Journal of Algebraic Combinatorics **14** (2001), 221–228

Linear Point Sets and Rédei Type k-blocking Sets in $PG(n, q)$

L. STORME* ls@cage.rug.ac.be
Dept. of Pure Maths and Computer Algebra, Ghent University, Krijgslaan 281, 9000 Gent, Belgium

P. SZIKLAI† sziklai@cs.bme.hu
Technical University Budapest, Pázmány P. sétany 1/d, Budapest, Hungary, H-1117

Received June 21, 2000; Revised May 16, 2001

Abstract. In this paper, k-blocking sets in $PG(n, q)$, being of Rédei type, are investigated. A standard method to construct Rédei type k-blocking sets in $PG(n, q)$ is to construct a cone having as base a Rédei type k'-blocking set in a subspace of $PG(n, q)$. But also other Rédei type k-blocking sets in $PG(n, q)$, which are not cones, exist. We give in this article a condition on the parameters of a Rédei type k-blocking set of $PG(n, q = p^h)$, p a prime power, which guarantees that the Rédei type k-blocking set is a cone. This condition is sharp. We also show that small Rédei type k-blocking sets are linear.

Keywords: Rédei type k-blocking sets, directions of functions, linear point sets

1. Introduction

There is a continuously growing theory on Rédei type blocking sets and their applications, also on 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.

Throughout this paper $AG(n, q)$ and $PG(n, q)$ denote the affine and the projective space of n dimensions over the Galois field $GF(q)$ where $q = p^h$, p a prime power. We consider $PG(n, q)$ as the union of $AG(n, q)$ and the 'hyperplane at infinity' H_∞. A point set in $PG(n, q)$ is called *affine* if it lies in $AG(n, q)$, while a subspace of $PG(n, q)$ is called *affine* if it is not contained in H_∞. So in this sense an affine line has one infinite point on it. Let $\theta_n = |PG(n, q)|$.

A *k-blocking set* $B \subset PG(n, q)$ is a set of points intersecting every $(n-k)$-dimensional subspace, it is called *trivial* if it contains a k-dimensional subspace. A point $b \in B$ is *essential* if $B\setminus\{b\}$ is no longer a k-blocking set (so there is an $(n-k)$-subspace L intersecting B in b only, such an $(n-k)$-subspace can be called a *tangent*); B is *minimal* if all its points are essential. Note that for $n = 2$ and $k = 1$ we get the classical planar blocking sets.

*http://cage.rug.ac.be/~ls

†Research was partially supported by OTKA F030737, T 029255, D 32817 and Eötvös grants. The second author is also grateful for the hospitality of the Ghent University where this work was done.

Definition 1 We say that a set of points $U \subset AG(n,q)$ *determines the direction* $d \in H_\infty$, if there is an affine line through d meeting U in at least two points. Denote by D the set of determined directions. Finally, let $N = |D|$, the number of determined directions.

We will always suppose that $|U| = q^k$. Now we show the connection between directions and blocking sets:

Proposition 2 *If $U \subseteq AG(n,q)$, $|U| = q^k$, then U together with the infinite points corresponding to directions in D form a k-blocking set in $PG(n,q)$. If the set D does not form a k-blocking set in H_∞ then all the points of U are essential.*

Proof: Any infinite $(n-k)$-subspace $H_{n-k} \subset H_\infty$ is blocked by D: there are q^{k-1} (disjoint) affine $(n-k+1)$-spaces through H_{n-k}, and in any of them, which has at least two points in U, a determined direction of $D \cap H_{n-k}$ is found.

Let $H_{n-k-1} \subset H_\infty$ and consider the affine $(n-k)$-subspaces through it. If $D \cap H_{n-k-1} \neq \emptyset$ then they are all blocked. If H_{n-k-1} does not contain any point of D, then every affine $(n-k)$-subspace through it must contain exactly one point of U (as if one contained at least two then the direction determined by them would fall into $D \cap H_{n-k-1}$), so they are blocked again. So $U \cup D$ blocks all affine $(n-k)$-subspaces and all the points of U are essential when D does not form a k-blocking set in H_∞. □

Unfortunately in general it may happen that some points of D are non-essential. If D is not too big (i.e. $|D| \leq q^k$, similarly to planar blocking sets) then it is never the case.

