Value sets of special polynomials and blocking sets

Tamás Szőnyi

Eötvös Loránd University and MTA-ELTE GAC Research Group
Budapest

29th June, 2016
PhD Summer School in Discrete Mathematics, Rogla

This talk is based on joint work with HÉGER, DE BEULE, VAN DE VOORDE.

Details can be found in the paper:

Blocking and double blocking sets in finite planes, *Electronic Journal of Combinatorics* **23** (2016) P 2.5. (online)

More results on value sets of polynomials and related material can be found in

G. Mullen, D. Panario, *Handbook of finite fields*, CRC Press, 2013, in particular **Section 8** and more specifically 8.3 written by G. MULLEN, M. ZIEVE.

Special thanks are due to TAMÁS HÉGER who drew the figures.

Tamás Héger

Value sets of polynomials

Definition

If $f(x) \in \mathrm{GF}(q)[x]$, then $V(f) = \{f(x) : x \in \mathrm{GF}(q)\}$.

This is related to e.g. the direction problem, permutation polynomials etc.
What do we know about $|V(f)|$?
Of course, $|V(f)| = q$ is possible: permutation polynomials.
But there are no "almost Permutation polynomials" of small degree.

Theorem (Wan, 1993)

If f is not a permutation polynomial, then $|V(f)| \leq q - \frac{q-1}{n}$, where $n = \deg(f)$. where

On the other hand, it is trivial that $|V(f)| \geq q/n$, where $n = \deg(f)$.

Some illustrative results

Theorem (Chou, Gómez-Calderón, Madden 1988–1992)

If $f(x))$ is a monic pol. of deg. $n > 15$, $n^4 < q$ and $|V(f)| < 2q/n$, then

- $f(x) = (x+a)^n + b$, *where* $n|q-1$;
- $f(x) = ((x+a)^{n/2} + b)^2 + c$, *where* $n|q^2-1$;
- $f(x) = ((x+a)^2 + b)^{n/2} + c$, *where* $n|q^2-1$.

If we fix n and q is large then most polynomials take roughly $e_n q$ values, where $e_n = \sum_{j=1}^{n}(-1)^{j-1}/j!)$ (so roughly $(1-1/e)q$ values). The remainder term is $a_n\sqrt{q}$.

Theorem (A. Biró, 2000)

If $|V(f)| = 2$, $\deg(f) < \frac{3}{4}(p-1)$, p prime, then f is a polynomial in $x^{(p-1)/d}$, for some $d = 2, 3$.

This was motivated by some questions of A. GÁCS about Rédei type blocking sets.

Assume that $(f(x)-f(y))/(x-y)$ is absolutely irreducible. A consequence of Weil's theorem gives a lower bound if $n=\deg(f)<\sqrt{q}$. The Stöhr-Voloch bound gives an improvement for larger n, in particular, when $q=p$ is a prime.

Theorem (Uchiyama 1955; Voloch 1989)

$|V(f)| \geq \max(\frac{1}{2}q - \frac{1}{4}(n-3)(n-2)(q^{1/2}+1), q/n)$.
For q prime $|V(f)| \geq \frac{1}{4}(q/n-1)^{4/3}$, $q^{1/4}<n<q$.

Value sets of special polynomials

Theorem (Cusick, Müller, 1996)

Let $q = s^h$ and $f(x) = (x+1)x^{s-1}$. Then $|V(f)| = q - q/s$.

This means that the above bound by WAN is essentially sharp. CUSICK and later ROSENDAHL studied value sets of polynomials of the form

$$s_a(x) = x^a(x+1)^{\sqrt{q}-1}$$

if q is a square, or more generally if $\mathrm{GF}(q) \subset \mathrm{GF}(q^h)$, then

$$s_a(x) = x^a(x+1)^{q-1}.$$

Here $0^{-a} = 0$. It is clearly a natural modification/generalization of the above polynomial.

Some results by Cusick and Rosendahl

Theorem (Cusick, Müller, 1996)

With the previous notation $|V(s_1)| = (1 - 1/q)q^h$.

Theorem (Rosendahl, 2008/9)

If $q \equiv 0 \pmod 3$, $h = 2$, *then*

$$|V(s_3)| = \frac{2}{3}q^2 - \frac{1}{6}q - \frac{1}{2}.$$

They also studied, for q even, the value sets of s_{-1}. Their results follow from ours, so we do not state them in detail. Our results will be given later.

Blocking sets

Definition

A *blocking set* in Π_q is a set of points that intersects each line. It is called *non-trivial* if it contains no line. *Minimality* is w.r.t. inclusion.

Geometrically a minimal blocking set has a *tangent line* at each point. Such a point is *essential*.

Theorem

For a blocking set B in Π_q we have $|B| \geq q+1$. In case of equality B is a line.

