Blocking Sets of Size $q^t + q^{t-1} + 1$

G. Lunardon and O. Polverino¹

Dip. di Matematica e Applicazioni, Complesso di Monte S. Angelo,
Edificio T, Via Cintia, 80126 Napoli, Italy
E-mail: lunardon@matna3.dma.unina.it, polverin@matna2.dma.unina.it

Communicated by Francis Buekenhout
Received May 11, 1999

We prove that in the desarguesian plane $PG(2, q^t)$ ($t > 4$) there are at least three inequivalent blocking sets of size $q^t + q^{t-1} + 1$. The first one has $q + 1$ Rédei lines, the second one has exactly one Rédei line, and the third one is not of Rédei type. For $GF(q)$ the largest subfield of $GF(q^t)$, our results disprove a conjecture quoted by A. Blokhuis (1998, in “Galois Geometry and Generalized Polygons,” Gent).

1. INTRODUCTION

A blocking set $B$ in a finite projective plane is a set of points intersecting every line. $B$ is called trivial if it contains a line. Throughout this paper, we will only consider non-trivial blocking sets.

A blocking set is called minimal if no proper subset of it is a blocking set. If $q$ is the order of the plane and $B$ has size $q + N$, then a line contains at most $N$ points of $B$: if such a line exists, $B$ is called of Rédei type and the line is said to be a Rédei line.

Two blocking sets are said to be equivalent if there is a collineation of the plane which maps one to the other.

Minimal blocking sets of a desarguesian plane $PG(2, q^t)$, $q = p^e$ $p$ prime, of size less than $\frac{3q^t+1}{2}$ are called small. They intersect every line in a number of points congruent to 1 modulo $p$ (see [12]).

It has been proved by Bruen in [3] that a blocking set $B$ has size $|B| \geq q + \sqrt{q} + 1$, and equality holds if and only if $B$ is a Baer subplane. Therefore, in a desarguesian plane of square order, all the blocking sets of minimum size are equivalent.

¹This paper was written while the first author was visiting the University of Gent. We thank the Department of Pure Mathematics and Computer Algebra for the financial support.
Let $GF(q) \subset GF(q')$, and let $tr(x) = x + x^{q} + \ldots + x^{q^{t-1}}$ be the trace of $GF(q')$ over $GF(q)$. If $(X_0, X_1, X_2)$ are the homogeneous coordinates of a point of $PG(2, q')$, then $R = \{(x, tr(x), b) | x \in GF(q'), b \in GF(q)\}$ is a small minimal blocking set of $PG(2, q')$ of size $q^{t} + q^{t-1} + 1$ such that $X_2 = 0$ is a Rédei line. It is easy to prove that all secant lines incident with the point $(1, 0, 0)$ are Rédei lines. For $t=2$, $R$ is a Baer subplane of $PG(2, q^2)$.

If $GF(q)$ is the largest subfield of $GF(q^t)$, it has been conjectured in [1] that a small minimal blocking set $B$ of $PG(2, q)$ has size $|B| \geq q^{t} + q^{t-1} + 1$, and equality holds if and only if $B$ is equivalent to $R$.

The proof of the conjecture for $t=2$ follows from Bruen’s characterisation of the Baer subplane as the blocking set of minimum size. For $p=2$ (prime) it has been proved in [2] that, up to equivalence, $R$ is the only Rédei blocking set of size $p^{3} + p^{2} + 1$. As for $p \geq 7$ the small minimal blocking sets of $PG(2, p^t)$ are of Rédei type (see [10]), the conjecture is true for $t=3$ and $p$ prime, $p \geq 7$. Hence, the first open case is $PG(2, p^3)$ with $p$ a prime number.

In this paper, using the linear blocking sets introduced in [7], we construct two blocking sets of size $q^{t} + q^{t-1} + 1$ in $PG(2, q^t)$, one of which is not of Rédei type (here $t>4$) while the other one has exactly one Rédei line (and $t>3$). We also prove that the $GF(q)$-linear blocking sets\(^2\) of $PG(2, q^t)$ of size $q^{t} + q^{t-1} + 1$ with $q+1$ Rédei lines are equivalent. If $GF(q)$ is the largest subfield of $GF(q^t)$, our results disprove the above conjecture.

As a corollary, we also prove that a small minimal blocking set with two Rédei lines is equivalent to the blocking set defined by the trace.

2. LINEAR BLOCKING SETS

Let $V$ be a vector space over a field $F$. We will denote by $PG(V, F)$ the projective geometry of the $F$-linear subspaces of $V$. Accordingly, given a subfield $K$ of $F$, the symbol $PG(V, K)$ will stand for the projective geometry of the $K$-linear subspaces of $V$. As usual, if $F = GF(q)$ and $V$ has finite rank $n + 1$, we will write $PG(V, F) = PG(n, q)$, and we denote by $\langle v \rangle$ the point of $PG(V, F)$ defined by the non-zero vector $v$ of $V$.