Proposition 3 *If $|D| < \frac{q^{n-1}-1}{q^{n-k-1}-1}$, then all the points of D are essential.*

Proof: Take any point $P \in D$. The number of $(n-k-1)$-subspaces through P in H_∞ is $\frac{\theta_{n-2}\theta_{n-3}\ldots\theta_k}{\theta_{n-k-2}\theta_{n-k-3}\ldots\theta_1\cdot 1}$. Any other $Q \in D\backslash\{P\}$ blocks at most $\frac{\theta_{n-3}\ldots\theta_k}{\theta_{n-k-3}\ldots\theta_1\cdot 1}$ of them. So some affine $(n-k)$-subspace through one of those infinite $(n-k-1)$-subspaces containing P only, will be a tangent at P. □

The k-blocking set B arising in this way has the property that it meets a hyperplane in $|B| - q^k$ points. On the other hand, if a minimal k-blocking set of size $\leq 2q^k$ meets a hyperplane in $|B| - q^k$ points then, after deleting this hyperplane, we find a set of points in the affine space determining these $|B| - q^k$ directions, so the following notion is more or less equivalent to a point set plus its directions: a k-blocking set B is of *Rédei type* if it meets a hyperplane in $|B| - q^k$ points. We remark that the theory developed by Rédei in his book [4] is highly related to these blocking sets. Minimal k-blocking sets of Rédei type are in a sense extremal examples, as for any (non-trivial) minimal k-blocking set B and hyperplane H, where H intersects B in a set $H \cap B$ which is not a k-blocking set in H, $|B \backslash H| \geq q^k$ holds.

Since the arising k-blocking set has size $q^k + |D|$, in order to find small k-blocking sets we will have to look for sets determining a small number of directions.

Hence the main problem is to classify sets determining few directions, which is equivalent to classifying small k-blocking sets of Rédei type. A strong motivation for the investigations is, 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:

Result 4 [1] *Let $U \cup D$ be a minimal blocking set of Rédei type in $PG(2, q)$, $q = p^h$, $U \subset AG(2, q)$, $|U| = q$, D is the set of directions determined by U, $N = |D|$. Let e (with $0 \leq e \leq h$) be the largest integer such that each line with slope in D meets U in a multiple of p^e points. Then we have one of the following*:

(i) $e = 0$ *and* $(q + 3)/2 \leq N \leq q + 1$,
(ii) $e = 1$, $p = 2$, *and* $(q + 5)/3 \leq N \leq q - 1$,
(iii) $p^e > 2$, $e \mid h$, *and* $q/p^e + 1 \leq N \leq (q - 1)/(p^e - 1)$,
(iv) $e = h$ *and* $N = 1$.

Moreover, if $p^e > 3$ or ($p^e = 3$ and $N = q/3 + 1$), then U is a $GF(p^e)$-linear subspace, and all possibilities for N can be determined explicitly.

We call a *Rédei* k-blocking set B of $PG(n, q)$ *small* when $|B| \leq q^k + \frac{q+3}{2}q^{k-1} + q^{k-2} + q^{k-3} + \cdots + q$. These small Rédei k-blocking sets will be studied in detail in the next sections.

It is our goal to study the following problem. A small Rédei k-blocking set in $PG(n, q)$ can be obtained by constructing a cone with vertex a $(k - 2)$-dimensional subspace Π_{k-2} in $PG(n, q)$ and with base a small Rédei blocking set in a plane Π'_2 skew to Π_{k-2}.

However, these are not the only examples of small k-blocking sets in $PG(n, q)$. For instance, the subgeometry $PG(2k, q)$ of $PG(n = 2k, q^2)$ is a small k-blocking set of $PG(2k, q^2)$, and this is not a cone.

We give a condition (Theorem 16) on the parameters of the small Rédei k-blocking set in $PG(n, q)$ which guarantees that this small Rédei k-blocking set is a cone; so that the exact description of this k-blocking set is reduced to that of the base of the cone.