Theorem (Bruen 1970–71)

For a minimal blocking set B in Π_q we have $|B| \geq q+\sqrt{q}+1$. In case of equality B is a Baer subplane (spl. of order $\sqrt{q}$).

Results for Galois planes: blocking sets

Theorem (Jamison 1977, Brouwer–Schrijver, 1978)

A blocking set of $\mathrm{AG}(2,q)$ *has at least* $2q-1$ *points.*

A blocking set S of $\mathrm{PG}(2,q)$) is small if $|S| < \frac{3}{2}(q+1)$.

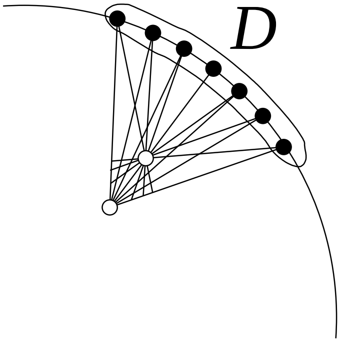
Theorem (Blokhuis 1994; Sziklai 2008; SzT 1997)

Each line meets a small minimal blocking set of $\mathrm{PG}(2,q)$ *in 1 modulo p points, where* $q = p^h$*. In particular, for* $q = p$*,* p *prime small minimal blocking sets are lines. If a line meets a blocking set in* $p+1$ *points, then it meets it in a subline.*

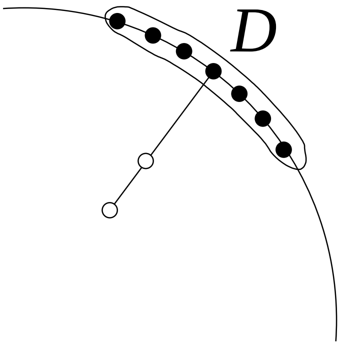
Non-desarguesian planes: Hall planes

The easiest definition of the Hall-plane is by *derivation*. Take the affine plane $\mathrm{AG}(2, q)$ and a Baer subline on the line at infinity. Replace those affine lines by Baer-subplanes whose point at infinity belongs to the Baer subline (*derivation set*). They are replaced by Baer subplanes containing the derivation set D.
More explicitly the points of the (affine) Hall plane are the points of the Galois plane, that is (x, y), $x, y \in \mathrm{GF}(q^2)$, and the lines with equation $y = mx + b$ with $m \notin \mathrm{GF}(q)$ remain the same ("old lines"), the "new lines" are the Baer subplanes of the form $\{(\lambda u + a, \lambda v + b)\}$, where $a, b \in \mathrm{GF}(q^2)$, λ runs through the multiplicative cosets of $\mathrm{GF}(q)^*$ in $\mathrm{GF}(q^2)^*$.
In this case the derivation set D is $\{(0), (\infty), (m) : m \in \mathrm{GF}(q)\}$.
A different transformation technique to obtain the Hall plane was introduced by P. QUATTROCCHI, ROSATI.

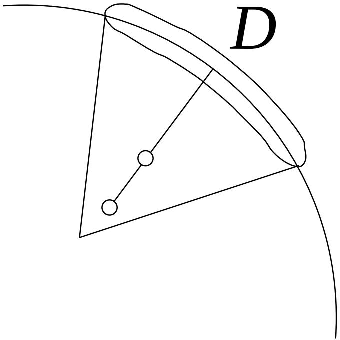
Derivation in figures I



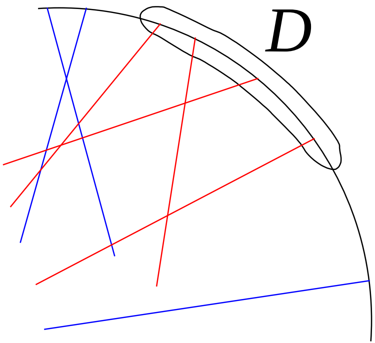
Derivation in figures II



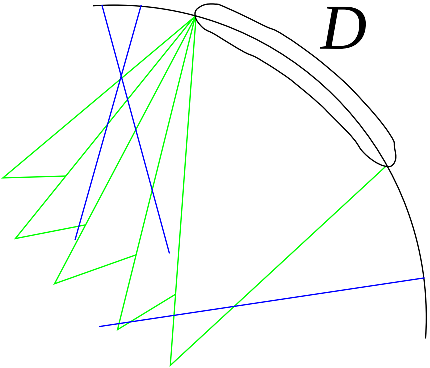
Derivation in figures III



Derivation in figures IV



Derivation in figures V



Other non-desarguesian planes: André planes

This is a generalization of Hall planes, in two sense. First, fields of order q^n are considered. Also for defining a new multiplication more general partitions are considered than in case of Moulton planes.
So, addition remains the same and for the multiplication we partition $\mathrm{GF}(q) = U_0 \cup U_1 \ldots U_{n-1}$. The new multiplication will be $a \circ b = ab^{q^i}$, if $\mathrm{N}(a) \in U_i$. One also assumes that $0, 1 \in U_0$. Here $\mathrm{N}(x) = x^{1+q+\ldots+q^{n-1}}$.
Note that in the Hall case $n = 2$ and $|U_1| = 1$ but the derivation set is $\{(m) : \mathrm{N}(m) = u_1\}$, where $U_1 = \{u_1\}$.
They can be obtained from Galois planes by multiple derivation.

