

A polynomial invariant for spreads

Abstract

In “Virtual Derivation” R. Liebler defined a new algebraic invariant for spreads of $PG(3, q)$ by considering spreads as elements of the free \mathbb{Z} -module based on lines. He connected this invariant with the concept of “virtual derivation” and proved some properties of this invariant. In this talk we will revisit this invariant (but not virtual derivation) and will see some results that suggest ways this new tool may be used.

PG(3,q)

Let $q = p^n$, p an odd prime number and let \mathbb{F}_q denote the field with q elements.

In V , a 4-dimensional vector space over \mathbb{F}_q , we say that points are the 1-dimensional subspaces of V , lines are the 2-dimensional subspaces of V , and planes are the 3-dimensional subspaces of V .

Under this labeling, V becomes $\Sigma = PG(3, q)$.

Spreads of $PG(3,q)$

A spread S of $PG(3, q)$, or of V , is a set of lines of $PG(3, q)$ that partition the set of points (vectors) of V .

The elements of S are called components of the spread.

Note that the direct sum of any two components is V .

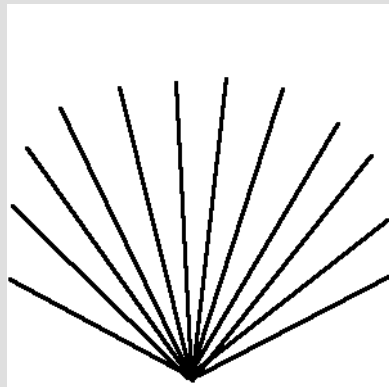


Fig. 1: Spread.

Important notation

For a fixed matrix $M \in M_2(q)$, call $(y = xM)$, or simply ℓ_M , the line of $PG(3, q)$ given by:

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

Note that any line of $PG(3, q)$ that does not intersect $(x = 0)$ may be represented as $(y = xM)$ for some suitable matrix $M \in M_2(q)$.

Example of a spread

Let θ be a non-square element in \mathbb{F}_q , then the set

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

is a field of order q^2 contained in $GL(2, q) \cup \{0\}$.

Define $S = \{(x = 0)\} \cup \{(y = xM) ; M \in F\}$.

The fact that F is a field implies that S is a spread.

Also, since F is a field, we say that S is a regular spread.

Starting to define the invariant

In Σ we fix two lines, ℓ and m , and coordinatize V so that $m = (y = 0)$ and $\ell = (x = 0)$.

Let L be the set of all lines in Σ , and let $L^* \subset L$ be the set of all lines not intersecting ℓ .

We identify L^* with $M_2(q)$ in the natural way.

Characteristic functions of sets of lines

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

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

Using C_M we define the characteristic function of a line of L^* in the obvious way. Also, we naturally extend χ to a characteristic function of 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 .

Characteristic polynomials

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.

The degree of a spread

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.

Liebler's article

Let \mathbb{L} be the free \mathbb{Z} -module based on all lines of $PG(3, q)$ and let Λ be

$$\Lambda = \langle R - R'; R \text{ is a regulus in } PG(3, q) \rangle_{\mathbb{Z}}$$

Definition: We say the spread S^* is obtained from the spread S by virtual derivation if $S^* - S \in \Lambda$.

Theorem: If S is virtually derivable from a regular spread, then S has degree $\leq 4q - 6$ with respect to any of its lines. The case of equality occurs for Hall planes whenever ℓ is not in the derivation set. In this case, there is a unique term of highest degree.

Questions proposed

- 1) Are there any spreads with degree less than $2(q-1)$?
- 2) Are there any spreads with degree larger than $4q-6$?
- 3) Are there any spreads that are not virtually derivable?

Remark: It is not true that for the Hall spread, there is a unique highest degree term in χ . However, if one represents spreads in $PG(3, q)$ as sets of elements in $\mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ then, for a Hall spread, the polynomial has a unique term of highest degree.

Bounds for $\deg(S)$

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.

To prove this, we represent $S \setminus \{\ell\}$ as:

$$S \setminus \{\ell\} = \left\{ \begin{bmatrix} g(t, u) & f(t, u) \\ t & u \end{bmatrix} ; t, u \in \mathbb{F}_q \right\}$$

for some polynomials f, g with degree at most $q - 1$ in each variable.

Then,

$$\chi_S \begin{pmatrix} x & y \\ z & w \end{pmatrix} = (1 - (y - f(z, w))^{q-1})(1 - (x - g(z, w))^{q-1})$$

The expressions that may have degree $\geq 4q - 6$ are

1) $y^{q-2}x^{q-2}f(g, z)g(z, w)$: At most degree $4q - 6$.

2) $x^{q-1}y^{q-2}f(z, w)$: At most degree $4q - 6$, as f has degree at most $q - 2$ in x because $f_y(x)$ is a permutation polynomial for every fixed y .

3) $y^{q-1}x^{q-2}g(z, w)$: Same as above.

Degree of a regular spread

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

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

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

Invariance

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

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

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

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

and

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

The proof of the previous theorem follows from

Let $\Psi = \begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$ and $M \in M_2(q)$.