This condition is also sharp since the k-blocking set $PG(2k, q)$ in $PG(2k, q^2)$ can be used to show that the conditions imposed on n, k and h in Theorem 16 cannot be weakened.

To obtain this result, we first of all prove that small Rédei k-blocking sets B of $PG(n, q)$ are linear (Corollary 12). In this way, our results also contribute to the study of *linear k-blocking sets in $PG(n, q)$* discussed by Lunardon [3].

Warning In the remaining part of this paper we always suppose that the conditions of the "moreover" part of Result 4 are fulfilled.

2. k-blocking sets of Rédei type

Proposition 5 *Let $U \subset AG(n, q)$, $|U| = q^k$, and let $D \subseteq H_\infty$ be the set of directions determined by U. Then for any point $d \in D$ one can find an $(n - 2)$-dimensional subspace $W \subseteq H_\infty$, $d \in W$, such that $D \cap W$ blocks all the $(n - k - 1)$-dimensional subspaces of W.*

The proposition can be formulated equivalently in this way: D is a union of some $B_1, \ldots, B_t$, each one of them being a $(k - 1)$-blocking set of a projective subspace $W_1, \ldots, W_t$ resp., of dimension $n - 2$, all contained in H_∞.

Proof: The proof goes by induction; for any point $d \in D$ we find a series of subspaces $S_1 \subset S_2 \subset \cdots \subset S_{n-1} \subset AG(n,q)$, $\dim(S_r) = r$ such that $s_r = |S_r \cap U| \geq q^{k-n+r} + 1$ and d is the direction determined by S_1. Then, using the pigeon hole principle, after the r-th step we know that all the $(n-k-1)$-dimensional subspaces of $S_r \cap H_\infty$ are blocked by the directions determined by points in S_r, as there are q^{k-n+r} disjoint affine $(n-k)$-subspaces through any of them in S_r, so at least one of them contains 2 points of $U \cap S_r$.

For $r = 1$ it is obvious as d is determined by at least $2 = q^0 + 1 \geq q^{k-n+1} + 1$ points of some line S_1. Then for $r+1$ consider the $\frac{q^{n-r}-1}{q-1}$ subspaces of dimension $r+1$ through S_r, then at least one of them contains at least

$$s_r + \frac{q^k - s_r}{\frac{q^{n-r}-1}{q-1}} = q^{k+1-n+r} + \frac{(s_r - q^{k-n+r})(q^{n-r} - q)}{q^{n-r} - 1} > q^{k+1-n+r}$$

points of U. □

Corollary 6 *For $k = n-1$ it follows that D is the union of some $(n-2)$-dimensional subspaces of H_∞.*

Observation 7 A *projective triangle* in $PG(2,q)$, q odd, is a blocking set of size $3(q+1)/2$ projectively equivalent to the set of points $\{(1,0,0), (0,1,0), (0,0,1), (0,1,a_0), (1,0,a_1), (-a_2,1,0)\}$, where a_0, a_1, a_2 are non-zero squares [2, Lemma 13.6]. The sides of the triangle defined by $(1,0,0)$, $(0,1,0)$, $(0,0,1)$ all contain $(q+3)/2$ points of the projective triangle, so it is a Rédei blocking set.

A cone, with a $(k-2)$-dimensional vertex at H_∞ and with the q points of a planar projective triangle, not lying on one of those sides of the triangle, as a base, has q^k affine points and it determines $\frac{q+3}{2}q^{k-1} + q^{k-2} + q^{k-3} + \cdots + q + 1$ directions.

