Note di Matematica **26,** n. 1, 2006, 121–130.

Directions in $AG(3,p)$ and their applications

Peter Sziklai[i]
Eötvös University Budapest, Pázmány P. s. 1/c,
Budapest, Hungary H-1117
sziklai@cs.elte.hu

Received: 6/4/2005; accepted: 19/5/2005.

Abstract. There is a still growing theory of Rédei type blocking sets and their applications, also of the set of directions determined by the graph of a function. Here we prove a theorem about the number of directions determined by a pointset of size p^2 in $AG(3,p)$, where p is prime. Then two results, which are applications of the planar theorem, are generalized using the new theorem.

Keywords: direction, Rédei

MSC 2000 classification: 05B25

1 Introduction

There is a still growing theory of Rédei type blocking sets and their applications, also of the set of directions determined by the graph of a function or, (as over a finite field every function is) a polynomial, the intimate connection of these two topics is obvious. Here we prove a theorem about the number of directions determined by a pointset of size p^2 in $AG(3,p)$, where p is prime. Then two results, which are applications of the planar theorem, are generalized using the new theorem.

Throughout this paper everything is finite and the common terminology is used. $AG(n,q)$ and $PG(n,q)$ denote the affine and the projective space of n dimension over the Galois field $GF(q)$ where $q = p^t$ is a power of the prime $p > 2$. We imagine $PG(n,q)$ as the union of $AG(n,q)$ and the 'hyperplane at infinity' H_∞. A *blocking set* B is a set of points intersecting every line, it is called *trivial* if it contains a hyperplane. A point $b \in B$ is *essential* if $B \setminus \{ b \}$ is no more a blocking set (so there is a line l intersecting B in b only, such a line can be called a *tangent*); B is *minimal* if all its points are essential.

1 Definition. We say that a set of points $U \subset AG(n,q)$ *determines the direction* $h \in H_\infty$, if there is an affine line through h meeting U in at least two

[i]Research was partially supported by OTKA D32817, F030737, F043772, T043758, T049662, FKFP0063/2001, Eötvös and Magyary grants.

points. We will always suppose that $|U| = q^{n-1}$. Denote by D the set of determined directions. Finally, let $N = |D|$, the number of determined directions.

The following proposition shows how this becomes an algebraic problem:

2 Proposition. *(i) If $|U| = q^{n-1}$ does not determine all directions (i.e. if $N < \theta_{n-1}$), then it can be taken as the graph of a polynomial (in $n-1$ variables).*

(ii) Suppose that we are in 2 dimensions and $U \subset AG(2,q)$ is the graph of the polynomial f. Then $D = \{ \frac{f(x)-f(y)}{x-y} : x \neq y \}$. QED

Now we show the connection between directions and blocking sets:

3 Proposition. *U together with infinite points corresponding to directions in D form a blocking set in $PG(n,q)$, which is minimal subject to inclusion (provided $N < |H_\infty|$).*

Proof. Let $h \in H_\infty$. The affine lines through h are all blocked by U if and only if they are all tangents, i.e. if h is not a determined direction. This means that if we want to complete U to a blocking set in $PG(n,q)$ by adding infinite points then we have to take the points in D. The points of U are all necessary, since $N < |H_\infty|$ implies that there exists an infinite point through which the affine lines are blocked by different points of U. This argument also shows that, as there is at least one tangent line through any point of D, all points of D are essential.

Any infinite line $l \subset H_\infty$ is blocked by D: there are q^{n-2} (disjoint) affine planes through l, and in any of them, which has at least two points in U, a determined direction of $D \cap l$ is found. QED

The blocking set B arising this way has the property to meet a hyperplane in $|B| - q^{n-1}$ points. On the other hand, if a blocking set meets a hyperplane in $|B| - q^{n-1}$ points then, after deleting this hyperplane, we find a set of points in the affine space determining $|B| - q^{n-1}$ directions, so the following notion is more or less equivalent to a pointset plus its directions: a blocking set B is of *Rédei type* if it meets a hyperplane in $|B| - q^{n-1}$ points. We remark that the theory developed by Rédei in his book [10] is highly related to these blocking sets, see [3]. For high-dimensional blocking sets of Rédei type we refer to [11]. Blocking sets of Rédei type are in a sense extremal examples, as for any (non-trivial) blocking set B and hyperplane H, $|B \setminus H| \geq q^{n-1}$ holds.

