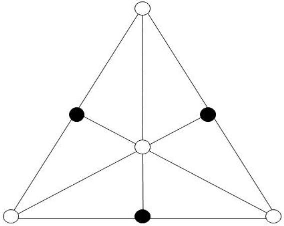
Note that:

- when q is even, the three black diagonal points of $\mathcal{Q}$ are collinear;
- when q is odd, the three black diagonal points of $\mathcal{Q}$ are not collinear.

A non trivial example of generalized hyperfocused arc
and our main result

EXAMPLE

Any 4-arc $\mathcal{Q}$ of white points, with its three black diagonal points, is a non trivial example of generalized hyperfocused arc.



Note that:

- when q is even, the three black diagonal points of $\mathcal{Q}$ are collinear;
- when q is odd, the three black diagonal points of $\mathcal{Q}$ are not collinear.

THEOREM (A.Blokhuis - G.Marino - F.M., 2013)

The $4-$arc is the only non trivial example of generalized hyperfocused arc, provided q is an odd prime.

Some Notations

From now on we set $\mathbb{F} = GF(p)$, p a prime $\neq 2, 3$.

Some Notations

From now on we set $\mathbb{F} = GF(p)$, p a prime $\neq 2, 3$.

- If $A = (a_1, a_2, a_3)$ is a non-zero vector of $\mathbb{F}^3$, we denote by $[A] = \langle (a_1, a_2, a_3) \rangle$ the point of $PG(2, p)$ with homogeneous coordinates $(a_1 : a_2 : a_3)$.

Some Notations

From now on we set $\mathbb{F} = GF(p)$, p a prime $\neq 2, 3$.

- If $A = (a_1, a_2, a_3)$ is a non-zero vector of $\mathbb{F}^3$, we denote by $[A] = \langle (a_1, a_2, a_3) \rangle$ the point of $PG(2, p)$ with homogeneous coordinates $(a_1 : a_2 : a_3)$.
- Sometimes, abusing notation, we will just write A instead of $[A]$ and, in this case, we mean that for the point $[A]$ we are considering the coordinates (a_1, a_2, a_3) or some other special ones, that should be clear from the context.

Some Notations

From now on we set $\mathbb{F} = GF(p)$, p a prime $\neq 2, 3$.

- If $A = (a_1, a_2, a_3)$ is a non-zero vector of $\mathbb{F}^3$, we denote by $[A] = \langle (a_1, a_2, a_3) \rangle$ the point of $PG(2, p)$ with homogeneous coordinates $(a_1 : a_2 : a_3)$.
- Sometimes, abusing notation, we will just write A instead of $[A]$ and, in this case, we mean that for the point $[A]$ we are considering the coordinates (a_1, a_2, a_3) or some other special ones, that should be clear from the context.
- We write $A \triangleq B$ if $[A] = [B]$, i.e. $A = \lambda B$, for some non zero λ in $\mathbb{F}$.

Some Notations

- For the following, let

$$\mathcal{H} = \{W_1 = [E_1], W_2 = [E_2], \ldots, W_{2n} = [E_{2n}]\}$$

be a generalized hyperfocused arc of order $2n$ in $PG(2, p)$, with black point-set $\mathcal{B}$.

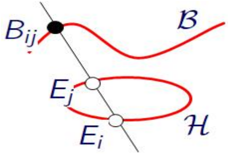
Some Notations

- For the following, let

$$\mathcal{H} = \{W_1 = [E_1], W_2 = [E_2], \ldots, W_{2n} = [E_{2n}]\}$$

be a generalized hyperfocused arc of order $2n$ in $PG(2,p)$, with black point-set $\mathcal{B}$.

- We denote by B_{ij} the unique black point on the line $< W_i, W_j >$ and we define b_{ij} by



$$B_{ij} \triangleq E_i + b_{ij} E_j .$$

Since $B_{ji} = B_{ij}$ we have $b_{ji} = 1/b_{ij}$.