Lemma 8 *Let $U \subset AG(n,q)$, $|U| = q^{n-1}$, and let $D \subseteq H_\infty$ be the set of directions determined by U. If $H_k \subseteq H_\infty$ is a k-dimensional subspace not completely contained in D then each of the affine $(k+1)$-dimensional subspaces through it intersects U in exactly q^k points.*

Proof: There are q^{n-1-k} mutually disjoint affine $(k+1)$-dimensional subspaces through H_k. If one contained less than q^k points from U then some other would contain more than q^k points (as the average is just q^k), which would imply by the pigeon hole principle that $H_k \subseteq D$, contradiction. □

Theorem 9 *Let $U \subset AG(n,q)$, $|U| = q^{n-1}$, and let $D \subseteq H_\infty$ be the set of directions determined by U. Suppose $|D| \leq \frac{q+3}{2}q^{n-2} + q^{n-3} + q^{n-4} + \cdots + q^2 + q$. Then for any affine line ℓ either*

(i) $|U \cap \ell| = 1$ *(iff $\ell \cap H_\infty \notin D$), or*

(ii) $|U \cap \ell| \equiv 0 \pmod{p^e}$ *for some $e = e_\ell | h$.*

(iii) *Moreover, in the second case the point set $U \cap \ell$ is $GF(p^e)$-linear, so if we consider the point at infinity p_∞ of ℓ; two other affine points p_0 and p_1 of $U \cap \ell$, with $p_1 = p_0 + p_\infty$, then all points $p_0 + xp_\infty$, with $x \in GF(p^e)$, belong to $U \cap \ell$.*

Proof: (i) A direction is not determined iff each affine line through it contains exactly one point of U. (ii) Let $|U \cap \ell| \geq 2$, $d = \ell \cap H_\infty$. Then, from Corollary 6, there exists an $(n-2)$-dimensional subspace $H \subset D$, $d \in H$. There are q^{n-2} lines through d in $H_\infty \setminus H$, so at least one of them has at most

$$\leq \frac{|D| - |H|}{q^{n-2}} \leq \frac{\frac{q+1}{2}q^{n-2} - 1}{q^{n-2}} = \frac{q+1}{2} - \frac{1}{q^{n-2}}$$

points of D, different from d. In the plane spanned by this line and ℓ we have exactly q points of U, determining less than $\frac{q+3}{2}$ directions. So we can use Result 4 for (ii) and (iii). □

Corollary 10 *Under the hypothesis of the previous theorem, U is a $GF(p^e)$-linear set for some $e \mid h$.*

Proof: Take the greatest common divisor of the values e_ℓ appearing in the theorem for each affine line ℓ with more than one point in U. □

The preceding result also means that for any set of affine points ('vectors') $\{a_1, a_2, \ldots, a_t\}$ in U, and $c_1, c_2, \ldots, c_t \in GF(p^e)$, $\sum_{i=1}^{t} c_i = 1$, we have $\sum_{i=1}^{t} c_i a_i \in U$ as well. This is true for $t = 2$ by the corollary, and for $t > 2$ we can combine them two by two, using induction, like

$$\begin{aligned} &c_1 a_1 + \cdots + c_t a_t \\ &\quad = (c_1 + \cdots + c_{t-1}) \left(\frac{c_1}{c_1 + \cdots + c_{t-1}} a_1 + \cdots + \frac{c_{t-1}}{c_1 + \cdots + c_{t-1}} a_{t-1} \right) + c_t a_t, \end{aligned}$$

where $c_1 + \cdots + c_t = 1$.

Theorem 11 *Let $U \subset AG(n, q)$, $|U| = q^k$, and let $D \subseteq H_\infty$ be the set of directions determined by U. If $|D| \leq \frac{q+3}{2} q^{k-1} + q^{k-2} + \cdots + q^2 + q$, then any line ℓ intersects U either in one point, or $|U \cap \ell| \equiv 0 \pmod{p^e}$, for some $e = e_\ell | h$. Moreover, the set $U \cap \ell$ is $GF(p^e)$-linear.*

