

Parallelisms of $PG(3, q)$

Oscar Vega
California State University, Fresno

February 21, 2008

Definition

Definition

Let V be a 4-dimensional vector space over the finite field $GF(q)$.

Definition

Definition

Let V be a 4-dimensional vector space over the finite field $GF(q)$.

The 3-dimensional projective space over $GF(q)$, called $PG(3, q)$, is the geometry obtained by considering

Definition

Definition

Let V be a 4-dimensional vector space over the finite field $GF(q)$.

The 3-dimensional projective space over $GF(q)$, called $PG(3, q)$, is the geometry obtained by considering

- i the 1-dimensional subspaces of V as points of $PG(3, q)$,

Definition

Definition

Let V be a 4-dimensional vector space over the finite field $GF(q)$.

The 3-dimensional projective space over $GF(q)$, called $PG(3, q)$, is the geometry obtained by considering

- i the 1-dimensional subspaces of V as points of $PG(3, q)$,
- ii the 2-dimensional subspaces of V as lines of $PG(3, q)$, and

Definition

Definition

Let V be a 4-dimensional vector space over the finite field $GF(q)$.

The 3-dimensional projective space over $GF(q)$, called $PG(3, q)$, is the geometry obtained by considering

- i the 1-dimensional subspaces of V as points of $PG(3, q)$,
- ii the 2-dimensional subspaces of V as lines of $PG(3, q)$, and
- iii the 3-dimensional subspaces of V as planes of $PG(3, q)$

Definition

Definition

Let V be a 4-dimensional vector space over the finite field $GF(q)$.

The 3-dimensional projective space over $GF(q)$, called $PG(3, q)$, is the geometry obtained by considering

- i the 1-dimensional subspaces of V as points of $PG(3, q)$,
- ii the 2-dimensional subspaces of V as lines of $PG(3, q)$, and
- iii the 3-dimensional subspaces of V as planes of $PG(3, q)$

Note that any two planes of $PG(3, q)$ must intersect.

Counting in $PG(3, q)$

As a 4-dimensional vector space over a finite field has finitely many subspaces, it is clear that $PG(3, q)$ has a finite number of points and lines.

Counting in $PG(3, q)$

As a 4-dimensional vector space over a finite field has finitely many subspaces, it is clear that $PG(3, q)$ has a finite number of points and lines.

Some easy counting yields

Counting in $PG(3, q)$

As a 4-dimensional vector space over a finite field has finitely many subspaces, it is clear that $PG(3, q)$ has a finite number of points and lines.

Some easy counting yields

- $PG(3, q)$ has $(q + 1)(q^2 + 1)$ points,

Counting in $PG(3, q)$

As a 4-dimensional vector space over a finite field has finitely many subspaces, it is clear that $PG(3, q)$ has a finite number of points and lines.

Some easy counting yields

- $PG(3, q)$ has $(q + 1)(q^2 + 1)$ points,
- $PG(3, q)$ has $(q^2 + 1)(q^2 + q + 1)$ lines,

Counting in $PG(3, q)$

As a 4-dimensional vector space over a finite field has finitely many subspaces, it is clear that $PG(3, q)$ has a finite number of points and lines.

Some easy counting yields

- $PG(3, q)$ has $(q + 1)(q^2 + 1)$ points,
- $PG(3, q)$ has $(q^2 + 1)(q^2 + q + 1)$ lines,
- Each line contains exactly $q + 1$ points,

Counting in $PG(3, q)$

As a 4-dimensional vector space over a finite field has finitely many subspaces, it is clear that $PG(3, q)$ has a finite number of points and lines.

Some easy counting yields

- $PG(3, q)$ has $(q + 1)(q^2 + 1)$ points,
- $PG(3, q)$ has $(q^2 + 1)(q^2 + q + 1)$ lines,
- Each line contains exactly $q + 1$ points,
- Each point is in exactly $q^2 + q + 1$ lines

Spreads of $PG(3, q)$

- A spread S of $PG(3, q)$ is collection of disjoint lines that cover all the points of $PG(3, q)$.