A basic relation
and a notation

- Using the computational technique of Segre's lemma of tangents one can prove that

$$b_{ij}b_{jk}b_{ki} = 1$$

for $i \neq j \neq k \neq i$.

- Using the computational technique of Segre's lemma of tangents one can prove that

$$b_{ij}b_{jk}b_{ki} = 1$$

  for $i \neq j \neq k \neq i$.

- From $B_{ij} \stackrel{\triangle}{=} E_i + b_{ij}E_j$, $i,j \neq 1$, we get

$$B_{ij} \stackrel{\triangle}{=} b_{1i}E_i + b_{1j}E_j, \text{ for all } \; i,j = 2, \dots, 2n.$$

  Taking into account that

$$B_{1j} \stackrel{\triangle}{=} E_1 + b_{1j}E_j \;\text{ and }\; B_{i1} \stackrel{\triangle}{=} E_i + b_{i1}E_1 \stackrel{\triangle}{=} E_1 + b_{1i}E_i \,,$$

- Using the computational technique of Segre's lemma of tangents one can prove that

$$b_{ij} b_{jk} b_{ki} = 1$$

for $i \neq j \neq k \neq i$.

- From $B_{ij} \overset{\triangle}{=} E_i + b_{ij} E_j$, $i, j \neq 1$, we get

$$B_{ij} \overset{\triangle}{=} b_{1i} E_i + b_{1j} E_j, \text{ for all } \; i, j = 2, \ldots, 2n.$$

Taking into account that

$$B_{1j} \overset{\triangle}{=} E_1 + b_{1j} E_j \;\text{ and }\; B_{i1} \overset{\triangle}{=} E_i + b_{i1} E_1 \overset{\triangle}{=} E_1 + b_{1i} E_i \,,$$

and rescaling our E_s to $b_{1s} E_s$, for each $s \neq 1$,

- Using the computational technique of Segre's lemma of tangents one can prove that

$$b_{ij} b_{jk} b_{ki} = 1$$

for $i \neq j \neq k \neq i$.

- From $B_{ij} \stackrel{\triangle}{=} E_i + b_{ij} E_j$, $i, j \neq 1$, we get

$$B_{ij} \stackrel{\triangle}{=} b_{1i} E_i + b_{1j} E_j, \text{ for all } \; i, j = 2, \ldots, 2n.$$

Taking into account that

$$B_{1j} \stackrel{\triangle}{=} E_1 + b_{1j} E_j \;\text{ and }\; B_{i1} \stackrel{\triangle}{=} E_i + b_{i1} E_1 \stackrel{\triangle}{=} E_1 + b_{1i} E_i \,,$$

and rescaling our E_s to $b_{1s} E_s$, for each $s \neq 1$, we get

$$B_{ij} \stackrel{\triangle}{=} E_i + E_j \,, \text{ for all } \; i, j = 1, 2, \ldots, 2n.$$

Let ℓ be a line intersecting $\mathcal{B}$ in exactly $m < p$ points, set

$$S = \ell \cap \mathcal{B} = \{B_1, B_2, \ldots, B_m\}.$$

Intersection numbers of $\mathcal{B}$

Let ℓ be a line intersecting $\mathcal{B}$ in exactly $m < p$ points, set

$$S = \ell \cap \mathcal{B} = \{B_1, B_2, \ldots, B_m\}.$$

For a fixed white point $W \in \mathcal{H}$, define the two disjoint sets

$$S^- = \{W_1^-, W_2^-, \ldots, W_m^-\} \ , \ S^+ = \{W = W_1^+, W_2^+, \ldots, W_m^+\}$$

where

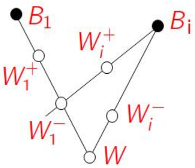
Let ℓ be a line intersecting $\mathcal{B}$ in exactly $m < p$ points, set

$$S = \ell \cap \mathcal{B} = \{B_1, B_2, \ldots, B_m\}.$$

For a fixed white point $W \in \mathcal{H}$, define the two disjoint sets

$$S^- = \{W_1^-, W_2^-, \ldots, W_m^-\} \ , \ S^+ = \{W = W_1^+, W_2^+, \ldots, W_m^+\}$$

