Innovations in Incidence Geometry
Volume 6-7 (2007-2008), Pages 211–226
ISSN 1781-6475

Minimal blocking sets in $\mathsf{PG}(2,q)$ arising from a generalized construction of Megyesi

Nóra V. Harrach Csaba Mengyán

Abstract

We generalize the Megyesi construction for Rédei minimal blocking sets by placing cosets of a multiplicative subgroup of $\mathsf{GF}(q)\setminus\{0\}$ on n lines of the affine plane. These points together with the determined directions give a minimal blocking set B with $|B| \geq (2-2/9)q+O(\sqrt{q})$. We also investigate some constructions in $\mathsf{PG}(2,q^h)$. We show that if there is a minimal blocking set of size $2q-x$ in $\mathsf{PG}(2,q)$, then minimal blocking sets of size $2q^h-x$ and $2q^h-x+1$ exist in $\mathsf{PG}(2,q^h)$, which are not necessarily of Rédei type.

Keywords: projective plane, blocking set, Rédei type
MSC 2000: 51E21

1 Introduction

Throughout this paper we will work in the Desarguesian projective plane $\mathsf{PG}(2,q)$ and its affine part $\mathsf{AG}(2,q)$. Hence q is a power of p, where p is prime. For these planes standard representations will be used, see [8]. We will use the notation $\mathbb{Z}_s = (\mathbb{Z}_s,+)$ for the additive group of integers modulo s and $\mathsf{GF}(q)^* := \mathsf{GF}(q)\setminus\{0\}$.

A *blocking set* B in a projective plane is a set of points which intersects every line. It is straightforward to check that lines are the smallest blocking sets, a blocking set containing a line is called *trivial*. (Note that the terminology is not standard. Sometimes it is supposed that a blocking set contains no line.) A blocking set is said to be *minimal*, when no proper subset of it is a blocking set. It is equivalent to saying that through each point of the blocking set there is a line meeting the set only in this point. Such lines will be called *tangents*. A point P of a blocking set is called *essential* if there is a tangent of B at P, i.e.

$B \setminus P$ is not a blocking set. If there is exactly one tangent t to B at P, then P is called a *critical point*, and t a *critical tangent* [5].

If B is a nontrivial minimal blocking set, then for any line l it is true that $|B \cap l| \leq |B| - q$. If there is a line l for which equality holds (which is equivalent to $|B \setminus l| = q$) then B is said to be a *Rédei blocking set* (or a blocking set of *Rédei type*). Such a line l is called a *Rédei line* of the blocking set.

There are several survey papers about blocking sets. See Blokhuis [1, 2], Szőnyi, Gács, Weiner [16], and Chapter 13 of the second edition of Hirschfeld's book [8] also contains a lot of recent results.

Throughout the paper $U = \{(a_i, b_i) \mid i = 1, \ldots, q\}$ will denote a q-element point set in $\mathsf{AG}(2, q)$. Given such a point set in $\mathsf{AG}(2, q)$, we call a point (m) on the line at infinity *determined* by U if $m = (b_i - b_j)/(a_i - a_j)$ for some points (a_i, b_i) and (a_j, b_j) in U. Note that if $a_i = a_j$ then $m = \infty$. The set of determined directions will be denoted by D; the set of non-determined directions by D^c.

A trivial way to construct blocking sets in $\mathsf{PG}(2, q)$ is to place q points in $\mathsf{AG}(2, q)$ and consider these together with the determined points from the line at infinity. This construction is called *Rédei's construction*.

Proposition 1.1. *Let $U \subset \mathsf{AG}(2, q)$ be a q-element point set; denote by D the set of directions determined by U. If $|D| < q + 1$ then the set $U \cup D$ is a minimal blocking set.*

A number of different methods are presently known for constructing such minimal blocking sets, some using polynomials [4, 7, 12], some using cosets [7]. One well-known and basic example of the latter is due to Megyesi.

Theorem 1.2 (Megyesi)**.** *Let d be a divisor of $q - 1$ and let G be a multiplicative subgroup of $\mathsf{GF}(q)^*$ of size d. Consider the set*

$$U = \{(0, 0)\} \cup \{(0, h) \mid h \notin G\} \cup \{(g, 0) \mid g \in G\}.$$

Then U determines exactly $q+1-d$ directions, and $B = U \cup D$ is a minimal blocking set of size $2q + 1 - d$. Similarly, if d divides q, then using additive subgroups and two parallel lines we get a minimal blocking set B of size $2q + 1 - d$.

Note that the points of the resulting blocking set will be on three lines. The first blocking set is often referred to as the *projective triangle* when $d = (q-1)/2$, while the second is the *projective triad* when $d = q/2$. A different example, contained in the union of four lines, was constructed by Gács [7] giving an infinite series of examples determining $7q/9$ directions approximately, thus yielding a minimal blocking set with size approximately $(2 - 2/9)q$.

Theorem 1.3 (Gács). *Let 3 be a divisor of $q-1$, and let $1, \alpha, \alpha^2$ be coset representatives of the multiplicative subgroup G of index 3. Let*

$$U_i = \{(0,0)\} \cup \{(x,0) \mid x \in \alpha^i G\} \cup \{(x,x) \mid x \in G\} \cup \{(0,x) \mid x \in \alpha^i G\}\,.$$

Denote by $|D_i|$ the number of directions determined by U_i. Then $|D_1| + |D_2| + |D_3| = 3q + 1 - 2(q-1)/3$, and $|D_i| = 7q/9 + O(\sqrt{q})$.

In both the Megyesi and the Gács constructions the cosets of a subgroup of $\mathsf{GF}(q)^*$ were used to select the points of U. We will say, that the cosets were *placed* on lines. The question arises whether a generalization would be possible when the number of cosets is larger than three, or when the number of lines from which points are taken is increased. As we show in this paper this problem can be formulated in the language of some elementary equations and solved by Weil's estimate [15].