Geertrui Van de Voorde

Blocking sets in the Hall plane

Theorem (De Beule, Héger, Van de Voorde, SzT, 2016)

Let $q^2 \geq 9$ be a square prime power. Then in the Hall plane of order q^2 there is a minimal blocking set of size $q^2 + 2q + 2$ admitting 1-, 2-, 3-, 4-, $(q+1)$- and $(q+2)$-secants.

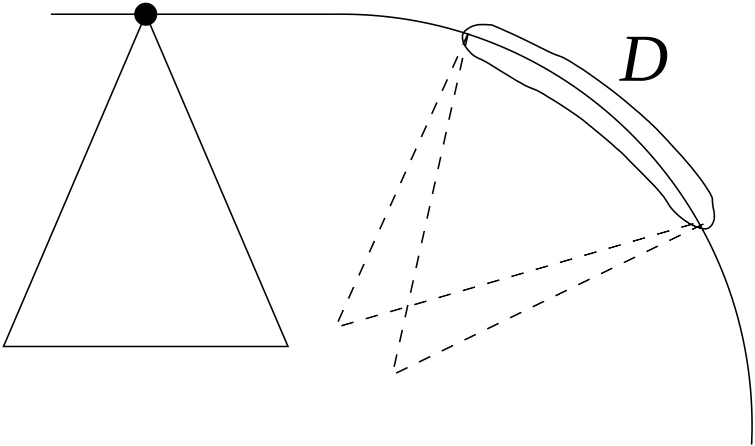
Theorem (De Beule, Héger, Van de Voorde, SzT, 2016)

Let $q^2 \geq 9$ be a square prime power. Then there exists an affine plane of order q^2 in which there is a blocking set of size $\lfloor 4q^2/3 + 5q/3 \rfloor$.

There was a counterexample known to the JAMISON, BROUWER-SCHRIJVER thm. for the translation plane of order $q = 9$: BRUEN-DE RESMINI. All planes of order 9: BIERBRAUER.

Jan De Beule

A figure showing the small blocking set in the Hall plane



JAN DE BEULE, TAMÁS HÉGER, GEERTRUI VAN DE VOORDE, SZT:

Take the Baer subplane B that has one infinite point not contained in the derivation set D. The clearly, $B \cup D$ is a blocking set of size $q + 2\sqrt{q} + 2$. Is it minimal? If we start from two disjoint Baer spls, then at least one point of D is necessay.

If the 1 modulo p result was true (and $q = p$ prime), then exactly one point of D can be deleted.

So our aim is to show that this is not possible, more generally the points of D are similar in their combinatorial properties (1 or 3 orbits).

Also results on the intersection of Baer subplanes can be used.

Intersections of Baer subplanes

BOSE, FREEMAN, GLYNN: general results on the intersections of two Baer subplanes in a plane Π_q, e.g. number of common points = number of common lines. For Galois planes:

Theorem (Bose, Freeman, Glynn, 1980)

In $\mathrm{PG}(2, q^2)$ two Baer subplanes intersect either in at most two points, three non-collinear points, a line of the Baer subplane, or a line and a point. (Actually, also the structure of common lines is determined simultaneously.)

This immediately implies that the subplane B and another subplane containing the derivation set D intersect in at most 3 (affine) points. If the intersection has 3 collinear points then it contains the Baer subline containig them.

Different ideal points in the Hall plane

A Baer subplane can be considered as $\{(x, x^q, 1)\}$ and its determined directions (i.e. $\{1, m, 0) : m^{q+1} = 1\}$). Put this in a different position to get the Baer subplane B_0 as the set $\{(u, 1, u^q)\}$ together with the determined directions on $y = 0$.
Take a new line (Baer spl), $L = \{x, mx^q + b, 1)\}$ with $\mathrm{N}(m)$ fixed (=1). To get $L \cap B$ we need to solve

$$(1/u)^q = m(1/u)^{q(q-1))} + b,$$

where $u^{q(q-1)} = u^{1-q}$. This gives $1 = mu^{2q-1} + bu^q$. Write $u = \lambda v$, then we get an equation with $m' = m\lambda^{2q-1}$, $b' = b\lambda^q$:

$$v^{q-1} = m'(1/v)^q + b',$$

and this has clearly as many sol'ns as the one above. Here we need $\lambda^{q+1} = 1$ and the fact that $(2q - 1, q + 1)$ =1 or 3 makes the differencee between $q \equiv 2 \pmod 3$, and q being not 2 mod 3. This indicates that the results will be different in these two cases.