where



- W_i^- is the unique white point other than W on the line $< W, B_i >$

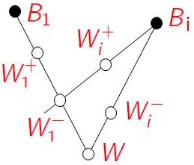
Let ℓ be a line intersecting $\mathcal{B}$ in exactly $m < p$ points, set

$$S = \ell \cap \mathcal{B} = \{B_1, B_2, \ldots, B_m\}.$$

For a fixed white point $W \in \mathcal{H}$, define the two disjoint sets

$$S^- = \{W_1^-, W_2^-, \ldots, W_m^-\} \ , \ S^+ = \{W = W_1^+, W_2^+, \ldots, W_m^+\}$$

where



- W_i^- is the unique white point other than W on the line $< W, B_i >$
- W_i^+ the unique white point other than W_1^- on the line $< W_1^-, B_i >$, $i = 1, \ldots, m$.

Intersection numbers of $\mathcal{B}$

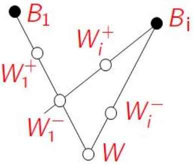
Let ℓ be a line intersecting $\mathcal{B}$ in exactly $m < p$ points, set

$$S = \ell \cap \mathcal{B} = \{B_1, B_2, \dots, B_m\}.$$

For a fixed white point $W \in \mathcal{H}$, define the two disjoint sets

$$S^- = \{W_1^-, W_2^-, \dots, W_m^-\} \ , \ S^+ = \{W = W_1^+, W_2^+, \dots, W_m^+\}$$

where



- W_i^- is the unique white point other than W on the line $< W, B_i >$
- W_i^+ the unique white point other than W_1^- on the line $< W_1^-, B_i >$, $i = 1, \dots, m$.

Using appropriate white points, $\mathcal{H}$ can be partitioned into pairs of blocks, each block of size m, so m **must be a divisor of** n.

$S \cup S^- \cup S^+$ is a dual 3-net of order m

Let $B = B_{ij}$ be the black point on the line $< W_i^+, W_j^- >$, $i, j = 1, 2, \ldots, m$, and fix coordinates of the black points on ℓ so that

$$B_i = E_1^+ + E_i^- = E + E_i^-.$$

$S \cup S^{-} \cup S^{+}$ is a dual 3-net of order m

Let $B = B_{ij}$ be the black point on the line $< W_i^+, W_j^- >$, $i, j = 1, 2, \ldots, m$, and fix coordinates of the black points on ℓ so that

$$B_i = E_1^+ + E_i^- = E + E_i^-.$$

Then

$$B = B_{ij} \stackrel{\triangle}{=} E_i^+ + E_j^- \stackrel{\triangle}{=} B_i - E_1^- + B_j - E_1^+$$

$$\stackrel{\triangle}{=} \alpha B_i + \beta B_j - (E_1^- + E_1^+) = \alpha B_i + \beta B_j + \gamma B_1,$$

for some constants α, β, γ. So B is on $\ell \cap \mathcal{B} = S$ and

Let $B = B_{ij}$ be the black point on the line $< W_i^+, W_j^- >$, $i, j = 1, 2, \ldots, m$, and fix coordinates of the black points on ℓ so that

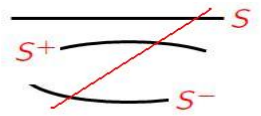
$$B_i = E_1^+ + E_i^- = E + E_i^-.$$

Then

$$B = B_{ij} \triangleq E_i^+ + E_j^- \triangleq B_i - E_1^- + B_j - E_1^+$$

$$\triangleq \alpha B_i + \beta B_j - (E_1^- + E_1^+) = \alpha B_i + \beta B_j + \gamma B_1,$$

for some constants α, β, γ. So B is on $\ell \cap \mathcal{B} = S$ and



$S \cup S^- \cup S^+$ is a dual 3-net of order m

Let $B = B_{ij}$ be the black point on the line $< W_i^+, W_j^- >$, $i, j = 1, 2, \ldots, m$, and fix coordinates of the black points on ℓ so that