In some sense the technique we use here is similar to techniques used by Korchmáros in [10] and Szőnyi in [14], though our method seems to be different from theirs.

2 Placing the cosets on three lines

In this section we investigate the case when the points of the minimal blocking set are on four lines: three concurrent lines in $\mathsf{AG}(2,q)$ and the fourth the line at infinity of the projective closure of $\mathsf{AG}(2,q)$. In particular, without loss of generality, we may assume that the three affine lines are $x = 0$, $y = 0$ and $x = y$.

Construction 2.1. *Let $s \geq 3$ be a divisor of $q-1$ and consider a multiplicative subgroup G of $\mathsf{GF}(q)^*$ with index s. Let $\alpha \in \mathsf{GF}(q)^*$ be an element for which $G, \alpha G, \alpha^2 G, \ldots, \alpha^{s-1}G$ are the cosets of G. Form three non-empty subsets $I, J, K \subset \mathbb{Z}_s$ such that $|I| + |J| + |K| = s$. Let*

$$U = \{(0,x) \mid x \in \alpha^i G, i \in I\} \cup \{(x,0) \mid x \in \alpha^j G, j \in J\} \\ \cup \{(x,x) \mid x \in \alpha^k G, k \in K\} \cup \{(0,0)\}\,.$$

Denote by D the set of directions determined by U. If $|D| < q+1$, then $B = U \cup D$ is a minimal blocking set.

Proof. This is a direct consequence of Proposition 1.1. □

The size of the minimal blocking set B of Construction 2.1 can be determined by determining $|D|$. This is equivalent to determining $|D^c|$, the number of non-determined points, as $|D| + |D^c| = q + 1$. First we will consider the question of determined directions in general: the set of directions determined by two cosets placed on two lines with slope m_1 and m_2 will be calculated. For K a subset of $\mathsf{GF}(q)$ and $a, b \in \mathsf{GF}(q)$, we will use the notations $aK + b = \{ax + b \mid x \in K\}$ and $1/K = \{1/x \mid x \in K\}$. For any element $x \in \mathsf{GF}(q)^*$, note that $x/0 = \infty$ and $x + \infty = \infty$. The set of directions is a subset of $\mathsf{GF}(q) \cup \{\infty\}$.

Lemma 2.2. *Let $m_1, m_2 \in \mathsf{GF}(q)$, $m_1 \neq m_2$, $i_1, i_2 \in \mathbb{Z}_s$.*

- *The set of directions determined by the sets*

$$\left\{(x, m_1 x) \mid x \in \alpha^{i_1} G\right\} \text{ and } \left\{(x, m_2 x) \mid x \in \alpha^{i_2} G\right\}$$

(apart from m_1, m_2) is

$$\left\{ \frac{m_1 - m_2 x}{1 - x} \,\middle|\, x \in \alpha^{i_2 - i_1} G \right\} = m_1 + \frac{m_2 - m_1}{1 - \alpha^{i_1 - i_2} G} = m_2 + \frac{m_1 - m_2}{1 - \alpha^{i_2 - i_1} G}\,.$$

- *The set of directions determined by the sets*

$$\left\{(x, m_1 x) \mid x \in \alpha^{i_1} G\right\} \text{ and } \left\{(0, x) \mid x \in \alpha^{i_2} G\right\}$$

(apart from m_1, ∞) is

$$\left\{m_1 - x \mid x \in \alpha^{i_2 - i_1} G\right\} = m_1 - \alpha^{i_2 - i_1} G\,.$$

Proof. These are basic calculations. □

Corollary 2.3. *The set of directions determined in Construction 2.1 is*

$$D = \{0, 1, \infty\} \cup \left(\bigcup_{\substack{i \in I \\ j \in J}} -\alpha^{i-j} G \right) \cup \left(\bigcup_{\substack{i \in I \\ k \in K}} 1 - \alpha^{i-k} G \right) \cup \left(\bigcup_{\substack{j \in J \\ k \in K}} \frac{1}{1 - \alpha^{j-k} G} \right).$$

Notation. For $m_1, m_2 \in \mathsf{GF}(q) \cup \{\infty\}$, $m_1 \neq m_2$, $u \in \mathbb{Z}_s$ the notation

$$f(m_1, m_2, u) := \begin{cases} m_2 + \dfrac{m_1 - m_2}{1 - \alpha^u G} & \text{if } m_1, m_2 \neq \infty \\ m_1 - \alpha^u G & \text{if } m_2 = \infty \\ m_2 - \alpha^{-u} G & \text{if } m_1 = \infty \end{cases}$$

will be used.

Lemma 2.4. *Let $m_1, m_2, m_3 \in \mathsf{GF}(q) \cup \{\infty\}$ all different, and $u, v, w \in \mathbb{Z}_s$. Then*

(1) $f(m_1, m_2, u) = f(m_2, m_1, -u)$;

(2) $f(m_1, m_2, u) \cap f(m_1, m_2, v) = \emptyset$, *if* $u \neq v$;

(3) $\bigcup_{u=0}^{s-1} f(m_1, m_2, u) = (\mathsf{GF}(q) \cup \{\infty\}) \setminus \{m_1, m_2\}$;

(4) $f(m_1, m_2, u) \cap f(m_2, m_3, v) \subset f(m_1, m_3, u + v)$;

(5) $f(m_1, m_2, u) \cap f(m_2, m_3, v) \cap f(m_1, m_3, w)$
$$= \begin{cases} \emptyset & \text{if } u + v \neq w, \\ f(m_2, m_3, v) \cap f(m_1, m_3, w) & \text{if } u + v = w. \end{cases}$$

Proof. Statement (1) follows from the definition of f, as $1/G = G$. Statements (2) and (3) are direct consequences of the facts: $\alpha^u G \cap \alpha^v G = \emptyset$ if $u \neq v$ and $\bigcup_{u=0}^{s-1} \alpha^u G = \mathsf{GF}(q) \setminus \{0\}$.