Proof: If $k = n-1$, then the previous theorem does the job, so suppose $k \leq n-2$. Take a line ℓ intersecting U in at least 2 points. There are at most $q^k - 2$ planes joining ℓ to the other points of U not on ℓ; and their infinite points together with D cover at most $q^{k+1} + \frac{1}{2}q^k + \cdots$ points of H_∞, so they do not form a $(k+1)$-blocking set in H_∞. Take any $(n-k-2)$-dimensional space H_{n-k-2} not meeting any of them, then the projection π of $U \cup D$ from H_{n-k-2} to any 'affine' $(k+1)$-subspace S_{k+1} is one-to-one between U and $\pi(U)$; $\pi(D)$ is the set of directions determined by $\pi(U)$, and the line $\pi(\ell)$ contains the images of $U \cap \ell$ only (as H_{n-k-2} is disjoint from the planes spanned by ℓ and the other points of U not on ℓ). The projection is a small Rédei k-blocking set in S_{k+1}, so, using the previous theorem, $\pi(U \cap \ell)$ is $GF(p^e)$-linear for some $e|h$. But then, as the projection preserves the cross-ratios of quadruples of points, the same is true for $U \cap \ell$. □

Corollary 12 *Under the hypothesis of the previous theorem, U is a $GF(p^e)$-linear set for some $e|h$.*

Proof: Let e be the greatest common divisor of the values e_ℓ appearing in the preceding theorem for each affine line with more than one point in U. □

3. Linear point sets in $AG(n, q)$

First we generalize Lemma 8.

Proposition 13 *Let $U \subset AG(n, q)$, $|U| = q^k$, and let $D \subseteq H_\infty$ be the set of directions determined by U. If $H_r \subseteq H_\infty$ is an r-dimensional subspace, and $H_r \cap D$ does not block every $(n-k-1)$-subspace of H_r then each of the affine $(r+1)$-dimensional subspaces through H_r intersects U in exactly $q^{r+k+1-n}$ points.*

Proof: There are q^{n-1-r} mutually disjoint affine $(r+1)$-dimensional subspaces through H_r. If one contained less than $q^{r+k+1-n}$ points from U then some other would contain more than $q^{r+k+1-n}$ points (as the average is just $q^{r+k+1-n}$), which would imply by the pigeon hole principle that $H_r \cap D$ would block all the $(n-k-1)$-dimensional subspaces of H_r, contradiction. □

Lemma 14 *Let $U \subseteq AG(n, p^h)$, $p > 2$, be a $GF(p)$-linear set of points. If U contains a complete affine line ℓ with infinite point v, then U is the union of complete affine lines through v (so it is a cone with infinite vertex, hence a cylinder).*

Proof: Take any line ℓ' joining v and a point $Q' \in U \setminus \ell$, we prove that any $R' \in \ell'$ is in U. Take any point $Q \in \ell$, let m be the line $Q'Q$, and take a point $Q_0 \in U \cap m$ (any affine combination of Q and Q' over $GF(p)$; see paragraph after the proof of Corollary 10). Now the cross-ratio of Q_0, Q', Q (and the infinite point of m) is in $GF(p)$. Let $R := \ell \cap Q_0R'$, so $R \in U$. As the cross-ratio of Q_0, R', R, and the point at infinity of the line $R'R$, is still in $GF(p)$, it follows that $R' \in U$. Hence $\ell' \subset U$. □

Lemma 15 *Let $U \subseteq AG(n, p^h)$ be a $GF(p)$-linear set of points. If $|U| > p^{n(h-1)}$ then U contains a line.*

Proof: The proof goes by double induction (the 'outer' for n, the 'inner' for r). The statement is true for $n=1$. First we prove that for every $0 \le r \le n-1$, there exists an affine subspace S_r, $\dim S_r = r$, such that it contains at least $|S_r \cap U| = s_r \ge p^{hr-n+2}$ points. For $r=0$, let S_0 be any point of U. For any $r \ge 1$, suppose that each r-dimensional affine subspace through S_{r-1} contains at most p^{hr-n+1} points of U, then

$$p^{hn-n+1} \le |U| \le \frac{p^{hn} - p^{h(r-1)}}{p^{hr} - p^{h(r-1)}}(p^{hr-n+1} - s_{r-1}) + s_{r-1}$$
$$\le \frac{p^{hn} - p^{h(r-1)}}{p^{hr} - p^{h(r-1)}}\left(p^{hr-n+1} - p^{h(r-1)-n+2}\right) + p^{h(r-1)-n+2}.$$

But this is false, contradiction.