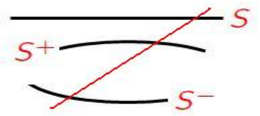
$$B_i = E_1^+ + E_i^- = E + E_i^-.$$

Then

$$B = B_{ij} \triangleq E_i^+ + E_j^- \triangleq B_i - E_1^- + B_j - E_1^+$$

$$\triangleq \alpha B_i + \beta B_j - (E_1^- + E_1^+) = \alpha B_i + \beta B_j + \gamma B_1,$$

for some constants α, β, γ. So B is on $\ell \cap \mathcal{B} = S$ and



$S \cup S^- \cup S^+$ is a dual 3-net of order m.

Classifying $\mathcal{H}$

By A.Blokhuis-G.Korchmáros-F.M. Theorem,

$S^- \cup S^+$ is a set of $2m$ points on a conic Γ and
m is the size of a subgroup of a group defined on $\Gamma \setminus \ell$.

Classifying $\mathcal{H}$

By A.Blokhuis-G.Korchmáros-F.M. Theorem,

$S^- \cup S^+$ is a set of $2m$ points on a conic Γ and
m is the size of a subgroup of a group defined on $\Gamma \setminus \ell$.

It follows that

m divides $p+1$ or $p-1$,

according to the fact that Γ has 0 or 2 points in common with ℓ, respectively.

Classifying $\mathcal{H}$

By A.Blokhuis-G.Korchmáros-F.M. Theorem,

$S^- \cup S^+$ is a set of $2m$ points on a conic Γ and
m is the size of a subgroup of a group defined on $\Gamma \setminus \ell$.

It follows that

m divides $p + 1$ or $p - 1$,

according to the fact that Γ has 0 or 2 points in common with ℓ, respectively.
According to this two cases, we say that $\mathcal{H}$ is of

elliptic or **hyperbolic type**,

respectively.

Classifying $\mathcal{H}$

By A.Blokhuis-G.Korchmáros-F.M. Theorem,

$S^- \cup S^+$ is a set of $2m$ points on a conic Γ and
m is the size of a subgroup of a group defined on $\Gamma \setminus \ell$.

It follows that

m divides $p+1$ or $p-1$,

according to the fact that Γ has 0 or 2 points in common with ℓ, respectively.
According to this two cases, we say that $\mathcal{H}$ is of

elliptic or **hyperbolic type**,

respectively.
The case $|\mathcal{H} \cap \ell| = 1$ cannot occur, otherwise m should divide p.

A first step

Assume that the equation of ℓ in $PG(2, p)$ is $z = 0$, w.r.t. coordinates $(x : y : z)$.

A first step

Assume that the equation of ℓ in $PG(2,p)$ is $z=0$, w.r.t. coordinates $(x:y:z)$.

- In the hyperbolic case we can assume that the conic Γ has equation $xy=z$ and we may take

$$S^+ = \{(u : \frac{1}{u} : 1) \ \ : \ \ u \in \mathbb{F}^* \text{ and } u^m = 1\}.$$

A first step

Assume that the equation of ℓ in $PG(2,p)$ is $z = 0$, w.r.t. coordinates $(x : y : z)$.

- In the hyperbolic case we can assume that the conic Γ has equation $xy = z$ and we may take
$$S^+ = \{(u : \frac{1}{u} : 1) \;\; : \;\; u \in \mathbb{F}^* \text{ and } u^m = 1\}.$$
- In the elliptic case we identify $AG(2,p) = PG(2,p) \setminus \ell$ with the field F_{p^2}. If we denote by $(a;1)$, with $a \in F_{p^2}$, the coordinates of affine points of $PG(2,p)$, we can assume that the conic Γ has equation $x^{p+1} = 1$ and we may take
$$S^+ = \{(x;1) \;\; : \;\; x^m = 1\}.$$

A first step

Assume that the equation of ℓ in $PG(2,p)$ is $z=0$, w.r.t. coordinates $(x:y:z)$.