For (4) in the case when $m_1, m_2 \neq \infty$, for an element in the left set there are $x, y \in G$ such that
$$\frac{m_1 - m_2\alpha^u x}{1 - \alpha^u x} = \frac{m_2 - m_3\alpha^v y}{1 - \alpha^v y}\,.$$
Thus
$$m_1 - m_2\alpha^u x - m_1\alpha^v y + m_2\alpha^{u+v}xy = m_2 - m_3\alpha^v y - m_2\alpha^u x + m_3\alpha^{u+v}xy\,.$$
Simplifying with $-m_2\alpha^u x$, switching the place of $m_2\alpha^{u+v}xy$ and $m_3\alpha^{u+v}xy$ and adding $m_3\alpha^{u+2v}xy^2$ to both sides yields
$$(m_1 - m_3\alpha^{u+v}xy)(1 - \alpha^v y) = (m_2 - m_3\alpha^v y)(1 - \alpha^{u+v}xy)\,,$$
from which
$$\frac{m_1 - m_3\alpha^{u+v}xy}{1 - \alpha^{u+v}xy} = \frac{m_2 - m_3\alpha^v y}{1 - \alpha^v y} \in f(m_1, m_3, u + v)\,.$$

If $m_3 = \infty$ then there are $x, y \in G$ such that
$$\frac{m_1 - m_2\alpha^u x}{1 - \alpha^u x} = m_2 - \alpha^v y\,,$$
from which
$$m_1 - m_2\alpha^u x = m_2 - \alpha^v y - m_2\alpha^u x + \alpha^{u+v}xy\,.$$
Simplify with $-m_2\alpha^u x$ and take $\alpha^{u+v}xy$ to the other side to get
$$m_1 - \alpha^{u+v}xy = m_2 - \alpha^v y \in f(m_1, \infty, u + v)\,.$$

In the case of $m_1 = \infty$ similar calculations give the result (or the use of (1) several times). As for $m_2 = \infty$: there are $x, y \in G$ such that

$$m_1 - \alpha^u x = m_3 - \alpha^{-v} y\,.$$

Taking $-\alpha^u x$ to the other side, and adding $-m_3\alpha^{u+v}x/y$ to both sides yields

$$\begin{aligned} m_1 - m_3\alpha^{u+v}x/y &= m_3 - \alpha^{-v}y - m_3\alpha^{u+v}x/y + \alpha^u x \\ &= (m_3 - \alpha^{-v}y)(1 - \alpha^{u+v}x/y)\,. \end{aligned}$$

We finally show (5). As a consequence of (4) and (2) the intersection is empty when $u + v \neq w$. In the case of $u + v = w$, (1) and (4) yield that any of the three terms can be omitted: $f(m_1, m_2, u) \cap f(m_2, m_3, v) \cap f(m_1, m_3, w) = f(m_2, m_3, v) \cap f(m_3, m_1, -w) \cap f(m_2, m_1, -u) = f(m_2, m_3, v) \cap f(m_1, m_3, w)$. □

Notation. Let I, J, K be non-empty subsets of $\mathbb{Z}_s$, such that $|I| + |J| + |K| = s$. Denote by $T(I, J, K)$ the set of ordered pairs $(u, v) \in \mathbb{Z}_s \times \mathbb{Z}_s$, for which I, $J + u$ and $K + v$ are pairwise disjoint (that is $\mathbb{Z}_s$ is a disjoint union of I, $J + u$ and $K + v$).

Theorem 2.5. *For the set of Construction 2.1*

$$D^c = \bigcup_{(u,v)\in T(I,J,K)} (-\alpha^u G \cap 1 - \alpha^v G)\,,$$

with the sets $(-\alpha^u G \cap 1 - \alpha^v G)$ *being pairwise disjoint.*

Proof. From Corollary 2.3

$$D^c = \left(\{0, 1, \infty\} \cup \Big(\bigcup_{u\in I-J} -\alpha^u G\Big) \cup \Big(\bigcup_{v\in I-K} 1 - \alpha^v G\Big) \cup \Big(\bigcup_{w\in J-K} \frac{1}{1-\alpha^w G}\Big)\right)^c.$$

Because of (2) and (3) of Lemma 2.4 we have

$$D^c = \Big(\bigcup_{u\notin I-J} -\alpha^u G\Big) \cap \Big(\bigcup_{v\notin I-K} 1 - \alpha^v G\Big) \cap \Big(\bigcup_{w\notin J-K} \frac{1}{1-\alpha^w G}\Big)\,.$$

Thus D^c is the union of intersections of the form

$$-\alpha^u G \cap (1 - \alpha^v G) \cap \frac{1}{1-\alpha^w G} = f(0, \infty, u) \cap f(1, \infty, v) \cap f(1, 0, w)\,,$$

with $u \notin I - J$, $v \notin I - K$, $w \notin J - K$. By Lemma 2.4(5) only those intersections are non-empty where $w + u = v$, and for such an intersection

$$-\alpha^u G \cap (1 - \alpha^v G) \cap \frac{1}{1-\alpha^w G} = -\alpha^u G \cap (1 - \alpha^v G)\,.$$

Thus

$$D^c = \bigcup \{-\alpha^u G \cap (1-\alpha^v G) \mid u \notin I-J, v \notin I-K, v-u \notin J-K\}\,.$$

Because of Lemma 2.4(2) these sets are pairwise disjoint, and the following lemma finishes the proof. □

Lemma 2.6. *Let A, B be non-empty subsets of $\mathbb{Z}_s$, $x \in \mathbb{Z}_s$. Then*

$$x \notin A-B \Longleftrightarrow B+x \cap A = \emptyset.$$

Proof. $x \notin A-B$ means $x \neq a-b$ for any $a \in A$, $b \in B$, that is $b+x \neq a$ for any $a \in A$, $b \in B$. □

The determination of $|D^c|$ now comes down to determining $|T(I,J,K)|$ and the size of a set $-\alpha^u G \cap (1-\alpha^v G)$.