Let $\Sigma^*$ be a projective space. A subset $\Sigma$ of points of $\Sigma^*$ is a subgeometry of $\Sigma^*$ if there is a set $\mathcal{L}$ of subsets of $\Sigma$ with the following properties:

\begin{enumerate}
  \item each element of $\mathcal{L}$ is contained in a line of $\Sigma^*$;
  \item $(\Sigma, \mathcal{L})$ is a projective space;
\end{enumerate}

\(^2\) In [7-9] $B$ is simply called linear.
(c) if a line $L$ of $\Sigma^*$ contains two points of $\Sigma$, then $L \cap \Sigma \in \mathcal{L}$;

(d) no line of $\Sigma^*$ belongs to $\mathcal{L}$.

If $\Sigma^*$ is a plane, we call $\Sigma$ a subplane.

Let $\Sigma = PG(V, GF(q))$ be a subgeometry of $\Sigma^* = PG(V^*, GF(q^*))$. We say that $\Sigma$ is a canonical subgeometry of $\Sigma^*$ when $V^* = GF(q^*) \oplus V$. This is equivalent to saying that a frame of $\Sigma$ is also a frame of $\Sigma^*$. A canonical subgeometry $\Sigma = PG(1, q)$ of $PG(1, q^*)$ is called a subline. We recall that not all the subgeometries are canonical (see, e.g., [6]).

Let $\pi = PG(2, q^*) = PG(V, GF(q^*))$ where $V$ is a 3-dimensional vector space over $GF(q^*)$. Regarding $V$ as a vector space of dimension $3t$ over $GF(q)$, each point $x$ of $\pi = PG(2, q^*)$ defines a $(t-1)$-dimensional subspace $P(x)$ of the projective space $PG(V, GF(q)) = PG(3t-1, q)$, and each line $l$ of $PG(2, q^*)$ defines a $(2t-1)$-dimensional subspace $P(l)$ of $PG(3t-1, q)$.

Let $\mathcal{F}$ be the set of all the $(t-1)$-dimensional subspaces $P(x)$ where $x$ is a point of $PG(2, q^*)$. Then $\mathcal{F}$ is a $(t-1)$-spread of $PG(3t-1, q)$. Moreover if $U$ is a $(2t-1)$-dimensional subspace of $PG(3t-1, q)$ containing two elements of $\mathcal{F}$, then a $(t-1)$-spread is induced by $\mathcal{F}$ in $U$, i.e., $U = P(l)$ for some line $l$ of $PG(2, q^*)$. We call $\mathcal{F}$ the $GF(q)$-linear representation of $\pi = PG(2, q^*)$.

A regulus $\mathcal{R}$ of $PG(2t-1, q)$ is a set of $q+1$ mutually disjoint $(t-1)$-dimensional subspaces such that each line intersecting three elements of $\mathcal{R}$ intersects all the elements of $\mathcal{R}$. Such a line is called a transversal line of $\mathcal{R}$. If $U$ is an element of $\mathcal{R}$, then each point of $U$ is incident with exactly one transversal line.

For each line $m$ of $PG(3t-1, q)$ not contained in any element $P(x)$ of $\mathcal{F}$, the subset $\mathcal{M} = \{P(x) \cap m \neq \emptyset \}$ is a regulus (see, e.g., [8]).

Let $L$ be a $t$-dimensional subspace of $PG(3t-1, q)$ and let $B_L = \{ x \in PG(2, q^*) : P(x) \cap L \neq \emptyset \}$. If $L$ is not contained in $P(l)$ for any line $l$ of $PG(2, q^*)$, then $B_L$ is a small minimal blocking set (see [7, 9]).

A blocking set $B$ of $PG(2, q^*) = PG(V, GF(q^*))$ is $GF(q)$-linear if and only if $B$ is equivalent to some $B_L$. By [8], $B$ is a $GF(q)$-linear blocking set if and only if there is a subset $W$ of $V$ such that:

(a) $W$ is a $GF(q)$-vector space of rank $t+1$;

(b) $V = \langle W \rangle$;

(c) $B = \{ \langle v \rangle : v \in W \setminus \{0\} \}$.

If $L$ is the subspace of $PG(3t-1, q)$ defined by $W$, then $B = B_L$. We note that $W$ is not uniquely defined, as proved in [8].

Suppose $\Sigma = PG(n, q)$ is a canonical subgeometry of $\Sigma^* = PG(n, q^*)$. A subspace $S$ of $\Sigma^*$ intersects $\Sigma$ in a subspace $S \cap \Sigma$ whose dimension is less
or equal than the dimension of $S$. When $S$ and $S \cap \Sigma$ have the same dimension we say that $S$ is a subspace of $\Sigma$. A collineation of $\Sigma$ defines a unique collineation of $\Sigma^*$, and a collineation of $\Sigma^*$ fixing $\Sigma$ induces a collineation of $\Sigma$. Moreover, the collineation group of $\Sigma^*$ acts transitively on the canonical subgeometries of $\Sigma^*$.