Spreads of $PG(3, q)$

- A spread S of $PG(3, q)$ is collection of disjoint lines that cover all the points of $PG(3, q)$.
- Equivalently, a spread of $PG(3, q)$ is collection of $q^2 + 1$ lines that cover all the points of $PG(3, q)$.

Spreads of $PG(3, q)$

- A spread S of $PG(3, q)$ is collection of disjoint lines that cover all the points of $PG(3, q)$.
- Equivalently, a spread of $PG(3, q)$ is collection of $q^2 + 1$ lines that cover all the points of $PG(3, q)$.
- The elements of S are called *the components of S* .

Spreads of $PG(3, q)$

- A spread S of $PG(3, q)$ is collection of disjoint lines that cover all the points of $PG(3, q)$.
- Equivalently, a spread of $PG(3, q)$ is collection of $q^2 + 1$ lines that cover all the points of $PG(3, q)$.
- The elements of S are called *the components of S* .
- **Theorem:** (André, 1954) Spreads, translation planes... the same thing.

Representation of lines

- We will write the vectors of V as $v = (x, y)$,

Representation of lines

- We will write the vectors of V as $v = (x, y)$, with $x = (x_1, x_2)$ and $y = (y_1, y_2)$.

Representation of lines

- We will write the vectors of V as $v = (x, y)$, with $x = (x_1, x_2)$ and $y = (y_1, y_2)$.
- The line of $PG(3, q)$ given by the subspace of all vectors of the form $(0, y)$ will be called $x = 0$.

Representation of lines

- We will write the vectors of V as $v = (x, y)$, with $x = (x_1, x_2)$ and $y = (y_1, y_2)$.
- The line of $PG(3, q)$ given by the subspace of all vectors of the form $(0, y)$ will be called $x = 0$.
- For a fixed matrix $M \in M_2(q)$, call $y = xM$ to the line given by the 2-dimensional subspace

Representation of lines

- We will write the vectors of V as $v = (x, y)$, with $x = (x_1, x_2)$ and $y = (y_1, y_2)$.
- The line of $PG(3, q)$ given by the subspace of all vectors of the form $(0, y)$ will be called $x = 0$.
- For a fixed matrix $M \in M_2(q)$, call $y = xM$ to the line given by the 2-dimensional subspace

$$\{(x, y) \in V; y = xM\}.$$

Representation of lines

- We will write the vectors of V as $v = (x, y)$, with $x = (x_1, x_2)$ and $y = (y_1, y_2)$.
- The line of $PG(3, q)$ given by the subspace of all vectors of the form $(0, y)$ will be called $x = 0$.
- For a fixed matrix $M \in M_2(q)$, call $y = xM$ to the line given by the 2-dimensional subspace

$$\{(x, y) \in V; y = xM\}.$$

- It is not hard to prove that any line of $PG(3, q)$ that is disjoint from $x = 0$ can be represented as $y = xM$, for some suitable $M \in M_2(q)$.

Spreads as sets of matrices

- Since a spread is just a bunch of lines, and (some) lines can be thought of as matrices, then it seems natural to think spreads as sets of matrices, but...

Spreads as sets of matrices

- Since a spread is just a bunch of lines, and (some) lines can be thought of as matrices, then it seems natural to think spreads as sets of matrices, but...
- we first need to be sure that $x = 0$ is a line of the spread.

Spreads as sets of matrices

- Since a spread is just a bunch of lines, and (some) lines can be thought of as matrices, then it seems natural to think spreads as sets of matrices, but...
- we first need to be sure that $x = 0$ is a line of the spread.
- We can always do that by just doing a change of basis in V .

Spreads as sets of matrices

- Since a spread is just a bunch of lines, and (some) lines can be thought of as matrices, then it seems natural to think spreads as sets of matrices, but...
- we first need to be sure that $x = 0$ is a line of the spread.
- We can always do that by just doing a change of basis in V .
- Spreads may be represented as the line $x = 0$ and a set of q^2 matrices.