Now if U determines all directions then it yields a trivial blocking set: it contains the hyperplane at infinity; so we will be interested in the case when U determines at most $|H_\infty| - 1$ directions. Since the arising blocking set has size $q^{n-1} + N$, to find small blocking sets we will have to find and classify sets determining a small number of directions.

A strong motivation for the investigations can be, that in the planar case, A. Blokhuis, S. Ball, A. Brouwer, L. Storme and T. Szőnyi classified blocking sets of Rédei type, with size $< q + \frac{q+3}{2}$, almost completely [4].

In this paper we will use the "direction" terminology, but all results can be translated to results about Rédei type blocking sets. In section 2 we recall the classical results about the $q = p =$ prime case and some well-known applications are collected as well. In section 3 the analogue of the planar result is proven for $AG(3,p)$, where p is a prime. Finally the generalizations of two planar applications are given in section 4.

2 Classical results and examples

The first result is due to Rédei and Megyesi [10] and was later found independently by A. W. M. Dress, M. H. Klin and M. E. Muzichuk [6]:

4 Result. A set of p points in $AG(2,p)$, which is not a line, determines at least $\frac{p+3}{2}$ directions. QED

This is part of the theorem Rédei proves in his book using the results about lacunary polynomials. The first ones to find a simple proof were Lovász and Schrijver [8], who could also describe the case of equality:

5 Result. A set of p points in $AG(2,p)$ $(p > 2)$ determines $\frac{p+3}{2}$ directions if and only if it is affine equivalent to the graph of the polynomial $x^{\frac{p+1}{2}}$. QED

In section 3 we will prove the three dimensional version of this result (Proposition 11, Theorem 15). As the blocking set in this theorem (called *the projective triangle* by some authors) is a very important one, we give here another natural form of it:

$$B_\triangle = U_\triangle \cup D_\triangle =$$
$$\{\,(0,0,1);\ (0,1,0);\ (1,0,0);\ (a^2,0,1);\ (0,a^2,1)\ (-a^2,1,0) : a \in GF(p)^*\,\}.$$

Sometimes, for brevity, we will call the affine part of this configuration, i.e. the affine transform of the graph of $f(x) = x^{\frac{p+1}{2}}$, so those p points lying on two lines, also (the affine part of) a projective triangle, which is (a convenient) abuse of language.

Recently A. Gács could essentially improve these results, proving

6 Result ([7])**.** Let U be a set of points in $AG(2,p)$, p prime. Then one of the following holds:

(i) U is a line determining one direction;

(ii) U is affinely equivalent to the projective triangle determining $\frac{p+3}{2}$ directions; or

(iii) U determines at least $\frac{2}{3}(p-1)+1$ directions.

We enlist here some algebraic applications of the Rédei-Megyesi theorem. They can be found in the nice survey paper of Szőnyi [13]. Many other applications in finite geometry can be found in Blokhuis [3].

First a theorem from the Hajós theory of Abelian groups.

7 Result ([8])**.** Let $G = C_p \times C_p$. Suppose $G = A + B$ is a normal factorization of it, i.e. $(0,0) \in A, B$ and every $g \in G$ can be written in the form $g = a+b, a \in A, b \in B$ in a unique way. Then A or B is a subgroup of G. QED

The next result is due to Rédei.

8 Result ([10])**.** Let $G = C_p \times C_p$, and $H_1, \ldots, H_k \leq G$ subgroups of size $|H_i| = p$. Suppose that $R \subset G$ is a common representing system, i.e. (i) $(0,0) \in R$; (ii) $|R| = p$; (iii) $R + H_i = G$ for $i = 1, \ldots, k$.

Suppose also that R is not a subgroup (which would be the 'trivial' case). Then $k \leq \frac{p-1}{2}$. If $k = \frac{p-1}{2}$ then R is the subset in Result 5 and the H_i subgroups are the sets $\{ (x, mx) \}$ where m is a direction not determined by R (after changing the two C_p factors of G if needed). QED

The third result was first proved by Wielandt in a very complicated way. Then Blokhuis and Seidel [5] realized that it is a direct consequence of Rédei's theorem.