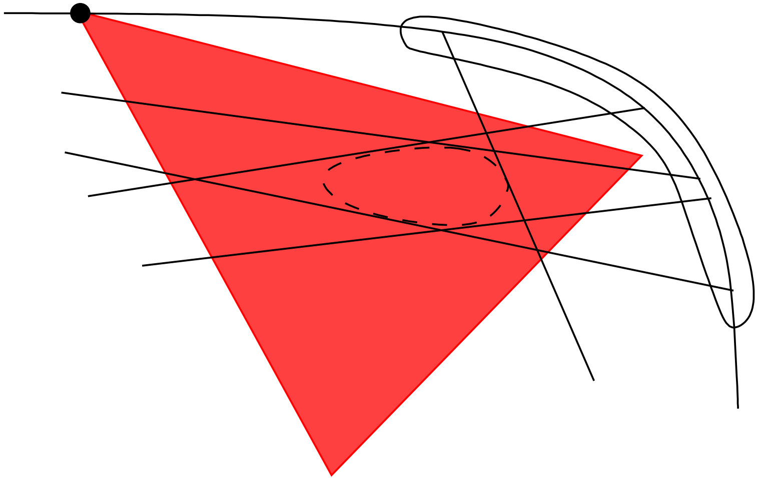
Lines through points of D and consequences

Consider the lines of B through the pts of D. There is one for each $d \in D$. In B they form a dual oval $\mathcal{O}$ (no 3 are collin.) So the pts of B are of 3 types:

pts on no line of $\mathcal{O}$: O^-,
points on two lines of $\mathcal{O}$: O^+,
points on one line of $\mathcal{O}$: O.

The sizes of O, O^+, O^- can easily be determined. The new lines through a point just cover the points on these 2,0, or 1 line inside B, and from this the possible intersection sizes can be determined: For example, when $P \in O^+$, then $q-1$ new lines meet B in three points of O^+ (incl. P) and two new lines meet in two points (a pt of O and P itself). From this the number of secants van basically be determined.

A figure illustrating $\mathcal{O}$



The previous considerations allow us to compute the number of 0-secants through affine and infinite points.

Lemma (De Beule, Héger, Van de Voorde, SzT, 2016)

Let B be our misplaced Baer spl., Q be an ideal pt (of new lines) in the Hall plane, and denote by $t_i(Q)$, the number os i-secants through Q. Then for q being not 2 mod 3 we have $t_0(Q) = (q^2 - q)/3$. If q is 2 mod 3, then there are $(q+1)/3$ points with $t_0(Q) = (q^2 - q - 2)/3$ and $2(q+1)/3$ points with $t_0(Q) = (q^2 - q + 1)/3$.

The other $t_i(Q)$'s can also be computed essentially.

A by-product for value sets

We can relate the size of $|V(s_{-1})|$ and the number of 0-secants of our set B_0 and obtain the size of the value set exactly.

Theorem (De Beule, Héger, Van de Voorde, SzT, 2016)

For q odd, $h = 2$, the value set $|V(s_{-1})|$ has size $\frac{2}{3}q^2 - \frac{1}{6}q - \frac{1}{2}$, if q is not 3 modulo 3, and the last $-\frac{1}{2}$ is replaced by $+\frac{1}{6}$ if q is 2 modulo 3.

Our proof also works for q even, where the results were obtained before by CUSICK and ROSENDAHL. We have fixed a minor mistake in Rosendahl's result.

A by-product on double blocking sets

Theorem (De Beule, Héger, Van de Voorde, 2016)

In $\mathrm{PG}(2, p^h)$ *for any (small) blocking set* B *of size at most* $\frac{3}{2}(p^h - p^{h-1}$ *there is a disjoint blocking set of size* $p^h + p^{h-1} + 1$.

As a corollary, we get that there are two disjoint blocking sets of size $p^h + p^{h-1} + 1$. This is the smallest known double blocking set e.g. for $h = 3$, and one might conjecture it is the smallest one.

What was known for double blocking sets?

POLVERINO-STORME: two disjoint blocking sets if $p \equiv 2 \pmod 7$

VAN DE VOORDE (PhD thesis): if a small blocking set meets every linear blocking set, then it must be a line

Difficulty of explicit constructions:
BLOKHUIS-BALL-BROUWER-STORME-SZT: if two small blocking sets of Rédei type have a common Rédei line, then they cannot be disjoint.
Relatively recent result in BACSÓ, HÉGER, SzT: in PG$(2, p^h)$ there are two disjoint blocking sets of size $(p^h + p^{h-1} + \ldots + p + 1$.

Thank you for your attention!