- In the hyperbolic case we can assume that the conic Γ has equation $xy=z$ and we may take

$$S^+ = \{(u : \frac{1}{u} : 1) \ : \ u \in \mathbb{F}^* \text{ and } u^m = 1\}.$$

- In the elliptic case we identify $AG(2,p) = PG(2,p) \setminus \ell$ with the field F_{p^2}. If we denote by $(a;1)$, with $a \in F_{p^2}$, the coordinates of affine points of $PG(2,p)$, we can assume that the conic Γ has equation $x^{p+1}=1$ and we may take

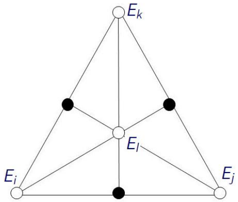
$$S^+ = \{(x;1) \ : \ x^m = 1\}.$$

Using these two representations of S^+ we can prove:

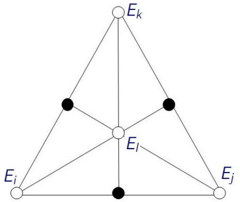
Lemma

If a line ℓ intersects $\mathcal{B}$ in exactly $m<p$ points, then $m \leq 4$.

A second step

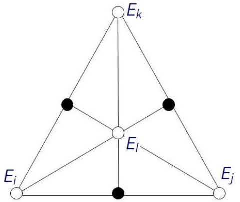


A second step



A 4-set $\{E_i, E_j, E_k, E_l\}$ of withe points of $\mathcal{H}$ is said to be *special* if $E_i + E_j + E_k + E_l = \mathbf{0}$. This means that $\{E_i, E_j, E_k, E_l\}$ is a non trivial generalized hyperfocused 4-arc contained in $\mathcal{H}$.

A second step



A 4-set $\{E_i, E_j, E_k, E_l\}$ of withe points of $\mathcal{H}$ is said to be *special* if $E_i + E_j + E_k + E_l = \mathbf{0}$. This means that $\{E_i, E_j, E_k, E_l\}$ is a non trivial generalized hyperfocused 4-arc contained in $\mathcal{H}$.

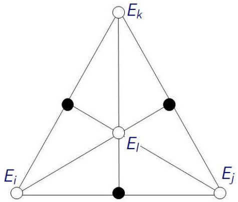
Lemma

Let $E_1, E_2, E_3, E_4, E_5, E_6$ be six distinct points of $\mathcal{H}$ such that

$$E_1 + E_2 \triangleq E_3 + E_4 \triangleq E_5 + E_6 \triangleq B\,.$$

Then, if $\{E_1, E_2, E_3, E_4\}$ and $\{E_1, E_2, E_5, E_6\}$ are special, $\{E_3, E_4, E_5, E_6\}$ is not.

A second step



A 4-set $\{E_i, E_j, E_k, E_l\}$ of withe points of $\mathcal{H}$ is said to be *special* if $E_i + E_j + E_k + E_l = \mathbf{0}$. This means that $\{E_i, E_j, E_k, E_l\}$ is a non trivial generalized hyperfocused 4-arc contained in $\mathcal{H}$.

Lemma

Let $E_1, E_2, E_3, E_4, E_5, E_6$ be six distinct points of $\mathcal{H}$ such that

$$E_1 + E_2 \triangleq E_3 + E_4 \triangleq E_5 + E_6 \triangleq B\,.$$

Then, if $\{E_1, E_2, E_3, E_4\}$ and $\{E_1, E_2, E_5, E_6\}$ are special, $\{E_3, E_4, E_5, E_6\}$ is not.

This lemma ensures that, if $n > 2$, $\mathcal{H}$ contains a non special $4-$set of withe points.