9 Result (Wielandt's visibility theorem)**.** Let G be a permutation group on the points of $AG(2,p)$. Suppose that G contains all translations. Let G_0 be the stabilizer of the origin. Let S be the set of k lines through the origin, $1 \leq k \leq \frac{p+1}{2}$. If G_0 maps the set of points in S onto itself then every $g \in G_0$ maps the lines in S to lines in S.

The following application is also a group theoretical one. Dress, Klin and Muzichuk [6], and, independently, Ott [9] noted that the famous theorem of Burnside can be proved using Rédei's theorem.

10 Result (Burnside)**.** Let G be a transitive permutation group of degree p. Then either G is doubly transitive or G is isomorphic to a subgroup of the affine transformations of form $x \mapsto ax + b$ $(a \neq 0, a, b \in GF(p))$. QED

In section 4 we will generalize Results 8 and 9.

3 Directions in $AG(3,p)$

First we prove the 3–dimensional analogue of the theorems of Rédei and Lovász-Schrijver:

11 Proposition. *Let $U \subset AG(3,p)$ be a pointset of size $|U| = p^2$, $p > 3$. Then for the number $N = |D|$ of determined directions one of the following possibilities holds:*

(i) U is a plane and $N = p + 1$;

(ii) U is a cylinder with the (affine part of the) projective triangle as a base, and $N = 1 + p\frac{p+3}{2}$;

(iii) $N \geq p + p\frac{p+3}{2}$.

12 Remark. If $p = 2$ then a set of 4 points is either coplanar and determines 3 directions, or the points are in general position and determine 6 directions.

If $p = 3$ then a set of 9 points can determine 11 directions (which would be forbidden by the bounds above) as the following example shows: let $P_1, P_2, \ldots, P_9$ be the points of an affine plane in $AG(3,3)$, such that P_7, P_8, P_9 are collinear, and Q_1, Q_2 be two points out of this plane, such that P_7, Q_1, Q_2 are collinear. Then the set

$$\{\, P_1, P_2, \ldots, P_7, Q_1, Q_2 \,\}$$

determines 11 directions. (If S is the infinite point of P_8P_9 and T is the infinite point of Q_1Q_2 then from the four points of the line ST only S and T are determined.) Note that this example is unique up to affine transformation.

The proof below shows that except for this example the theorem holds for $p = 3$ as well, so 9 points in $AG(3,3)$ determine either 4 directions (and then U is a plane), or 10 directions (U is the 'lifted' projective triangle), or 11 directions (the configuration above), or at least 12 directions.

Proof. Suppose $N < \frac{p+5}{2}p$. Then D can not form a $\frac{p+3}{2}$–fold blocking set in the infinite plane H_∞, see [1]. So there exists a line $\ell \subset H_\infty$ such that $|l \cap D| < \frac{p+3}{2}$. It means that for any affine plane S through ℓ the points $U \cap S$ determine less than $\frac{p+3}{2}$ directions, so at most one. Hence each of these planes contain at most p points, so (as there are p affine planes through ℓ) exactly p points, and in each of these planes, by Lovász-Schrijver, they form a line. If two of these lines were skew then their $2p$ points would determine $p^2 + 2$ directions, (they do not determine the $p - 1$ points on the infinite line joining the infinite points of l_1 and l_2, but not on either of them), a contradiction if $p > 3$. Hence all these lines are concurrent in an infinite point C ($\in \ell$) and U is cylindric.

Let S_0 be an affine plane not through C, $U_0 := U \cap S_0$, and denote by N_0 the number of directions determined by U_0 in S_0. (N.B. $|U_0| = p$.) Then $N = 1 + pN_0$. So either $N = 1 + p$ and U_0 is collinear so U is coplanar; or $N = 1 + p\frac{p+3}{2}$ and U_0 is the projective triangle and we are in *(ii)*; or $N_0 \geq \frac{p+5}{2}$ contradicting $N < \frac{p+5}{2}p$. QED

This bound can be improved, using the quoted Result 6 of A. Gács [7]. The following lemma, that can be proved by elementary calculations, will also help.