Let $\Sigma = PG(t, q)$ ($t \geqslant 3$) be a canonical subgeometry of $\Sigma^* = PG(t, q')$. Let $\pi^*$ be a $(t-3)$-dimensional subspace of $\Sigma^*$ disjoint from $\Sigma$, and let $\pi$ be a plane of $\Sigma^*$ disjoint from $\pi^*$. Define the map $p_{\pi^*, \pi, \Sigma}$ from $\Sigma$ to $\pi$ by $x \mapsto \langle x, \pi^* \rangle \cap \pi$ for each point $x$ of $\Sigma$.

**Theorem 1** [8]. $B = p_{\pi^*, \pi, \Sigma}(\Sigma)$ is a $GF(q)$-linear blocking set of $\pi = PG(2, q')$.

### 3. REGULI AND BLOCKING SETS OF $PG(2, q^5)$

Let $\Sigma^* = PG(V^*, GF(q')) = PG(5, q')$. Fix a basis $\{e_0, e_1, e_2, e_3, e_4, e_5\}$ of $V^*$ and denote by $(x_0, x_1, x_2, x_3, x_4, x_5)$ the homogeneous coordinates of the point $\langle x_0 e_0 + x_1 e_1 + x_2 e_2 + x_3 e_3 + x_4 e_4 + x_5 e_5 \rangle$ of $\Sigma^*$. Let $\sigma$ be the semilinear map of $V^*$ to itself defined by

$$
\sigma: \sum_{i=0}^{5} x_i e_i \mapsto \sum_{i=0}^{5} x_i^q e_i.
$$

Then $V = \{v \in V^* | v^\sigma = v\}$ is a 6-dimensional $GF(q)$-vector space and $\{e_0, e_1, e_2, e_3, e_4, e_5\}$ is also a basis of $V$ over $GF(q)$. Hence $V^* = GF(q') \otimes V$, i.e. $\Sigma = PG(V, GF(q))$ is a canonical subgeometry of $\Sigma^*$. If $x = (x_0, x_1, x_2)$ and $y = (x_3, x_4, x_5)$, put $(x, y) = (x_0, x_1, x_2, x_3, x_4, x_5)$. Let

$$
F(\infty) = \{(0, y) | y = (a, b, c); a, b, c \in GF(q)\},
$$

$$
F(\lambda) = \{(x, \lambda x) | x = (a, b, c); a, b, c \in GF(q)\}, \quad \lambda \in GF(q),
$$

$$
\mathcal{R} = \{F(i) | i = \infty \ \text{or} \ i \in GF(q)\}.
$$

Then $\mathcal{R}$ is a regulus of $\Sigma$. Denote by $\mathcal{R}^*$ the regulus of $\Sigma^*$ defined by $\mathcal{R}$, i.e.,

$$
\mathcal{R}^* = \{F^*(i) | i = \infty \ \text{or} \ i \in GF(q^5)\},
$$
where
\[ F^*(\infty) = \{ (0, y) \mid y = (a, b, c); a, b, c \in GF(q^5) \}, \]
\[ F^*(\lambda) = \{ (x, \lambda x) \mid x = (a, b, c); a, b, c \in GF(q^5) \}, \quad \lambda \in GF(q^5). \]

We note that if \( i = \infty \) or \( i \in GF(q) \), then \( F^*(i) \cap \Sigma = F(i) \).

**Lemma 1.** If \( \lambda \in GF(q^5) \setminus GF(q) \), then \( F^*(\lambda) \cap \Sigma = \emptyset \).

**Proof.** For \( x = (a, b, c) \), put \( x^* = (a^6, b^6, c^6) \). The point \((x, \lambda x) \neq (0)\) belongs to \( \Sigma \) if and only if \( (x^*, \lambda^* x^*) = \mu(x, \lambda x) \) for some element \( \mu \) of \( GF(q^5) \) different from 0. Hence \( x^* = \mu x \) and \( \lambda^* x^* = \mu \lambda x \). This implies \( \lambda^* = \lambda \).

**Theorem 2.** Fix \( \lambda \in GF(q^5) \setminus GF(q) \). Let \( \pi^* = F^*(\lambda) \) and \( \pi = F^*(\infty) \). Then \( B = p_{\pi^* \cap \pi}(\Sigma) \) is a non-Rédei blocking set in \( \pi = PG(2, q^5) \) of size \( q^5 + q^4 + 1 \).