Proposition 2.7. *Let I, J and K be three non-empty subsets of $\mathbb{Z}_s$, such that $|I|+|J|+|K| = s$. Denote by $T(I,J,K)$ the set of ordered pairs $(u,v) \in \mathbb{Z}_s \times \mathbb{Z}_s$, for which I, $J+u$ and $K+v$ are disjoint. Then*

$$|T(I,J,K)| \leq 2s^2/9\,.$$

Equality holds if and only if s is divisible by 3 and $I, J, K \in \{H, H+1, H+2\}$ where $H = \{0,3,6,\ldots,s-3\} = 3 \cdot \mathbb{Z}_s$.

Proof. As $|T(I,J,K)|$ is invariant under translations of I, J, K and permutations of (I,J,K), we may assume I, J, K to be disjoint, and $|I| \geq |J| \geq |K|$, which yields $|K| \leq s/3$ and $|J \cup K| \leq 2s/3$. Here equality holds if and only if $|I| = |J| = |K| = s/3$.

The number of u's satisfying $J+u \cap I = \emptyset$ is clearly at most $|J \cup K|$ (as an element of J can only be translated to elements of $J \cup K$) and for such a u the number of v's satisfying $K+v \cap (I \cup J+u) = \emptyset$ is at most $|K|$. Thus $|T(I,J,K)| \leq 2s^2/9$.

In the case of equality we have $3 \mid s$ and $|I| = |J| = |K| = s/3$ clearly holds. But $|T(I,J,K)| = 2s^2/9$ means that for any u for which $J+u \cap I = \emptyset$, there are $s/3$ translations mapping K onto itself, which proves that K has to be a coset of a subgroup of $\mathbb{Z}_s$. The same is true for I and J. □

For the estimation of the size of a set $-\alpha^u G \cap (1-\alpha^v G)$, a result from Sziklai [13] will be used, which is a variant of the Weil estimate. First we need a definition:

Definition 2.8. Let $f_1, \dots, f_m \in \mathsf{GF}(q)[X]$ be given polynomials. We say that their system is *d-power independent*, if no partial product $f_{i_1}^{s_1} f_{i_2}^{s_2} \cdots f_{i_j}^{s_j}$ (with $1 \le j \le m; 1 \le i_1 < i_2 < \cdots < i_j \le m; 1 \le s_1, s_2, \dots, s_j \le d-1$) can be written as a constant multiple of a d-th power of a polynomial (i.e. $f_{i_1}^{s_1} f_{i_2}^{s_2} \dots f_{i_j}^{s_j} \neq c g^d$).

Lemma 2.9 (Sziklai)**.** *Let $f_1, \dots, f_m \in \mathsf{GF}(q)[X]$ be a set of d-power independent polynomials, where $d \mid (q-1)$; $d, m \ge 2$. Denote by N the number of solutions $\{x \in \mathsf{GF}(q) \mid f_i(x)$ is a d-th power in $\mathsf{GF}(q)$ for all $i = 1, \dots, m\}$. Then*

$$\left| N - \frac{q}{d^m} \right| \le \sqrt{q} \sum_{i=1}^{m} \deg f_i \,.$$

Corollary 2.10. *The number of elements in $-\alpha^u G \cap (1 - \alpha^v G)$ is approximately q/s^2.*

Proof. $x \in G$ is equivalent to $x = y^s$ for some $y \in \mathsf{GF}(q)^*$. Thus $x \in m - \alpha^u G$ is equivalent to $x = m - \alpha^u y^s$, which is equivalent to $\alpha^{-u}(m-x)$ being an s-th power. But then $|-\alpha^u G \cap (1 - \alpha^v G)|$ equals the number of x's, for which the polynomials $f_1(X) = -\alpha^{-u} X$ and $f_2(X) = \alpha^{-v}(1-X)$ are s-th powers. The number of such x's is $q/s^2 + C\sqrt{q}$, with $|C| \le 2$. □

Thus from Theorem 2.5, Proposition 2.7 and Corollary 2.10 we have:

Theorem 2.11. *For the set of Construction 2.1*

$$|D^c| = \frac{|T(I,J,K)|}{s^2}\, q + C\sqrt{q} \le \frac{2}{9} q + C\sqrt{q} \,,$$

with $|C| \le 4s^2/9$. If s is relatively small compared to q, then

$$|B| \ge \left(2 - \frac{2}{9}\right) q + O(\sqrt{q}) \,.$$

This result is in accordance with that of Gács [7]. The point sets given in Theorem 1.3 give smallest examples of our construction. We will now present some further examples.

Theorem 2.12. *Let s be a divisor of $q-1$, $s \ge 3$. In $\mathsf{PG}(2,q)$ minimal blocking sets of size $(2 - \frac{t}{s^2})q + C\sqrt{q}$ exist, where $t \in \{1, 2, k, kl\}$ with $k \mid s$, and $l \mid s$ such that $kl < s$, and $|C| \le 2t$.*

Proof. Here are some examples for the given t's:

$t = 1$: For $I = \mathbb{Z}_s \setminus \{0,1,2\}$, $J = \{1\}$, $K = \{0,2\}$, $T(I,J,K) = \{(0,0)\}$, $D^c = -G \cap (1-G)$, $|D^c| \le q/s^2 + 2\sqrt{q}$.

$t = 2$: For $I = \mathbb{Z}_s \setminus \{u, v\}$, $J = \{u\}$, $K = \{v\}$, $T(I, J, K) = \{(0, 0), (v - u, u - v)\}$, $D^c = (-G \cap 1 - G) \cup (-\alpha^{v-u}G \cap 1 - \alpha^{u-v}G)$, $|D^c| \leq 2q/s^2 + 4\sqrt{q}$.

$t = k$: Let H be a proper subgroup of $\mathbb{Z}_s$, $|H| = k$ (note that $1 \notin H$). For $I = \mathbb{Z}_s \setminus (H \cup \{1\})$, $J = H$, $K = \{1\}$, $T(I, J, K) = \{(0, 0), (h, 0), (2h, 0), \dots\}$, with h a generator element of H. $D^c = \bigcup_{h \in H} \left(-\alpha^h G \cap (1 - G)\right)$, $|D^c| \leq k(q/s^2 + 2\sqrt{q})$.