13 Lemma. *If one fixes the set of determined directions of the projective triangle $U_\Delta \subset AG(2,p)$ then any other pointset determining exactly the same directions is of form*

$$U = \{\, (cx^2 + a, b, 1);\ (a, cx^2 + b, 1) \ :\ x \in GF(p) \,\}.$$

QED

We shall intensively use the following result as well.

14 Lemma ([14])**.** *Let $f_1, \ldots, f_m \in GF(q)[x]$ be given polynomials, suppose that no partial product $f_{i_1} f_{i_2} \cdots f_{i_j}, 1 \leq i_1 < i_2 < \cdots < i_j \leq m$ can be written as a constant multiple of a square of a polynomial. If $2^{m-1} \sum_{i=1}^m \deg(f_i) \leq \sqrt{q} - 1$ then there is an $x_0 \in GF(q)$ such that $f_i(x_0)$ is a non-square for every $i = 1, \ldots, m$. More precisely, if we denote the number of these x_0-s by N then*

$$|N - q/2^m| \leq \sum_{i=1}^{m} \deg(f_i) \frac{\sqrt{q} + 1}{2}.$$

QED

This lemma says that "being a square (or a non-square) element of GF(q)" is a random event with probability 1/2, and the "error term" of this statement is $\sum_{i=1}^m \deg(f_i)\frac{\sqrt{q}+1}{2}$. This result was generalized in [12] for other powers in GF(q).

Now

15 Theorem. *Let $U \subset AG(3,p)$ be a pointset of size $|U| = p^2$, $p > 11$. Then for the number $N = |D|$ of determined directions one of the following possibilities holds:*

(i) U is a plane and $N = p + 1$;

(ii) U is a cylinder with the projective triangle as a base, and $N = 1 + p\frac{p+3}{2}$;

(iii) $N \geq \frac{2}{3}(p-1)p + 2p$.

Proof. The proof is similar to the previous one, but it is a bit longer. If $N < p(\frac{2}{3}(p-1) + 2)$ then on the infinite plane the directions cannot form

a $\frac{2}{3}(p-1)+1$-fold blocking set. So we have a pencil of parallel affine planes through an infinite line ℓ, each containing p points of U determining less than $\frac{2}{3}(p-1)+1$ directions on ℓ. Hence the pointsets in the planes can be affine lines or projective triangles. Note that if there are at least two projective triangles then their set of infinite points (the directions) must coincide, otherwise by Lemma 14, $|D \cap \ell| \geq \frac{3}{4}p$.

If there are lines only then the previous proof goes through. Suppose that there is a projective triangle and at least $\frac{p+1}{2}$ lines then the lines should be parallel (see the proof above). Let l_1 and l_2 be two of the parallel lines and the (affine part of the) projective triangle $T \subset m_1 \cup m_2$, where m_1 and m_2 are affine lines. After a suitable affine transformation one may assume that $T = (T \cap m_2) \cup (T \cap m_1) = \{\, (x^2,0,0,1);\, (0,x^2,0,1) : x \in GF(p) \,\}$; $l_1 = \{\, (x, ax+b_1, c_1, 1) : x \in GF(p) \,\}$; $l_2 = \{\, (x, ax+b_2, c_2, 1) : x \in GF(p) \,\}$. Then the direction $(u,v,1,0)$ is determined by l_1 and $T \cap m_1$ if the equations $\frac{x_1}{c_1} = u$ and $\frac{ax_1+b_1-y_1^2}{c_1} = v$ have a solution (x_1,y_1), so if $c_1(au-v)+b_1$ is a square element in $GF(p)$. It happens for roughly the half of the possible (u,v) pairs. The similar condition for l_2 and $T \cap m_1$ is that $c_2(au-v)+b_2$ should be a square element, and these two conditions are dependent iff $b_2 = \frac{c_2}{c_1}b_1$. If this is not the case then l_1, l_2 and $T \cap m_1$ already determine roughly $\frac{3}{4}p^2$ directions. If they are dependent and $\frac{c_2}{c_1}$ is a non-square element, then l_1, l_2 and $T \cap m_1$ already determine roughly p^2 directions. But, as there are at least $\frac{p+1}{2}$ lines, there exists at least a pair of them for which $\frac{c_2}{c_1}$ is a non-square.