Spreads as sets of matrices

- Since a spread is just a bunch of lines, and (some) lines can be thought of as matrices, then it seems natural to think spreads as sets of matrices, but...
- we first need to be sure that $x = 0$ is a line of the spread.
- We can always do that by just doing a change of basis in V .
- Spreads may be represented as the line $x = 0$ and a set of q^2 matrices.
- The non-zero matrices in a spread must be invertible, and any non-zero difference of them must be invertible as well.

An example

- Let q be odd, and let θ be a non-square in $GF(q)$. Then, the set

An example

- Let q be odd, and let θ be a non-square in $GF(q)$. Then, the set

$$\mathcal{S} = \left\{ \begin{bmatrix} u & \theta t \\ t & u \end{bmatrix} ; t, u \in GF(q) \right\}$$

An example

- Let q be odd, and let θ be a non-square in $GF(q)$. Then, the set

$$\mathcal{S} = \left\{ \begin{bmatrix} u & \theta t \\ t & u \end{bmatrix} ; t, u \in GF(q) \right\}$$

defines a spread of $PG(3, q)$.

An example

- Let q be odd, and let θ be a non-square in $GF(q)$. Then, the set

$$\mathcal{S} = \left\{ \begin{bmatrix} u & \theta t \\ t & u \end{bmatrix} ; t, u \in GF(q) \right\}$$

defines a spread of $PG(3, q)$.

- Of course, we are assuming that the line $x = 0$ is also in the spread above.

An example

- Let q be odd, and let θ be a non-square in $GF(q)$. Then, the set

$$\mathcal{S} = \left\{ \begin{bmatrix} u & \theta t \\ t & u \end{bmatrix} ; t, u \in GF(q) \right\}$$

defines a spread of $PG(3, q)$.

- Of course, we are assuming that the line $x = 0$ is also in the spread above.
- Note that \mathcal{S} is a field of order q^2 .

Regular spreads

- Spreads given by fields of matrices are called *regular*.

Regular spreads

- Spreads given by fields of matrices are called *regular*.
- Not all spreads of $PG(3, q)$ are regular.

Regular spreads

- Spreads given by fields of matrices are called *regular*.
- Not all spreads of $PG(3, q)$ are regular.
- Regular spreads have the nicest properties among spreads.

Parallelisms

- Since $PG(3, q)$ has $(q^2 + 1)(q^2 + q + 1)$ lines, and each spread is formed by $q^2 + 1$ lines, then it seems natural to see if one can partition the set of lines into $q^2 + q + 1$ disjoint spreads.

Parallelisms

- Since $PG(3, q)$ has $(q^2 + 1)(q^2 + q + 1)$ lines, and each spread is formed by $q^2 + 1$ lines, then it seems natural to see if one can partition the set of lines into $q^2 + q + 1$ disjoint spreads.
- A partition of the set of lines into disjoint spreads is called a parallelism of $PG(3, q)$.

Parallelisms

- Since $PG(3, q)$ has $(q^2 + 1)(q^2 + q + 1)$ lines, and each spread is formed by $q^2 + 1$ lines, then it seems natural to see if one can partition the set of lines into $q^2 + q + 1$ disjoint spreads.
- A partition of the set of lines into disjoint spreads is called a parallelism of $PG(3, q)$.
- A parallelism formed by only regular spreads is called a regular parallelism.

Existence of parallelisms

- There are parallelisms of $PG(3, q)$, for every q .

Existence of parallelisms

- There are parallelisms of $PG(3, q)$, for every q .
- There are 'regular' parallelisms of $PG(3, q)$, for all $q \equiv 2 \pmod{3}$.

Existence of parallelisms

- There are parallelisms of $PG(3, q)$, for every q .
- There are 'regular' parallelisms of $PG(3, q)$, for all $q \equiv 2 \pmod{3}$.
- There are no regular parallelisms of neither $PG(3, 3)$ nor $PG(3, 4)$.