$t = k$: Let H be a proper subgroup of $\mathbb{Z}_s$, $|H| = k$, $a \in H$. For $I = \mathbb{Z}_s \setminus H$, $J = H \setminus \{a\}$, $K = \{a\}$, $T(I, J, K) = \{(0, 0), (h, h), (2h, 2h), \dots\}$, with h a generator element of H. $D^c = \bigcup_{h \in H} \left(-\alpha^h G \cap (1 - \alpha^h G)\right)$, $|D^c| \leq k(q/s^2 + 2\sqrt{q})$. Note that instead of H the union of some cosets of H could be used, and for K an arbitrary subset of the union, while $J = \cup H \setminus K$ and $I = \mathbb{Z}_s \setminus (J \cup K)$. This and the previous case are the same in this sense (switch I and J).

$t = kl$: Let H_1 and H_2 be proper subgroups of $\mathbb{Z}_s$ with $H_1 \neq H_2$, $|H_1| = k$, $|H_2| = l$, such that $kl < s$. Then there is an element $x \in \mathbb{Z}_s$ such that $H_1 \cap (H_2 + x) = \emptyset$ (because if none of the sets $H_1 \cap (H_2 + x)$, $x = 0, \dots, s/l - 1$ were empty, it would lead to $k \geq s/l$). For $I = \mathbb{Z}_s \setminus (J \cup K)$, $J = H_1$, $K = H_2 + x$, $T(I, J, K) = H_1 \times H_2$, $D^c = \cup_{h_1 \in H_1, h_2 \in H_2} (-\alpha^{h_1} G \cap 1 - \alpha^{h_2} G)$ and $|D^c| \leq lk(q/s^2 + 2\sqrt{q})$. □

In our examples when $T(I, J, K) > 2$, at least one of I, J or K is a union of some cosets of a subgroup of $\mathbb{Z}_s$. If I, J, K are the unions of some cosets of the same subgroup $H \subset \mathbb{Z}_s$, then in Construction 2.4 G can be replaced by the subgroup $\bigcup_{h \in H} \alpha^h G$ of index $s/|H|$.

3 Placing the cosets on $n \geq 4$ lines

In this section we investigate the case when the points of the minimal blocking set are on $n+1$ lines: n concurrent lines in $\mathsf{AG}(2, q)$ and the line at infinity of the projective closure of $\mathsf{AG}(2, q)$. Without loss of generality, we may assume that the n affine lines are $x = 0$ and $y = m_i x$, $i = 2, \dots, n$. The theorems and proofs will be very much the same as when $n = 3$.

Construction 3.1. *Consider a multiplicative subgroup G of $\mathsf{GF}(q)^*$ with index s ($s \geq n$) and an $\alpha \in \mathsf{GF}(q)^*$ such that $\alpha^i G$, $i = 0, \dots, s - 1$ are the cosets of G. Let $m_1 = \infty$ and $\{m_2, m_3, \dots, m_n\} \subset \mathsf{GF}(q)$ be the set of slopes. Form n non-empty subsets $A_1, A_2, \dots, A_n$ in $\mathbb{Z}_s$ such that $|A_1| + |A_2| + \dots + |A_n| = s$. Let*

$$U = \{(0, 0)\} \cup \{(0, x) \mid x \in \alpha^a G, a \in A_1\} \cup \bigcup_{i=2}^{n} \{(x, m_i x) \mid x \in \alpha^a G, a \in A_i\}.$$

If D is the set of directions determined by U and $|D| < q+1$, then the set $B = U \cup D$ is a minimal blocking set.

Notation. For $A_1, A_2, \ldots, A_n$ non-empty subsets of $\mathbb{Z}_s$, such that $\sum_{i=1}^{n} |A_i| = s$, denote by $T(A_1, \ldots A_n)$ the set of ordered $(n-1)$-tuples

$$(u_2, u_3, \ldots, u_n) \in \mathbb{Z}_s \times \cdots \times \mathbb{Z}_s$$

for which $A_1, A_2 + u_2, \ldots, A_n + u_n$ are pairwise disjoint.

Theorem 3.2. *With the previous notations,*

$$D^c = \bigcup \big\{ (m_2 - \alpha^{u_2} G) \cap \cdots \cap (m_n - \alpha^{u_n} G) \\ \mid (u_2, \ldots, u_n) \in T(A_1, A_2, \ldots, A_n) \big\},$$

and this is a disjoint union.

Proof. From Lemma 2.2

$$D = \{\infty\} \cup \{m_i \mid i = 2, \ldots, n\} \cup \bigcup_{1 \le i < j \le n} \Big(\bigcup_{u \in A_i - A_j} f(m_j, m_i, u) \Big).$$

By Lemma 2.4(2 and 3)

$$D^c = \bigcap_{1 \le i < j \le n} \bigcup_{u \notin A_i - A_j} f(m_j, m_i, u) = \bigcup \bigcap_{1 \le i < j \le n} f(m_j, m_i, u_{j,i}) \,.$$

By Lemma 2.4(5), only those intersections

$$f(m_2, m_1, u_{2,1}) \cap f(m_3, m_1, u_{3,1}) \cap \cdots \cap f(m_n, m_{n-1}, u_{n,n-1})$$

are non-empty for which for any 3 indices $i > j > k$: $u_{i,j} + u_{j,k} = u_{i,k}$ holds, and if this is the case, then for any three terms $f(m_i, m_j, u_{i,j})$, $f(m_j, m_k, u_{j,k})$, $f(m_i, m_k, u_{i,k})$ one can be omitted. Thus for any two indices $i > j$ the intersection

$$f(m_i, m_1, u_{i,1}) \cap f(m_j, m_1, u_{j,1}) \cap f(m_i, m_j, u_{i,j})$$

can be replaced by

$$f(m_i, m_1, u_{i,1}) \cap f(m_j, m_1, u_{j,1})$$

with $u_{i,1} \notin A_1 - A_i$, $u_{j,1} \notin A_1 - A_j$ and $u_{i,j} = u_{i,1} - u_{j,1} \notin A_j - A_i$, which is equivalent to the sets A_1, $A_i + u_{i,1}$ and $A_j + u_{j,1}$ being pairwise disjoint. □