**Proof.** We will prove that for each point \((x, y)\) of \( \Sigma \) the intersection \( \langle \pi^*, (x, y) \rangle \cap \Sigma \) is either the point \((x, y)\) or a line of \( \Sigma \) incident with \((x, y)\).

By way of contradiction, suppose that for some point \((x, y)\) the subspace \( \langle \pi^*, (x, y) \rangle \) contains a plane \( \pi \) of \( \Sigma \). Let \( m = \pi \cap \pi^* \). As \( \pi \) is a plane of \( \Sigma \), the collineation \( \sigma \) fixes \( \pi \). Therefore, the line \( m^* \) is contained in \( \pi \). This implies that \( m \) and \( m^* \) are not disjoint, i.e., \( \pi^* = F^*(\lambda) \) and \( (\pi^*)^* = F^*(\lambda^*) \) are two distinct elements of \( \mathcal{B}^* \) we have the required contradiction.

If \((x, y)\) is a point of \( \Sigma \) incident with an element of \( \mathcal{B} \), then \( \langle \pi^*, (x, y) \rangle \cap \Sigma \) is the transversal line of \( \mathcal{B} \) incident with \((x, y)\).

Suppose that for some point \((x, y)\) of \( \Sigma \) the subspace \( \langle \pi^*, (x, y) \rangle \) contains a line \( m \) of \( \Sigma \) incident with \((x, y)\). Then \( m \) intersects \( F^*(\lambda), F^*(\lambda^*), F^*(\lambda^*), F^*(\lambda^*), F^*(\lambda^*), F^*(\lambda^*), F^*(\lambda^*), F^*(\lambda^*), F^*(\lambda^*), F^*(\lambda^*) \) because \( m \) is fixed by the collineation \( \sigma \). As \( \lambda \) does not belong to \( GF(q) \), the planes \( F^*(\lambda), F^*(\lambda^*), F^*(\lambda^*), F^*(\lambda^*), F^*(\lambda^*), F^*(\lambda^*) \) are pairwise distinct. Therefore, \( m \) is a transversal line of \( \mathcal{B}^* \).

Hence \( m \) is a transversal line of \( \mathcal{B} \) because it is a line of \( \Sigma \). This implies that the point \((x, y)\) belongs to an element of \( \mathcal{B} \).

There are exactly \( q^3 - q \mid q^2 + q + 1 \) transversal lines of \( \mathcal{B} \) and exactly \( (q^3 - q)(q^2 + q + 1) \) points of \( \Sigma \) not incident with an element of \( \mathcal{B} \), then the size of \( B \) is
\[ |B| = (q^3 - q)(q^2 + q + 1) + q^2 + q + 1 = q^5 + q^4 + 1. \]

If a hyperplane \( H \) of \( \Sigma \) contains \( \pi^* = F^*(\lambda) \), then \( H \) contains also the plane \( (\pi^*)^* = F^*(\lambda^*) \) because \( H^* = H \). This implies that \( F^*(\lambda) \) and \( F^*(\lambda^*) \) are skew because \( H \) has dimension 4. As \( F^*(\lambda) \) and \( F^*(\lambda^*) \) are skew, we have proved that no hyperplane of \( \Sigma \) contains \( \pi^* \).
If a line $l$ of $\pi$ is a Rédei line of $B$, then the hyperplane $H = \langle \pi^*, l \rangle$ contains at least $q^t + 1$ points of $\Sigma$. Therefore $H$ is a hyperplane of $\Sigma$. As no hyperplanes of $\Sigma$ contain $\pi^*$, we conclude that $B$ is not of Rédei type. 

**Corollary 1.** In the hypotheses of Theorem 2, we have $B = \{(0, -xv + y) | y, v \in GF(q^3)\}$.

4. TWO EXAMPLES OF BLOCKING SETS

If $\pi = PG(2, q') = PG(V, GF(q'))$ and $w_0, w_1, w_2$ is a $GF(q')$-basis of $V$, denote by $(X_0, X_1, X_2)$ the homogeneous coordinates of the point $\langle X_0w_0 + X_1w_1 + X_2w_2 \rangle$ of $\pi$. Let $\mathcal{F}$ be the $GF(q')$-linear representation of $PG(3t - 1, q) = PG(V, GF(q'))$.

**Lemma 2.** Let $B = B_L$ be a $GF(q)$-linear blocking set and let $m$ be a Rédei line of $B$. If $|B| \geq q^t + q^{t-1} + 1$, then $P(m) \cap L$ has dimension $t - 1$, and for all the points $(X_0, X_1, X_2)$ of $B$ not incident with $m$, the subspace $P(X_0, X_1, X_2) \cap L$ is a point.