Existence of parallelisms

- There are parallelisms of $PG(3, q)$, for every q .
- There are 'regular' parallelisms of $PG(3, q)$, for all $q \equiv 2 \pmod{3}$.
- There are no regular parallelisms of neither $PG(3, 3)$ nor $PG(3, 4)$.
- This is when I tell Lunardon's theorem's story

Deficiency k parallelisms

- A set of $q^2 + q + 1 - k$ disjoint spreads is said to be a parallelism of deficiency k .

Deficiency k parallelisms

- A set of $q^2 + q + 1 - k$ disjoint spreads is said to be a parallelism of deficiency k .
- A parallelism of deficiency one can always be extended to a 'full' parallelism.

Deficiency k parallelisms

- A set of $q^2 + q + 1 - k$ disjoint spreads is said to be a parallelism of deficiency k .
- A parallelism of deficiency one can always be extended to a 'full' parallelism.
- A very old conjecture says that a **regular** parallelism of deficiency one can only be extended to a **regular** parallelism.

Deficiency k parallelisms

- A set of $q^2 + q + 1 - k$ disjoint spreads is said to be a parallelism of deficiency k .
- A parallelism of deficiency one can always be extended to a 'full' parallelism.
- A very old conjecture says that a **regular** parallelism of deficiency one can only be extended to a **regular** parallelism.
- There are examples of parallelisms where all but one of the spreads belong to the same class.

Definition

In $PG(3, q)$ we fix two lines, ℓ and m , and choose a basis of V so that m is $y = 0$ and ℓ is $x = 0$.

Let $L^* \subset L$ be the set of all lines not intersecting ℓ . We identify L^* with $M_2(q)$ in the natural way.

Fix $M \in M_2(q)$. Consider the characteristic function of M , which is given by

$$\chi_M : M_2(q) \rightarrow \mathbb{F}_q, \quad C_M(N) = \begin{cases} 1 & \text{for } M = N \\ 0 & \text{for } M \neq N \end{cases}$$

Using χ_M we define the characteristic function of a line of L^* in the obvious way. Also, we naturally extend χ to any $A \subset L^*$.

Note that the definition of χ depends on the initial choice of ℓ and m , but the set L^* only depends on ℓ .

For $A \subset L^*$, the function χ_A goes from $M_2(q)$ to \mathbb{F}_q , thus it can be represented in a unique way as a polynomial in four variables with degree at most $q - 1$ in each variable.

From now on, we will consider all characteristic functions to be polynomials with these conditions.

Let S be a spread that contains the line ℓ , we will call χ_S to the characteristic function of the set $S \setminus \{\ell\}$. Also, the total degree of χ_S will be called the degree of S , and will be denoted $\deg(S)$.

Liebler proposes the degree of a spread as a tool that may be used to classify spreads. This is the “invariant” we want to study.

Theorem The degree of a spread S containing ℓ and m is bounded by $2(q - 1)$ and $4q - 6$. Moreover, both bounds are reached.

Example Let $\theta \notin (\mathbb{F}_q)^2$. Consider the regular spread

$$S = \left\{ \begin{bmatrix} u & \theta t \\ t & u \end{bmatrix}; t, u \in \mathbb{F}_q \right\}.$$

Its polynomial

$$\chi_S \left(\begin{array}{cc} x & y \\ z & w \end{array} \right) = (1 - (y - \theta z)^{q-1})(1 - (x - w)^{q-1})$$

clearly has degree $2(q - 1)$.

Consider the group Ω that stabilizes ℓ , note that it also leaves L^*

invariant.

$$\Omega = \left\{ \left[\begin{array}{cc} A & B \\ 0 & D \end{array} \right]; A, B, D \in M_2(q), \det(AD) \neq 0 \right\}.$$

Theorem Let $U, V \subset L^*$, and $\Psi \in \Omega$, then

$$\deg(\chi_{\Psi(U)}) = \deg(\chi_U).$$

and

$$\deg(\chi_{\Psi(U)} - \chi_{\Psi(V)}) = \deg(\chi_U - \chi_V).$$

Note that the matrix of $\Psi(M)$ is $A^{-1}(B + MD)$. Then,

$$\chi_{\Psi(M)}(X) = \chi_M((AX - B)D^{-1})$$

for every $X \in GF(q)^4$. Since the expression $(AX - B)D^{-1}$ is linear, then the degree does not change.