The main result

Assume $n > 2$ and let E_1, E_2, E_3, E_4 be a non special $4-$set. Then we have 5 different black points:

$$B_{12} = B_{34},\ B_{13},\ B_{14},\ B_{23},\ B_{24}.$$

The main result

Assume $n > 2$ and let E_1, E_2, E_3, E_4 be a non special $4-$set. Then we have 5 different black points:

$$B_{12} = B_{34},\ B_{13},\ B_{14},\ B_{23},\ B_{24}.$$

Moreover it is possible to show that they are in a position that we may put

$$B_{12} = B_{34} = (0,0,1),\ \ B_{13} = (1,0,0),\ \ B_{24} = (1,0,1),$$

$$B_{14} = (0,1,0),\ \ B_{23} = (0,1,1).$$

The main result

Assume $n > 2$ and let E_1, E_2, E_3, E_4 be a non special 4−set. Then we have 5 different black points:

$$B_{12} = B_{34},\ B_{13},\ B_{14},\ B_{23},\ B_{24}.$$

Moreover it is possible to show that they are in a position that we may put

$$B_{12} = B_{34} = (0,0,1),\ \ B_{13} = (1,0,0),\ \ B_{24} = (1,0,1),$$

$$B_{14} = (0,1,0),\ \ B_{23} = (0,1,1).$$

Finally, using this frame and after long and non trivial calculations, we can prove our main result.

THEOREM

If p is an odd prime and $\mathcal{H}$ is a hyperfocused arc of size $2n$, in $PG(2,p)$ then $n \leq 2$.

- Generalized hyperfocused arcs were introduced as a generalization of hyperfocused arcs, but this is not how we hit upon them.

- Generalized hyperfocused arcs were introduced as a generalization of hyperfocused arcs, but this is not how we hit upon them.
- We see them as a special case of a configuration whose study is motivated by the (strong) cylinder conjecture.

- Generalized hyperfocused arcs were introduced as a generalization of hyperfocused arcs, but this is not how we hit upon them.
- We see them as a special case of a configuration whose study is motivated by the (strong) cylinder conjecture.

The strong cylinder conjeture (Ball, 2011)

A set C of q^2 points in $AG(3, q)$ that intersects every plane in 0 mod q points must be a cylinder, i.e. the union of q parallel lines.

The ordinary conjecture states the same thing for q a prime.

In an attempt to prove the ordinary cylinder conjecture we found in $PG(2, p)$ configurations consisting of

In an attempt to prove the ordinary cylinder conjecture we found in $PG(2, p)$ configurations consisting of

- a set $\mathcal{W}$ of $k \leq (p+1)/2$ 'white' points,

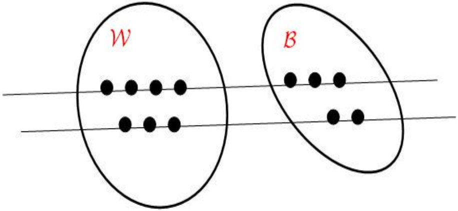
In an attempt to prove the ordinary cylinder conjecture we found in $PG(2, p)$ configurations consisting of

- a set $\mathcal{W}$ of $k \leq (p+1)/2$ 'white' points,
- a *multiset* $\mathcal{B}$ of $k-1$ 'black' points,

In an attempt to prove the ordinary cylinder conjecture we found in $PG(2, p)$ configurations consisting of

- a set $\mathcal{W}$ of $k \leq (p+1)/2$ 'white' points,
- a *multiset* $\mathcal{B}$ of $k-1$ 'black' points,

with the property that every line containing $m > 0$ white points contains exactly $m-1$ black points (counted with multiplicity).



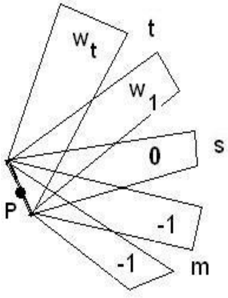
- Let C be a set of q^2 points in $AG(3, q)$ that intersects every plane in 0 mod q points.

- Let C be a set of q^2 points in $AG(3, q)$ that intersects every plane in 0 mod q points.
- Take a point $P \in AG(3, q) \setminus C$ and project C from P, i.e. consider the quotient geometry $\pi = PG(2, q)$ in P (points and lines in the quotient are lines and planes trough P in $PG(3, q)$, respectively).