**Proof.** As $B$ has size at least $q^t + q^{t-1} + 1$, the subspace $P(m) \cap L$ has dimension $t - 1$ because it contains at least $q^{t-1} + 1$ points. Therefore, if $(X_0, X_1, X_2)$ belongs to $B \setminus m$, then $P(X_0, X_1, X_2)$ intersects $L$ in a point because $P(X_0, X_1, X_2)$ and $P(m)$ are disjoint. 

**Theorem 3.** Let $t > 3$ and fix a primitive element $\lambda$ of $GF(q')$. Let

$$B = \{(x_0 + x_1\lambda, y_0 + y_1\lambda + \cdots + y_{t-3}\lambda^{t-3}, z_0) | x_0, x_1, y_0, y_1, \ldots, y_{t-3}, z_0 \in GF(q')\}.$$ 

Then $B$ is a $GF(q')$-linear blocking set of size $q^t + q^{t-1} + 1$, and $X_2 = 0$ is the unique Rédei line of $B$.

**Proof.** Let $W$ be the set of all the vectors of $V$ of the form $(x_0 + x_1\lambda, y_0 + y_1\lambda + \cdots + y_{t-3}\lambda^{t-3}, z_0)$ such that $x_0, x_1, y_0, y_1, \ldots, y_{t-3}, z_0 \in GF(q)$. As $V = \langle W \rangle$ and $W$ is a $GF(q')$-vector space of rank $t + 1$, it defines a $t$-dimensional subspace $L$ of $PG(V, GF(q')) = PG(3t - 1, q)$ not contained in any subspace $P(l)$ for $l$ a line of $\pi$. By definition, $B = B_L$ is a $GF(q')$-linear blocking set of $\pi$.

Let $m$ be the line with equation $X_2 = 0$. Then, $P(m) \cap L$ has dimension $t - 1$, i.e., $m$ is a Rédei line of $B$ (see [7, Sect. 5]). We note that $P(0, 1, 0) \cap L$ has dimension $t - 3$. Hence, for each point $(1, u, 0)$ of the line $X_2 = 0$, the intersection $P(1, u, 0) \cap L$ is a line or a point or empty.
A point of $P(1, u, 0) \cap L$ has coordinates $(\beta, \beta u, 0) = (x_0 + x_1 \lambda, y_0 + y_1 \lambda + \cdots + y_{t-1} \lambda^{t-1}, 0)$ where $\beta \in GF(q^t)$ and $x_0, y_0, \ldots, y_{t-1} \in GF(q)$. If $\alpha = u_0 + u_1 \lambda + \cdots + u_{t-1} \lambda^{t-1}$ with $u_0, u_1, \ldots, u_{t-1} \in GF(q)$, then

$$(x_0 + x_1 \lambda)(u_0 + u_1 \lambda + \cdots + u_{t-1} \lambda^{t-1}) = y_0 + y_1 \lambda + \cdots + y_{t-1} \lambda^{t-1}.$$ 

As $\lambda' = a_0 + a_1 \lambda + \cdots + a_{t-1} \lambda^{t-1}$ for suitable elements $a_0, a_1, \ldots, a_{t-1} \in GF(q)$ because $\lambda$ is a primitive element of $GF(q')$, we have

$$
\begin{align*}
&x_0 u_0 + x_1 u_{t-1} a_0 = y_0, \\
x_0 u_1 + x_1 (u_0 + u_{t-1} a_1) = y_1, \\
x_0 u_2 + x_1 (u_1 + u_{t-1} a_2) = y_2, \\
&\vdots \\
x_0 u_{t-3} + x_1 (u_{t-4} + u_{t-1} a_{t-3}) = y_{t-3}, \\
x_0 u_{t-2} + x_1 (u_{t-3} + u_{t-1} a_{t-2}) = 0, \\
x_0 u_{t-1} + x_1 (u_{t-2} + u_{t-1} a_{t-1}) = 0.
\end{align*}
$$

If $(u_{t-3}, u_{t-2}, u_{t-1}) \neq (0, 0, 0)$, then $P(1, u, 0) \cap L$ is either a point or empty. If $(u_{t-3}, u_{t-2}, u_{t-1}) = (0, 0, 0)$, then the points of $P(1, u, 0) \cap L$ have coordinates

$$(x_0 + x_1 \lambda, x_0 u_0 + (x_0 u_1 + u_0 x_1) \lambda + \cdots + (x_0 u_{t-3} + x_1 u_{t-4}) \lambda^{t-3}, 0),$$

i.e., $P(1, u, 0)$ intersects $L$ in a line.

Then we have $q' - 3$ elements of $S$ intersecting $L$ in a line and exactly one element of $S$ intersecting $L$ in a $(t - 3)$-dimensional subspace. All the other elements of $S$ intersect $L$ in at most one point. Hence, $B$ has size $q^t + q'^{-1} + 1$.