So in particular for $r = n - 1$, there exists an affine subspace S_r containing at least $|S_r \cap U| \geq p^{h(n-1)-n+2}$ points of U. But then, from the $(n-1)$-st ('outer') case we know that $S_{n-1} \cap U$ contains a line. □

Now we state the main theorem of this paper. We assume $p > 3$ to be sure that Result 4 can be applied.

Theorem 16 *Let $U \subset AG(n, q)$, $n \geq 3$, $|U| = q^k$. Suppose U determines $|D| \leq \frac{q+3}{2}q^{k-1} + q^{k-2} + q^{k-3} + \cdots + q^2 + q$ directions and suppose that U is a $GF(p)$-linear set of points, where $q = p^h$, $p > 3$.*

If $n - 1 \geq (n-k)h$, then U is a cone with an $(n - 1 - h(n-k))$-dimensional vertex at H_∞ and with base a $GF(p)$-linear point set $U_{(n-k)h}$ of size $q^{(n-k)(h-1)}$, contained in some affine $(n-k)h$-dimensional subspace of $AG(n, q)$.

Proof: It follows from the previous lemma (as in this case $|U| = p^{hk} \geq p^{n(h-1)+1}$) that $U = U_n$ is a cone with some vertex $V_0 = v_0 \in H_\infty$. The base U_{n-1} of the cone, which is the intersection with any hyperplane disjoint from the vertex V_0, is also a $GF(p)$-linear set, of size q^{k-1}. Since U is a cone with vertex $V_0 \in H_\infty$, the set of directions determined by U is also a cone with vertex V_0 in H_∞. Thus, if U determines N directions, then U_{n-1} determines at most $(N-1)/q \leq \frac{q+3}{2}q^{k-2} + q^{k-3} + q^{k-4} + \cdots + q^2 + q$ directions. So if $h \leq \frac{(n-1)-1}{(n-1)-(k-1)}$ then U_{n-1} is also a cone with some vertex $v_1 \in H_\infty$ and with some $GF(p)$-linear base U_{n-2}, so in fact U is a cone with a one-dimensional vertex $V_1 = \langle v_0, v_1 \rangle \subset H_\infty$ and an $(n-2)$-dimensional base U_{n-2}, and so on; before the r-th step we have V_{r-1} as vertex and U_{n-r}, a base in an $(n-r)$-dimensional space, of the current cone (we started "with the 0-th step"). Then if $h \leq \frac{(n-r)-1}{(n-r)-(k-r)}$, then we can find a line in U_{n-r} and its infinite point with V_{r-1} will generate V_r and a U_{n-1-r} can be chosen as well. When there is equality in $h \leq \frac{(n-r)-1}{(n-r)-(k-r)}$, so when $r = n - (n-k)h - 1$, then the final step results in $U_{(n-k)h}$ and $V_{n-1-h(n-k)}$. □

The previous result is sharp as the following proposition shows.

Proposition 17 *In $AG(n, q = p^h)$, for $n \leq (n-k)h$, there exist $GF(p)$-linear sets U of size q^k containing no affine line.*

Proof: For instance, $AG(2k, p)$ in $AG(2k, p^2)$ for which $n = 2k = (n-k)h = (2k-k)2$.

More generally, write $hk = d_1 + d_2 + \cdots + d_n$, $1 \leq d_i \leq h - 1$ $(i = 1, \ldots, n)$ in any way. Let U_i be a $GF(p)$-linear set contained in the i-th coordinate axis, $O \in U_i$, $|U_i| = p^{d_i}$ $(i = 1, \ldots, n)$. Then $U = U_1 \times U_2 \times \cdots \times U_n$ is a proper choice for U. □

References

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

2. J.W.P. Hirschfeld, *Projective Geometries over Finite Fields* (*Second Edition*), Oxford University Press, Oxford, 1998.
3. G. Lunardon, "Linear k-blocking sets in $PG(n, q)$," *Combinatorica*, to appear.
4. L. Rédei, *Lückenhafte Polynome über endlichen Körpern*, Birkhäuser Verlag, Basel, 1970. (English translation: Lacunary Polynomials over Finite Fields, North-Holland, Amsterdam, 1973).