- Let C be a set of q^2 points in $AG(3, q)$ that intersects every plane in 0 mod q points.
- Take a point $P \in AG(3, q) \setminus C$ and project C from P, i.e. consider the quotient geometry $\pi = PG(2, q)$ in P (points and lines in the quotient are lines and planes trough P in $PG(3, q)$, respectively).
- The projection of C is a multiset X of q^2 points in $PG(2, q)$ with a multiple of q points on every line.

- Let C be a set of q^2 points in $AG(3, q)$ that intersects every plane in 0 mod q points.
- Take a point $P \in AG(3, q) \setminus C$ and project C from P, i.e. consider the quotient geometry $\pi = PG(2, q)$ in P (points and lines in the quotient are lines and planes trough P in $PG(3, q)$, respectively).
- The projection of C is a multiset X of q^2 points in $PG(2, q)$ with a multiple of q points on every line.
- Let the *weight* of a line α in π be $k - 1$, if α contains kq points of C as plane of $PG(3, q)$.

- Let C be a set of q^2 points in $AG(3, q)$ that intersects every plane in 0 mod q points.
- Take a point $P \in AG(3, q) \setminus C$ and project C from P, i.e. consider the quotient geometry $\pi = PG(2, q)$ in P (points and lines in the quotient are lines and planes trough P in $PG(3, q)$, respectively).
- The projection of C is a multiset X of q^2 points in $PG(2, q)$ with a multiple of q points on every line.
- Let the *weight* of a line α in π be $k - 1$, if α contains kq points of C as plane of $PG(3, q)$.
- All points of a line of weight -1 do not occur in the multiset X, that is they have weight 0 as points of X.



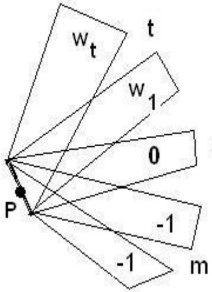
$$m+s+t=q+1$$

$$(w_1+1)q+\cdots(w_t+1)q+sq=q^2$$

$$w_1+\cdots w_t+t+s=q$$

$$w_1+\cdots w_t-m=q-t-s-k=-1$$

$$w_1+\cdots w_t=m-1$$



$$m + s + t = q + 1$$

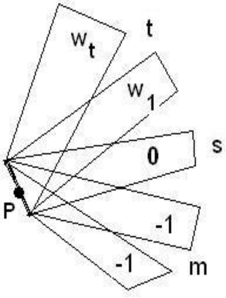
$$(w_1 + 1)q + \cdots (w_t + 1)q + sq = q^2$$

$$w_1 + \cdots w_t + t + s = q$$

$$w_1 + \cdots w_t - m = q - t - s - k = -1$$

$$w_1 + \cdots w_t = m - 1$$

- If we add up the weights of the lines through a zero-point, we get -1



$$m+s+t=q+1$$
$$(w_1+1)q+\cdots(w_t+1)q+sq=q^2$$
$$w_1+\cdots w_t+t+s=q$$
$$w_1+\cdots w_t-m=q-t-s-k=-1$$
$$w_1+\cdots w_t=m-1$$

- If we add up the weights of the lines through a zero-point, we get -1
- If Q is a point on $m>0$ lines of weight -1, then the weights of the positive lines through Q add up to $m-1$.

If we dualize last construction, we obtain two disjoint sets of points of $PG(2, q)$, namely:

If we dualize last construction, we obtain two disjoint sets of points of $PG(2, q)$, namely:

- a set $\mathcal{W}$ of "white points" corresponding to the duals of the lines of weight -1;

If we dualize last construction, we obtain two disjoint sets of points of $PG(2, q)$, namely:

- a set $\mathcal{W}$ of "white points" corresponding to the duals of the lines of weight -1;
- a multi-set $\mathcal{B}$ of "black points" corresponding to the duals of the positive weighted lines, the multiplicity of a black point being the weight of the corresponding line.