If $n$ is a Rédei line of $B$, by Lemma 2, $P(n)$ intersects $L$ in a $(t - 1)$-dimensional subspace, and $n$ contains every point $(a, b, c)$ of $PG(2, q')$ such that $P(a, b, c)$ intersects $L$ in a subspace containing a line. Hence $X_2 = 0$ is the unique Rédei line of $B$.

**Theorem 4.** Let $t \geq 5$ and let $\lambda$ be a primitive element of $GF(q')$. Let

$$B = \{ (x_0 + x_1 \lambda + \cdots + x_{t-4} \lambda^{t-4}, y_0 + y_1 \lambda, z_0 + z_1 \lambda) \mid x_0, x_1, \ldots, x_{t-4}, y_0, y_1, z_0, z_1 \in GF(q) \}.$$

Then $B$ is a $GF(q)$-linear blocking set of size $q^t + q'^{-1} + 1$ without Rédei lines.

**Proof.** Let $W$ be the set of all vectors of $V$ of the form $(x_0 + x_1 \lambda + \cdots + x_{t-4} \lambda^{t-4}, y_0 + y_1 \lambda, z_0 + z_1 \lambda)$ where $x_0, x_1, \ldots, x_{t-4}, y_0, y_1, z_0, z_1 \in GF(q)$. As $V = \langle W \rangle$ and $W$ is a $GF(q)$-vector space of rank $t + 1$, it defines a $t$-dimensional subspace $L$ of $PG(V, GF(q)) = PG(3t - 1, q)$ not
contained in any subspace $P(l)$ where $l$ is a line of $\pi$. By definition $B = B_L$ is a $GF(q)$-linear blocking set of $P(2, q^t) = PG(2, GF(q^t))$.

Let $m$ be the line $X_2 = 0$. Then $P(m) \cap L$ has dimension $t - 2$. The $(t - 1)$-dimensional subspace $P(1, 0, 0)$ intersects $L$ in a $(t - 4)$-dimensional subspace. A point $(x_0 + x_1 \lambda + \cdots + x_{t-4} \lambda^{t-4}, y_0 + y_1 \lambda, 0)$ of $P(m) \cap L$ belongs to $P(v, 1, 0)$ if and only if there is an element $\beta$ of $GF(q^t)$ such that

$$\beta = y_0 + y_1 \lambda \quad \text{and} \quad (y_0 + y_1 \lambda) v = (x_0 + x_1 \lambda + \cdots + x_{t-4} \lambda^{t-4}).$$

As in Theorem 3, we can prove that there are exactly $q^{t-4}$ elements $P(v, 1, 0)$ intersecting $L$ in a line. All the other elements of $\mathcal{S}$ different from $P(1, 0, 0)$ and contained in $P(m)$ intersect $P(m) \cap L$ in at most one point. Hence, $m$ contains exactly $q^{t-2} + 1$ points of $B$.

If the point $(v, u, 1)$ belongs to $B$, then there is an element $\beta$ of $GF(q^t)$ such that

$$\begin{cases}
\beta = z_0 + z_1 \lambda, \\
(z_0 + z_1 \lambda) u = y_0 + y_1 \lambda, \\
(z_0 + z_1 \lambda) v = x_0 + x_1 \lambda + \cdots + x_{t-4} \lambda^{t-4}.
\end{cases}$$

with $x_0, x_1, \ldots, x_{t-4}, y_0, y_1, z_0, z_1 \in GF(q)$.

Let $v = v_0 + v_1 \lambda + \cdots + v_{t-4} \lambda^{t-4}$ and $u = u_0 + u_1 \lambda + \cdots + u_{t-4} \lambda^{t-4}$. If $P(v, u, 1) \cap L$ contains a line, then the equality $(z_0 + z_1 \lambda) u = y_0 + y_1 \lambda$ implies $u = u_0$.

If $(v_{t-4}, v_{t-3}, v_{t-2}, v_{t-1}) = (0, 0, 0, 0)$, then $(z_0 + z_1 \lambda) v = x_0 + x_1 \lambda + \cdots + x_{t-4} \lambda^{t-4}$ has solution for all $z_0$ and $z_1$ in $GF(q)$, i.e., $P(v, u, 1) \cap L$ is a line.

If $(v_{t-4}, v_{t-3}, v_{t-2}, v_{t-1}) \neq (0, 0, 0, 0)$, then $(z_0 + z_1 \lambda) v = x_0 + x_1 \lambda + \cdots + x_{t-4} \lambda^{t-4}$ has at most $q$ solutions, i.e., $P(v, u, 1) \cap L$ is either a point or empty.

Then, we have exactly $q^t - q^{t-4}$ points $(v, u, 1)$ such that $P(v, u, 1)$ intersects $L$ in a line. For all the other points not incident with $X_2 = 0$ the subspace $P(v, u, 1)$ intersects $L$ in at most one point. As $L \cap P(m)$ has dimension $t - 2$, there are exactly $q^t + q^{t-1} - q^{t-2} - q^{t-3}$ elements of $\mathcal{S}$ not in $P(m)$ and intersecting $L$ in a point and exactly $q^{t-4}$ intersecting $L$ in a line. Then, $B$ has order $q^t + q^{t-1} + 1$.