The previous results consider χ constructed with respect to a fixed pair of lines, ℓ and m .

However, using these lemmas, we were able to prove that changing the line m does not affect the degree of any given subset of L^* . Of course, we cannot change the line ℓ , as this would change the set L^* .

A spread S is called regular if for any three lines of S , the regulus determined by them is contained in S .

Ω acts transitively on the sets of regular spreads that contain ℓ , and on the set of regular spreads that do not contain ℓ .

Theorem Let S be a spread that contains ℓ . S is regular, if and only if, its degree is $2(q - 1)$.

Given a regulus R contained in a spread S , it is possible to construct a new spread S' by substituting R by its opposite regulus. This process is often called “reversing a regulus”.

If S' is a spread such that there is a chain of spreads

$$S = S^{(1)}, S^{(2)}, \dots, S^{(t)} = S'$$

where S is regular and S_{i+1} is constructed by reversing a regulus in S_i , then S' is called a subregular spread.

Theorem For every subregular spread S' there exists a regular spread S and a set of disjoint reguli $\{R_i\}$ in S so that S' is constructed via the simultaneous substitution of each R_i by its opposite regulus.

The minimum number of reguli necessary to construct S' is called the index of S' .

Let S be a regular spread and let R be a regulus in S and R' be its opposite regulus. Let $S' = (S \setminus R) \cup R'$, a subregular spread of index one (Hall spread).

Note that if ℓ is not in R then $\ell \in S'$. Moreover,

$$\chi_{S'} = (\chi_S - \chi_R) + \chi_{R'} = \chi_S + (\chi_{R'} - \chi_R).$$

Therefore, in order to know the degree of $\chi_{S'}$ we need to compute the degree of $\chi_{R'} - \chi_R$.

Simple computations show that the degree of $\chi_{R'_k} - \chi_{R_k}$ is $4q - 6$. It follows that, for any $k \in \mathbb{F}_q^*$, the degree of the Hall spread S_k obtained by replacing the regulus R_k by R'_k in the regular spread S is also $4q - 6$.

It is not hard to see that Ω acts transitively on the set of reguli containing ℓ . This implies:

All sets of the form $S \setminus R$ where S is a regular spread and R is a regulus such that their opposite regulus contains ℓ have the same degree... which turns out to be $3(q - 1)$.

All reguli that contain ℓ have the same degree... also $3(q - 1)$.

The degree of a Hall spread is $4q - 6$ as long as ℓ is not in the reversed regulus. If ℓ is a line of the reversed regulus, then its degree is $3(q - 1)$.

Using the way the expression of highest degree in χ_{S_k} looks like we can construct (André) subregular spreads of any index having degree either $4q - 6$ or less than $4q - 6$.

The degree of an (André) subregular spread is larger or equal than $3(q - 1)$. The degree could be exactly $3(q - 1)$ only if the index of the spread is $(q - 1)/2$.

Spreads that come from flocks of quadratic cones have degree less than $3(q - 1)$, when ℓ is taken to be the line shared by all the reguli in the spread.

We believe the degree of a spread could be a useful tool to address this problem. We have some results that support this idea.

Theorem Let $P^- = \{S_1, \dots, S_{q^2+q}\}$ be a regular partial parallelism with deficiency one, and let S be the spread that extends P^- to a parallelism. Then, S has degree $\leq 3(q-1)$ with respect to any of its lines.

Corollary If the unknown spread is (André) subregular of index t , then $t < (q-1)/2$. In particular, if $q \neq 3$ then the unknown spread is not Hall.