Finally suppose that there are at least $\frac{p+1}{2}$ projective triangles, not all in a cylinder. After a suitable linear transformation they are of form

$$T_i = \{\, (w_i x^2 + a_i, b_i, d_i, 1);\, (a_i, w_i x^2 + b_i, d_i, 1) : x \in GF(p) \,\}.$$

Then T_i and T_j determine the following directions:

$$\begin{aligned}\{\, &(x, b_j-b_i, d_j-d_i, 0), (a_j-a_i, x, d_j-d_i, 0),\\ &(a_j-a_i+w_jx^2, b_j-b_i-w_iy^2, d_j-d_i, 0),\\ &(a_j-a_i-w_iy^2, b_j-b_i+w_jx^2, d_j-d_i, 0) : x,y \in GF(p) \,\}.\end{aligned}$$

This set has cardinality $2p-1+\frac{(p-1)^2}{2}$ or $2p-1+\frac{(p-1)^2}{4}$ according as $-w_j/w_i$ is a non-square or a square.

Now if -1 is a non-square then there are many pairs (i,j) for which $-w_j/w_i$ is a non-square and we are done. If -1 is a square and there exists a w_i which is non-square then we are in a similarly easy situation. (Alternatively, one can prove the last two sentences in the manner of what follows.) So suppose that

-1 and all the elements w_i are squares. From Lemma 13 we can assume that $\forall i\ w_i = 1$ so we have

$$T_i = \{\, (x^2 + a_i, b_i, d_i, 1);\ (a_i, x^2 + b_i, d_i, 1) : x \in GF(p) \,\}$$

and T_i and T_j determine the following directions:

$$\{\, (x, b_j - b_i, d_j - d_i, 0), (a_j - a_i, x, d_j - d_i, 0),\\ (a_j - a_i + x^2, b_j - b_i + y^2, d_j - d_i, 0) : x, y \in GF(p) \,\}.$$

Suppose that we have at least four triangles in "general position" (so not in a cylinder), then from the exclusion-inclusion formula and Lemma 14 (we have to use it for some linear polynomials of form $(d_j - d_i)u - (a_j - a_i)$ and $(d_j - d_i)v - (b_j - b_i)$) we get that they determine at least

$$\geq \binom{4}{1}\left(\frac{p-1}{2}\right)^2 - \binom{4}{2}\left(\frac{p}{4} + \sqrt{p} + 1\right)^2 + \\ \binom{4}{3}\left(\frac{p}{8} - \frac{3}{2}(\sqrt{p}+1)\right)^2 - \binom{4}{4}\left(\frac{p}{16} + (2\,(\sqrt{p}+1))\right)^2 > \frac{2}{3}p^2,$$

a contradiction again. QED

The next proposition shows that D should have an interesting structure:

16 Proposition. *D is the union of some lines.*

Proof. Let $d \in D$ be a direction determined by U. It means that there exists an affine line ℓ such that $\ell \cap H_\infty = d$ and $|l \cap U| \geq 2$. By the pigeon hole principle there exists an affine plane through ℓ containing at least

$$|l \cap U| + \lceil \frac{p^2 - |l \cap U|}{p+1} \rceil = |l \cap U| + p - 1 \geq p + 1$$

points, so in that plane they determine all directions. Hence in H_∞ for any $d \in D$ there exists a line l_d such that $d \in l_d \subset D$. QED

4 Applications

Here we generalize two results in Section 2 using Theorem 15 (or Proposition 11) as we promised.

17 Theorem. *Let $G = C_p \times C_p \times C_p$, and $H_1, \ldots, H_k \leq G$ subgroups of size $|H_i| = p$. Suppose that $R \subset G$ is a* common representing system*, i.e.*

- $(0, 0, 0) \in R$;

- $|R| = p^2$;
- $R + H_i = G$ *for* $i = 1, \ldots, k$.

Suppose also that R is not a subgroup (which would be the 'trivial' case). Then

$$k \leq p\frac{p-1}{2}.$$

If $k = p\frac{p-1}{2}$ then (after changing the three C_p factors of G if needed) R is the set U of Theorem 13.(ii) and the H_i subgroups are the lines through the origin, with slope not determined by R.