By way of contradiction, suppose there is a Rédei line $r$ of $B$. By Lemma 2, $P(r) \cap L$ has dimension $t - 1$, and $r$ contains every point $(X_0, X_1, X_2)$ of $PG(2, q^t)$ such that $P(X_0, X_1, X_2)$ intersects $L$ in a subspace containing a line. Then $r$ is incident with the three non-collinear points $(1, 0, 0), (0, 1, 0)$, and $(0, 0, 1)$.

Theorem 4 generalizes the example constructed in Theorem 2 using a regulus for $t > 5$. 


5. EQUIVALENT $GF(q)$ – LINEAR BLOCKING SETS

Let $GF(q) \subset GF(q')$, and let $tr(x) = x + x^q + \ldots + x^{q-1}$ be the trace of $GF(q')$ over $GF(q)$. If $(X_0, X_1, X_2)$ are the homogeneous coordinates of a point of $PG(2, q')$, then $R = \{(z, tr(z), b) | z \in GF(q'), b \in GF(q)\}$ is a small minimal blocking set of $PG(2, q')$ of size $q' + q'^{-1} + 1$ which has $q + 1$ Rédei lines.

**Theorem 5.** Let $B$ be a $GF(q)$-linear blocking set of $PG(2, q')$ of order $|B| \geq q' + q'^{-1} + 1$. If $B$ has at least two Rédei lines then it is equivalent to the blocking set $R$ defined by the trace of $GF(q')$ over $GF(q)$.

**Proof.** Let $B = B_2$ be a $GF(q)$-linear blocking set of $PG(2, q')$. Let $l$ and $m$ be two Rédei lines of $B$. By Lemma 2, $P(l) \cap L$ and $P(m) \cap L$ have dimension $t - 1$. If $x$ denotes the common point of $l$ and $m$, then $T = P(x) \cap L$ has dimension $t - 2$. Hence, all secant lines of $PG(2, q')$ incident with $x$ are Rédei lines of $B$ and $|B| = q' + q'^{-1} + 1$ (see [7, Sect. 5]). If $r$ is a line of $L$ disjoint from $T$, then an element of $\mathcal{S}$ intersects $r$ in at most one point. If both $P(y)$ and $P(z)$ contain a point of $r$, then $\mathcal{S} = \{P(w) | P(w) \cap r \neq \emptyset\}$ is a regulus of the $(2t - 1)$-dimensional subspace $\langle P(y), P(z) \rangle$ and $r$ is a transversal line of $\mathcal{S}$. If $n$ is the line of $PG(2, q')$ joining the points $y$ and $z$, then $\bar{n} = \{n \cap P(a) | P(a) \in \mathcal{S}\}$ is a subline isomorphic to $PG(1, q)$ (see [7]). Hence, we can choose two vectors $w_0$ and $w_1$ in $V$ such that $y = \langle w_0 \rangle$, $z = \langle w_1 \rangle$ and $\bar{n} = \{\langle aw_0 + bw_1 \rangle | a, b \in GF(q), (a, b) \neq (0, 0)\}$. If $x = \langle w_2 \rangle$, then there are $(t - 1)$ elements $\lambda_i \in GF(q')$ such that $w = \langle w_0, w_1, \lambda_1 w_2, \lambda_2 w_2, \ldots, \lambda_{t-1} w_2 \rangle$ is a $(t + 1)$-dimensional $GF(q')$-vector space and $B = \{\langle w \rangle | w \in W^\perp \{0\}\}$.

Let $B'$ be a $GF(q)$-linear blocking set with $q + 1$ Rédei lines incident with the point $x' = \langle w_0' \rangle$ and let $n'$ be a secant line not incident with $x'$. We can choose a basis $w_0', w_1', w_2'$ of $V$ such that $n' \cap B' = \{\langle aw_0' + bw_1' \rangle | a, b \in GF(q')\}$ is a subline of $n'$, and $W' = \langle w_0', w_1', \lambda_1 w_2', \lambda_2 w_2', \ldots, \lambda_{t-1} w_2' \rangle$ is a $(t + 1)$-dimensional $GF(q')$-vector space such that $B' = \{\langle w' \rangle | w' \in W'^\perp \{0\}\}$.