If we dualize last construction, we obtain two disjoint sets of points of $PG(2,q)$, namely:

- a set $\mathcal{W}$ of "white points" corresponding to the duals of the lines of weight -1;
- a multi-set $\mathcal{B}$ of "black points" corresponding to the duals of the positive weighted lines, the multiplicity of a black point being the weight of the corresponding line.

Moreover,

- every line containing $m > 1$ white points contains exactly $m-1$ black points;

If we dualize last construction, we obtain two disjoint sets of points of $PG(2, q)$, namely:

- a set $\mathcal{W}$ of "white points" corresponding to the duals of the lines of weight -1;
- a multi-set $\mathcal{B}$ of "black points" corresponding to the duals of the positive weighted lines, the multiplicity of a black point being the weight of the corresponding line.

Moreover,

- every line containing $m > 1$ white points contains exactly $m - 1$ black points;
- every line having exactly one white point has no black points;

If we dualize last construction, we obtain two disjoint sets of points of $PG(2, q)$, namely:

- a set $\mathcal{W}$ of "white points" corresponding to the duals of the lines of weight -1;
- a multi-set $\mathcal{B}$ of "black points" corresponding to the duals of the positive weighted lines, the multiplicity of a black point being the weight of the corresponding line.

Moreover,

- every line containing $m > 1$ white points contains exactly $m - 1$ black points;
- every line having exactly one white point has no black points;
- the total number of black points is one less than the number of white points.

In the example of the cylinder the configuration of all black and white points is on a line, so the study of the ordinary cylinder conjecture is related to the following problem:

In the example of the cylinder the configuration of all black and white points is on a line, so the study of the ordinary cylinder conjecture is related to the following problem:

Is it possible to find (and exclude) the other configurations?

In the example of the cylinder the configuration of all black and white points is on a line, so the study of the ordinary cylinder conjecture is related to the following problem:

Is it possible to find (and exclude) the other configurations?

- In case the set $\mathcal{W}$ is an arc the multiset $\mathcal{B}$ is an ordinary set and we are looking at a generalized hyperfocused arc. Our main result therefore is that this situation essentially does not occur.

In the example of the cylinder the configuration of all black and white points is on a line, so the study of the ordinary cylinder conjecture is related to the following problem:

Is it possible to find (and exclude) the other configurations?

- In case the set $\mathcal{W}$ is an arc the multiset $\mathcal{B}$ is an ordinary set and we are looking at a generalized hyperfocused arc. Our main result therefore is that this situation essentially does not occur.
- To classify these configurations in general seems to be hopeless but the prime case could be doable (and might settle the cylinder conjecture!).

Known examples of configurations of withe and black points with at most $(p+1)/2$ white points, p a prime

Known examples of configurations of withe and black points with at most $(p+1)/2$ white points, p a prime

- **(White and black points are collinear)** All white points are collinear, black points are arbitrary other points on this line, the right number of them (this is the only example coming from cylinders).

Known examples of configurations of withe and black points with at most $(p+1)/2$ white points, p a prime

- **(White and black points are collinear)** All white points are collinear, black points are arbitrary other points on this line, the right number of them (this is the only example coming from cylinders).
- **(White points on two lines)** In $AG(2,p)$ consider as white points $(a,0)$ and $(0,b)$ where a and b are in a subgroup of $GF(p)^*$ of order n say (or in a coset). Take black points at infinity in the points $(a:-b:0) = (1:-b/a:0)$, and take the origin with multiplicity $n-1$.

Known examples of configurations of withe and black points with at most $(p+1)/2$ white points, p a prime

- **(White and black points are collinear)** All white points are collinear, black points are arbitrary other points on this line, the right number of them (this is the only example coming from cylinders).
- **(White points on two lines)** In $AG(2,p)$ consider as white points $(a,0)$ and $(0,b)$ where a and b are in a subgroup of $GF(p)^*$ of order n say (or in a coset). Take black points at infinity in the points $(a:-b:0)=(1:-b/a:0)$, and take the origin with multiplicity $n-1$.
- **(White points form an arc)** The white points form a 4-arc, and there are 3 black points, the diagonal points.

The end

The end

THANKS FOR ATTENTION