Proposition 3.3. *Let $A_1, A_2, \ldots, A_n$ be non-empty subsets of $\mathbb{Z}_s$ such that $|A_1| + |A_2| + \cdots + |A_n| = s$. Denote by $T(A_1, A_2, \ldots, A_n)$ the ordered $(n-1)$-tuples $(u_2, \ldots, u_n)$, with $u_2, \ldots, u_n \in \mathbb{Z}_s$, for which $A_1, A_2+u_2, \ldots, A_n+u_n$ are pairwise disjoint. Then*

$$|T(A_1, A_2, \ldots, A_n)| \leq \frac{(n-1)!\, s^{n-1}}{n^{n-1}}\,.$$

Equality holds if and only if $n \mid s$ and $A_i \in \{H, H+1, H+2, \ldots, H+(n-1)\}$ where $H = \{0, n, 2n, \ldots, s-n\}$ (that is the A_i's are cosets of the subgroup $n \cdot \mathbb{Z}_s$).

Proof. The proof is exactly as in Proposition 2.7:

$$|T(A_1, A_2, \ldots, A_n)| \leq \Big(\sum_{i=2}^{n} |A_i|\Big) \cdot \Big(\sum_{i=3}^{n} |A_i|\Big) \ldots \Big(\sum_{i=n}^{n} |A_i|\Big).$$

If $|A_1| \geq |A_2| \geq \cdots \geq |A_n|$ holds, then $\sum_{i=k+1}^{n} |A_i| \leq (n-k)s/n$. □

Proposition 3.4.

$$|(m_2 - \alpha^{u_2} G) \cap \cdots \cap (m_n - \alpha^{u_n} G)| \leq \frac{q}{s^{n-1}} + (n-1)\sqrt{q}\,.$$

Proof. Identical to that of Proposition 2.10. Use Lemma 2.9 for the polynomials $f_i(X) = \alpha^{-u_i}(m_i - X)$. □

From Theorem 3.2, Proposition 3.3 and Proposition 3.4, we deduce the following result.

Theorem 3.5. *For the set of Construction 3.1,*

$$|D^c| = \frac{|T(A_1, \ldots, A_n)|}{s^{n-1}} q + C\sqrt{q} \leq \frac{(n-1)!}{n^{n-1}} q + C\sqrt{q}\,,$$

with $|C| \leq \frac{(n-1)!}{n^{n-2}} s^{n-1}$. If s is relatively small compared to q, then

$$|B| \geq \left(2 - \frac{(n-1)!}{n^{n-1}}\right) q + O(\sqrt{q})\,.$$

When s is relatively small compared to q, minimal blocking sets of size $2q - \frac{t}{s^{n-1}}\, q + O(\sqrt{q})$ exist, where t is a number depending on some elementary equations.

4 Constructions in $\mathsf{PG}(2, q^h)$

From the existing minimal blocking sets some new ones can be constructed using embeddings of $\mathsf{PG}(2,q)$ into $\mathsf{PG}(2,q^h)$ for some $h>1$. In this section we investigate two possible methods and use them on the minimal blocking sets constructed in this paper and in a paper by Danielsson [6].

Construction 4.1. *Consider a minimal blocking set B of $\mathsf{PG}(2,q)$. Embed $\mathsf{PG}(2,q)$ into $\mathsf{PG}(2,q^h)$ for some $h>1$. Denote by l and m two lines of $\mathsf{PG}(2,q^h)$ that intersect $\mathsf{PG}(2,q)$ in $q+1$ points. If $Q:=l\cap m$ is not a point of B, then suppose also that $|B\cap l|<q$ and $|B\cap m|<q$, and in this case denote by C the set of critical points of B which have their critical tangents through Q. Consider the point set*

$$B' = B \cup \{l \setminus \mathsf{PG}(2,q)\} \cup \{m \setminus \mathsf{PG}(2,q)\} \cup \{Q\} \setminus C\,.$$

We note that if B is a nontrivial blocking set of size less than $2q$ then all lines intersect B in at most $q-1$ points (because through the point not belonging to B on a q-secant there are q further lines to be blocked, thus $|B|\geq 2q$).

Proposition 4.2. *If $|C|\leq 1$ then B' of Construction 4.1 is a minimal blocking set in $\mathsf{PG}(2,q^h)$ of size*

(1) $2q^h-2q+|B|$, *if $Q\in B$;*

(2) $2q^h-2q+|B|+1-|C|$, *if $Q\notin B$.*

Proof. Observe that any line of $\mathsf{PG}(2,q^h)$ through a point of $l\cap\mathsf{PG}(2,q)$ is blocked by the points of B, $m\setminus\mathsf{PG}(2,q)$ or the point Q, and the points of B' on $l\setminus\mathsf{PG}(2,q)$ block the remaining lines proving the blocking property.

Minimality follows as at all points of B' there are tangents. At the points of B the lines containing the tangents to B in $\mathsf{PG}(2,q)$ are tangents as these intersect l and m in $l\cap\mathsf{PG}(2,q)$ and $m\cap\mathsf{PG}(2,q)$, respectively. If through a point of B there is only one tangent, which is on $Q\notin B$, then by definition this point is not in B'. At the points of B' on $l\setminus\mathsf{PG}(2,q)$ the lines through the points of $\{m\cap\mathsf{PG}(2,q)\setminus B\}$ are tangents, and at the points of B' on $m\setminus\mathsf{PG}(2,q)$ the lines through the points of $\{l\cap\mathsf{PG}(2,q)\setminus B\}$ are tangents. At Q all the lines of $\mathsf{PG}(2,q^h)$ intersecting $\mathsf{PG}(2,q)$ in exactly Q are tangents to B'.