PROOF. If we identify G with $AG(3,p)$, the subgroups become subspaces through the origin. So the subgroups H_i are lines and R is representing with respect to H_i if and only if $r_1 - r_2 \notin H_i$, i.e. the directions determined by the points of R are different from the direction of H_i. If $k > p\frac{p-1}{2}$ then $p^2+p+1-k < 1+p\frac{p+3}{2}$, so there is no such (non-subgroup, i.e. non-planar) representing system.

If $k = p\frac{p-1}{2}$ then we are in *(ii)* of Theorem 14 and the description of R and the sets H_i is straightforward. QED

Our result helps us to generalize Wielandt's visibility theorem:

18 Theorem (Wielandt's visibility theorem in three dimensions)**.** *Let G be a permutation group on the points of $AG(3,p)$. Suppose that G contains all translations. Let G_0 be the stabilizer of the origin. Let S be the set of k planes through the origin, $1 \leq k \leq \frac{p+1}{2}$. If G_0 maps the set of points in S onto itself then every $g \in G_0$ maps the planes in S to planes in S.*

PROOF. We simply reconstruct the method of Blokhuis and Seidel. Let $g \in G_0$, and $\tau(u)$ be the translation by the vector $u \in AG(3,p)$. If $\pi \in S$, then for any two points $x, y \in \pi$ the direction determined by $g(x)$ and $g(y)$ is also a direction determined by the origin and a point of S as

$$\tau(-g(y))\ g\ \tau(y)\ (x-y) = g(x) - g(y) \in S,$$

because $\tau(-g(y))\ g\ \tau(y)$ stabilizes the origin. So the points $\{\, g(x) : x \in \pi \,\}$ determine at most $\frac{p+1}{2}(p+1) < 1+p\frac{p+3}{2}$ directions, so they are coplanar. QED

References

[1] S. BALL: *Multiple blocking sets and arcs in finite planes*, J. London Math. Soc. (2), **54**, (1996), 581–593.

[2] A. BEUTELSPACHER, F. EUGENI: *Blocking sets of a given index, with particular attention to index* 3 (in Italian, with English summary), Boll. Un. Mat. Ital. A (6), **4**, (1985), n. 3, 441–450.

[3] A. Blokhuis: *Blocking sets in Desarguesian planes*, Combinatorics: Paul Erdős is Eighty, Vol. 2, János Bolyai Mathematical Society, Budapest (1993), 133–155.

[4] A. Blokhuis, S. Ball, A. Brouwer, L. Storme, T. Szőnyi: *On the number of slopes determined by a function on a finite field*, J. Combin. Theory Ser. A, **86**, (1999), 187–196.

[5] A. Blokhuis, J. J. Seidel: *Remark on Wielandt's visibility theorem*, Lin. Alg. and its Appl., **71**, (1985), 29–30.

[6] A. W. M. Dress, M. H. Klin, M. E. Muzichuk: *On p-configurations with few slopes in the affine plane over F_p and a theorem of W. Burnside*, Bayreuther Math. Schriften, **40**, (1992), 7–19.

[7] A. Gács: *On a generalization of Rédei's theorem*, Combinatorica, **23**, (2003), 585–598.

[8] L. Lovász, A. Schrijver: *Remarks on a theorem of Rédei*, Studia Scient. Math. Hungar., **16**, (1981), 449–454.

[9] U. Ott: *Group association schemes and Schur rings*,Le Matematiche (Catania), **XLVII**, (1992), 281–294.

[10] L. Rédei: Lückenhafte Polynome über endlichen Körpern, Birkhäuser Verlag, Basel 1970. (English translation: Lacunary polynomials over finite fields, North Holland, Amsterdam 1973).

[11] L. Storme, P. Sziklai: *Linear pointsets and Rédei type k-blocking sets in $PG(n, q)$*, J. Alg. Comb., **14**, (2001), 221–228.

[12] P. Sziklai: *A lemma on the randomness of d-th powers in GF(q), $d|q-1$*, Bull. Belg. Math. Soc., **8**, (2001), 95–98.

[13] T. Szőnyi: *Some new applications of the Rédei theory of lacunary polynomials* (in Hungarian), Polygon, **V**, (1995), 49–78.

[14] T. Szőnyi: *Note on the existence of large minimal blocking sets in Galois planes*, Combinatorica, **12**, (1992), 227–235.