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.

Q. For a fixed spread S , what is the largest group acting on the lines of $PG(3, q)$ that does not affect $deg(S)$?

m is not important

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^* .

Reguli

A regulus R is a set of $q + 1$ disjoint lines with the property that whenever a line intersects three of its lines, it intersects all the lines of R .

Given a regulus R , the set of $q + 1$ lines that intersects all the lines in R is also a regulus, the opposite to R .

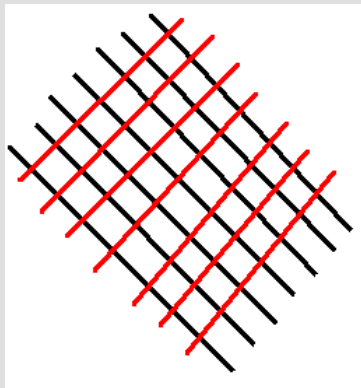


Fig. 2: A regulus and its opposite regulus.

Regular spreads

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 $2(q - 1)$.

Reversing a regulus

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”.

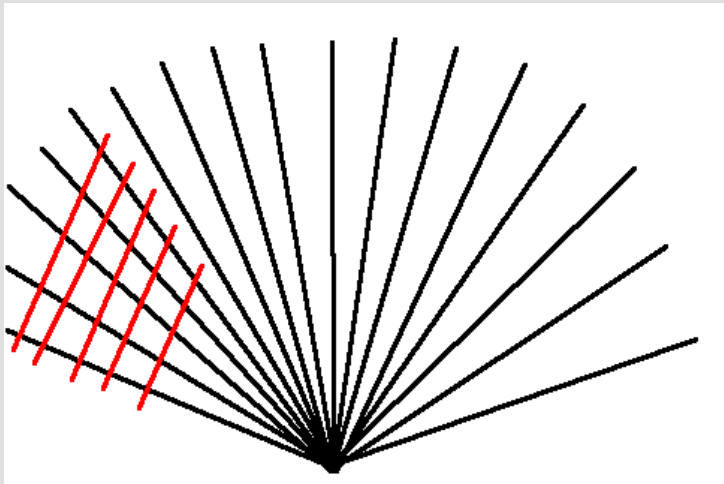


Fig. 3: A regulus reversed.

Subregular spreads

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' .

Hall spreads

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 $\chi_{R'} - \chi_R$.

$\chi_{R'} - \chi_R$

Consider the regular spread S considered before, for a fixed $k \in \mathbb{F}_q^*$ define the regulus:

$$R_k = \left\{ \begin{bmatrix} u & \theta t \\ t & u \end{bmatrix} ; u^2 - \theta t^2 = k \right\}.$$

It is not hard to see that

$$R'_k = \left\{ \begin{bmatrix} r & -\theta s \\ s & -r \end{bmatrix} ; r^2 - \theta s^2 = k \right\}$$

is the regulus opposite to R_k .

The degree of a Hall spread

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 $4q - 6$.

Remark There are four terms of degree $4q - 6$ in χ_{S_k} . Moreover, we can write them as $kp(x, y, z, w)$, where p is a polynomial having coefficients that do not depend on k .

The action of Ω

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

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

A few more results

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 $3(q - 1)$.

2) 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 $4q - 6$.

3) 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 $(q - 1)/2$.

4) 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.

Just note that, the matrices of such a spread look like

$$S = \left\{ \left[\begin{array}{cc} u + f(t) & g(t) \\ t & u \end{array} \right] ; t, u \in \mathbb{F}_q \right\}.$$

Parallelisms

A parallelism P is a set of $q^2 + q + 1$ disjoint spreads, that necessarily partition the lines of Σ .

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

Definitions:

1. A parallelism P is called regular if every spread of P is regular.
2. A partial parallelism with deficiency d is a set of $(q^2 + q + 1) - d$ disjoint spreads.

Regular parallelisms

There are regular parallelisms of $PG(3, 2)$, $PG(3, 5)$ and $PG(3, 8)$. They are cyclic and there are only two non-equivalent classes for each $q = 2, 5, 8$. On the other hand, there are no regular parallelisms of neither $PG(3, 3)$ nor $PG(3, 4)$.

Penttila and Williams constructed an infinite class of non-isomorphic cyclic regular parallelisms, two per each $q \equiv 2 \pmod{3}$. These classes include all the cyclic regular parallelisms mentioned above.

Partial parallelisms with deficiency one

If P^- is a partial parallelism with deficiency one, then it can always be completed to a parallelism.

There is a conjecture saying that if every spread in a partial parallelism with deficiency one is regular, then the unknown spread must also be regular.

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

Results on regular partial parallelisms with deficiency one

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.

Proof We take ℓ and m to be lines of S .

$$1 = \chi_{L^*} = \chi_{S \setminus \{\ell\}} + \sum_{i=1}^{q^2+q} \chi_{S_i \setminus R_i}$$

where R_i is a regulus in S_i such that ℓ is in its opposite regulus.

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.

Proof In page 28 we learned that 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 $(q - 1)/2$.