The size of B' is simply $|l\setminus\mathsf{PG}(2,q)|+|m\setminus\mathsf{PG}(2,q)|+|B|$ if $Q\in B$ and $|l\setminus\mathsf{PG}(2,q)|+|m\setminus\mathsf{PG}(2,q)|+|B|+1-|C|$ if $Q\notin B$. □

When $Q\notin B$ and $|C|>1$ then the set B' of Construction 4.1 may not be a blocking set at all, because in B a line through two points of C may have been blocked by only these points. In this case some of the points of C have

to be added to B', and thus the size of the resulting blocking set can be only determined given the concrete case. But as the next proposition shows, this problem does not arise when $|B| < 2q$.

Proposition 4.3. *Let $x \geq 1$ be an integer. If the size of B is $2q-x$ then the number of tangents at any point of B is at least $x+1$. Hence there are no critical points of B.*

Proof. We follow the argument of Blokhuis and Brouwer from [3] that is based on a result of Jamison [9]. If B is a minimal blocking set then each point of B is on at least one tangent. Let $P \in B$ be a point on t tangents, call one of them l. Form a blocking set of $\mathsf{AG}(2,q) = \mathsf{PG}(2,q) \setminus l$ with $|B| - 1 + (t-1)$ points by placing a point on each of the $t-1$ tangents ($\neq l$) of P and taking the points of $B \setminus \{P\}$. Then the inequality $t \geq 2q + 1 - |B|$ can be deduced, because in [9] Jamison proved that a blocking set of $\mathsf{AG}(2,q)$ has at least $2q-1$ points. □

Theorem 4.4. *Let $x \geq 1$ be an integer. If there is a minimal blocking set of size $2q-x$ in $\mathsf{PG}(2,q)$ then there are minimal blocking sets of size $2q^h - x$ and $2q^h - x + 1$ in $\mathsf{PG}(2,q^h)$. If there is a Rédei type minimal blocking set of size $2q-x$ in $\mathsf{PG}(2,q)$ then there are both Rédei type and non Rédei type minimal blocking sets of size $2q^h - x$ and $2q^h - x + 1$ in $\mathsf{PG}(2,q^h)$.*

Proof. Use Construction 4.1. Note that $l \cap \mathsf{PG}(2,q)$ (or equivalently $m \cap \mathsf{PG}(2,q)$) is a Rédei line of B if and only if m is a Rédei line of B', as $|B' \setminus m| = |B \setminus m| + q^h - q$. All other lines intersect B' in less than q points. □

In [6] Danielsson proves the existence of Rédei type minimal blocking sets of size $2p-3$ and $2p-2$.

Theorem 4.5 (Danielsson)**.** *There are Rédei type minimal blocking sets of size $2p-3$, where $p > 5$ is a prime and $p \equiv 1 \pmod 4$ and of size $2p-2$, where $p > 5$ is a prime and $p \equiv 3 \pmod 4$.*

Using the previous constructions the following can be proved:

Corollary 4.6. *Let $q = p^h$ with $h > 1$ and $p > 5$ prime. In $\mathsf{PG}(2,q)$ there are both Rédei and non Rédei type minimal blocking sets of size $2q-2$. If $p \equiv 1 \pmod 4$, then in $\mathsf{PG}(2,q)$ there are both Rédei and non Rédei type minimal blocking sets with size $2q-3$.*

We now turn attention to another embedding method, described in [11] and [16]. Here we only repeat the construction and a theorem from these papers, and investigate what this method means for the minimal blocking sets obtained in this paper. For further details of this construction we refer to the papers [11, 16].

Construction 4.7. *Let B be a minimal blocking set in $\mathsf{PG}(2,q)$. Embed $\mathsf{PG}(2,q)$ into $\mathsf{PG}(h+1,q)$. Choose an $(h-2)$-dimensional subspace V', so that $\mathsf{PG}(2,q)\cap V'=\emptyset$. Let B' be the cone with base B and vertex V'. Embed $\mathsf{PG}(h+1,q)$ as a subgeometry in $\mathsf{PG}(h+1,q^h)$. Assume that R is an $(h-1)$-dimensional subspace of $\mathsf{PG}(h+1,q)$, and let R^* be the unique $(h-1)$-dimensional subspace of $\mathsf{PG}(h+1,q^h)$ that contains R. Choose an $(h-2)$-dimensional subspace P in R^*, such that P does not intersect the subgeometry $\mathsf{PG}(h+1,q)$, and project B' from this subspace onto a plane π of $\mathsf{PG}(h+1,q^h)$, where $\pi\cap P=\emptyset$. The cardinality of the projection, B'' satisfies $|B''|=|B'|+1-|R\cap B'|$.*

Note that B' is a minimal blocking set of $\mathsf{PG}(h+1,q)$ with respect to lines and $|B'|=q^{h-1}|B|+\frac{q^{h-1}-1}{q-1}$, thus if $|B|<2q$ then $|B'|<2q^h$.

Theorem 4.8. *Let B' be a minimal blocking set of $\mathsf{PG}(h+1,q)$ with respect to lines and suppose that $|B|'\leq 2q^h-1$. Then the projection B'' of B' is a minimal blocking set of $\mathsf{PG}(2,q^h)$.*

By Theorem 4.8 the projection according to Construction 4.7 of all the minimal blocking sets constructed in this paper will give minimal blocking sets for sufficiently large q. The size of the resulting blocking set B'' depends on the choice of R. Following the reasonings of [16, page 262] it can be proved that depending on the dimension of $R\cap V'$ (which can vary between $h-2$ and $h-4$) the size of $|R\cap B'|$ can be: $\frac{q^{h-1}-1}{q-1}$, $q^{h-1}+\frac{q^{h-1}-1}{q-1}$, $rq^{h-2}+\frac{q^{h-2}-1}{q-1}$ (where B has an r-secant in $\mathsf{PG}(2,q)$) and $|B|q^{h-3}+\frac{q^{h-3}-1}{q-1}$.