The $GF(q)$-linear blocking sets $B$ and $B'$ are equivalent if and only if there is a collineation of $PG(2, q')$ which maps $B$ to $B'$. As $PFL(2, q')$ is transitive on the points, we can suppose $x = x' = (0, 0, 1)$. A linear collineation of $PG(2, q')$ fixing $x$ is defined by a matrix

$$
\begin{pmatrix}
1 & 0 & x \\
0 & 1 & \beta \\
0 & 0 & 1
\end{pmatrix}
\begin{pmatrix}
1 & 0 & 0 & a & b \\
0 & 1 & 0 & c & d \\
0 & 0 & 1 & \lambda
\end{pmatrix},
$$

where $a, \beta, \lambda, a, b, c, d \in GF(q')$. 

\[\]
The group
\[
\begin{pmatrix}
1 & 0 & x \\
0 & 1 & \beta \\
0 & 0 & 1
\end{pmatrix}, \quad x, \beta \in GF(q^t)
\]
is transitive on the lines of \(PG(2, q^t)\) not incident with \(x\). Then we can suppose \(n=n'\).

The group
\[
\begin{pmatrix}
a & b & 0 \\
c & d & 0 \\
0 & 0 & 1
\end{pmatrix}, \quad ad-bc \neq 0, a, b, c, d \in GF(q^t)
\]
is 3-transitive on the points of \(n\) and it is transitive on the subline of \(PG(1, q^t)\) isomorphic to \(PG(1, q)\). Then, we can suppose \(w_0=w'_0, w_1=w'_1\).

The group
\[
\tau_{\lambda} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \lambda \end{pmatrix}, \quad \lambda \in GF(q^t), \lambda \neq 0
\]
induces the identity on \(n\). Moreover, it induces a cyclic group of order \(q^t-1+\cdots+q+1\) which is sharply transitive on the points of \(P(x)\). Hence, it is transitive on the \((t-2)\)-dimensional subspaces of \(P(x)\) because the points and the hyperplanes of a projective geometry form a symmetric design (see [5] 3.3.2). Therefore there is a non-zero element \(\mu \in GF(q^t)\) such that \(\tau_{\mu}: W \cap \langle w_2 \rangle \mapsto W' \cap \langle w_2 \rangle\). This proves that \(B\) and \(B'\) are equivalent.

Remark. Suppose \(GF(q)\) is the largest subfield of \(GF(q^t)\). If \(t>5\), then \(PG(2, q^t)\) has three inequivalent blocking sets of size \(q^t+q^t-1+1\). The first one has \(q+1\) Rédei lines, the second one has exactly one Rédei line, and the third one has no Rédei lines.

**Corollary 2.** If \(B\) is a small minimal blocking set in \(PG(2, p^n)\) with at least two Rédei lines, then \(B\) is equivalent to the blocking set defined by the trace of \(GF(p^n)\) over some subfield.

**Proof.** By [4, Example 3.1 and Example 3.2] (see also [11]), there is a subfield of order \(q=p^r\) of \(GF(p^n)=GF(q^t)\) and a \((t-1)\)-dimensional \(GF(q)\)-subspace \(U\) of \(GF(q^t)\) such that either \(B\) is equivalent to
\[
\{(u, \alpha, \beta) \mid u \in U, \alpha, \beta \in GF(q)\}
\]
(i.e., $B$ is $GF(q)$-linear), or $q = 2$ and $B$ is equivalent to
$$\{(u + c, 0, 1) | u \in U\} \cup \{(u + c, 1, 0) | u \in U\} \cup \{(u, 1, 1) | u \in U\} \cup \{(1, 0, 0)\},$$
where $c$ does not belong to $U$.

For $q = 2$, the collineation $\omega: (X_0, X_1, X_2) \mapsto (X_0 + c(X_1 + X_2), X_1, X_2)$ maps
$$B = \{(u + c, 0, 1) | u \in U\} \cup \{(u + c, 1, 0) | u \in U\}$$
$$\cup \{(u, 1, 1) | u \in U\} \cup \{(1, 0, 0)\}$$
to the $GF(2)$-linear blocking set
$$B' = \{ (u, \alpha, \beta) | u \in U, \alpha, \beta \in GF(2) \}.$$

Hence, $B = B_L$ is a $GF(q)$-linear blocking set of $PG(2, q')$ such that
$P(1, 0, 0)$ intersect $L$ in a $(t - 2)$-dimensional subspace, and all the secants incident with $(1, 0, 0)$ are Rédéi lines of $B$. Therefore all the elements $P(X_0, X_1, X_2)$ different from $P(1, 0, 0)$ intersects $L$ in at most one point. Hence, $B$ has order $q'^t + q'^{t-1} + 1$. The corollary follows by Theorem 5.  

REFERENCES

6. M. Limbos, A characterisation of the embeddings of $PG(m, q)$ into $PG(n, q')$, J. Geom. 16 (1981), 50–55.
8. G. Lunardon, Linear $k$-blocking sets, Combinatorica, in press.
10. O. Polverino, Small blocking sets in $PG(2, p^n)$, submitted for publication.