Theorem 4.9. *Let B be a minimal blocking set of $\mathsf{PG}(2,q)$ with $|B|=2q-x$, where $x\geq 1$. Using Construction 4.7 one can obtain blocking sets of $\mathsf{PG}(2,q^h)$, $h>1$ with sizes*

- $2q^h-xq^{h-1}+1$,
- $2q^h-(x+1)q^{h-1}+1$,
- $2q^h-xq^{h-1}-q^{h-2}+(x+1)q^{h-3}+1$,
- $2q^h-xq^{h-1}-(r-1)q^{h-2}+1$, *where B has an r-secant in $\mathsf{PG}(2,q)$.*

It is not difficult to see that given a Rédei type minimal blocking set, we can choose R in such a way that the projection will be Rédei or non Rédei. For simplicity let $h=2$, thus R is a line of $\mathsf{PG}(h+1,q)$ (with either $V'\in R$ or $V'\notin R$). Let B be a minimal blocking set of size $2q-x$ with $x\geq 1$. There will be three types of lines in the projection:

(i) lines that were projected from lines of $\mathsf{PG}(h+1,q)$: these intersect B'' in at most $q+1$ points;

(ii) lines that were projected from a plane β through R, with $V' \notin \beta$ (only if $V' \notin R$): these intersect B'' in $|B| + 1 - |R \cap B'|$ points;

(iii) lines that were projected from a plane β through R, with $V' \in \beta$: these intersect B'' in $rq + 2 - |R \cap B'|$ points, where $r = |\beta \cap B|$.

(For a precise discussion on intersection numbers of B'' with respect to lines, see [11, p. 742].) For B'' to be a Rédei minimal blocking set we must have some lines intersect B'' in $|B|q + 2 - |R \cap B'| - q^2 = q^2 - qx + 2 - |R \cap B'|$ points. For the lines of type (i) this is impossible. For a line of type (ii) to be a Rédei line, the equation $|B|q + 2 - |R \cap B'| - q^2 = |B| + 1 - |R \cap B'|$ has to hold, which leads to $|B| = q + 1$, a contradiction. For a line of type (iii) to be a Rédei line, the equation $|B|q + 2 - |R \cap B'| - q^2 = rq + 2 - |R \cap B'|$ has to hold, from which $|B| - q = r$, which is equivalent to $\beta \cap \mathsf{PG}(2, q)$ being a Rédei line of B. Thus B'' will be a Rédei type blocking set if and only if there is a plane on R and V' intersecting $\mathsf{PG}(2, q)$ in a Rédei line of B.

Acknowledgment. The authors wish to thank T. Szőnyi for fruitful discussions and insights into the inherent problems.

References

[1] **A. Blokhuis**, Blocking sets in Desarguesian planes, in: Paul Erdős is Eighty, Volume 2, (D. Miklós, V.T. Sós and T. Szőnyi, eds.), *Bolyai Soc. Math. Stud.* **2**, Bolyai Society, Budapest, 1996, 133–155.

[2] _____, Combinatorial problems in finite geometry and lacunary polynomials, in: Li, Ta Tsien (ed.) et al., *Proceedings of the International Congress of Mathematicians, ICM 2002, Beijing, China, 2002, Vol. III: Invited lectures*, Beijing, Higher Education Press, 537–545 (2002).

[3] **A. Blokhuis** and **A. Brouwer**, Blocking sets in Desarguesian projective planes, *Bull. London Math. Soc.* **18** (1986), 132–134.

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

[5] **A. Bruen** and **K. Drudge**, The return of the Baer subplane, *J. Combin. Theory Ser. A* **85** (1999), 228–231.

[6] **J. Danielsson**, Minimal blocking sets of size $2p-2$ and $2p-3$ in $\mathsf{PG}(2, p)$, p prime and $p > 5$, *J. Geom.* **88** (2008), 15–18.

[7] **A. Gács**, On the number of directions determined by a point set in AG$(2, p)$, *Discrete Math.* **208/209** (1999), 299–309.

[8] **J. W. P. Hirschfeld**, *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1979, 2nd edition, 1998.

[9] **R. Jamison**, Covering finite fields with cosets of subspaces, *J. Combin. Theory Ser. A* **22** (1977), 253–266.

[10] **G. Korchmáros**, New examples of complete k-arcs in PG$(2, q)$, *European J. Combin.* **4** (1983), 329–334.

[11] **O. Polverino**, **T. Szőnyi** and **Zs. Weiner**, Blocking sets in Galois planes of square order, *Acta Sci. Math. (Szeged)* **65** (1999), 737–748.

[12] **L. Rédei**, *Lacunary Polynomials over Finite Fields*, North-Holland Publishing Co., Amsterdam, American Elsevier Pub. Co., New York, 1973.

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

[14] **T. Szőnyi**, Combinatorial problems for Abelian groups arising from geometry, *Period. Polytech. Mech. Engrg.* **19** (1991), 91–100.

[15] _____, Some applications of algebraic curves in finite geometry and combinatorics, *Surveys in Combinatorics, Proc. British Comb. Conf.* 1997 (ed. R.A. Bailey), 197–236.

[16] **T. Szőnyi**, **A. Gács** and **Zs. Weiner**, On the spectrum of minimal blocking sets in PG$(2, q)$, *J. Geom.* **76** (2003), 256–281.

Nóra V. Harrach

Department of Computer Science, Eötvös Loránd University, Pázmány Péter sétány 1/C, H-1117 Budapest, Hungary

e-mail: hanovi@cs.elte.hu

Csaba Mengyán

Department of Computer Science, Eötvös Loránd University, Pázmány Péter sétány 1/C, H-1117 Budapest, Hungary

e-mail: mengyan@cs.elte.hu