Small proper double blocking sets in Galois planes of prime order

Petr Lisoněk*, Joanna Wallis

Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada V5A 1S6

Received 20 October 2006; received in revised form 26 July 2007; accepted 26 July 2007

Available online 6 September 2007

Abstract

A proper double blocking set in PG(2, p) is a set B of points such that 2 ≤ |B ∩ l| ≤ (p + 1) − 2 for each line l. The smallest known example of a proper double blocking set in PG(2, p) for large primes p is the disjoint union of two projective triangles of side (p + 3)/2; the size of this set is 3p + 3. For each prime p ≡ 3 (mod 4) we construct a proper double blocking set with 3p + 1 points, and for each prime p ≥ 7 we construct a proper double blocking set with 3p + 2 points.

Keywords: Blocking set; Double blocking set; Galois plane

1. Introduction

Let PG(2, q) denote the projective plane over Fq, the finite field of order q. A set of points B ⊆ PG(2, q) is called a t-fold blocking set if t ≤ |B ∩ l| for each line l of PG(2, q).

Some applications of blocking sets require that the complement of the blocking set have the same blocking property; see for example [1, Section 8.6] where the application to committee scheduling is mentioned. We say that B ⊆ PG(2, q) is a proper t-fold blocking set if t ≤ |B ∩ l| ≤ (q + 1) − t for each line l of PG(2, q). A (proper) twofold blocking set will be called a (proper) double blocking set.

Blokhuis [2] proved that if p is a prime, then each proper onefold blocking set in PG(2, p) has at least 3(p + 1)/2 points; for odd p this bound is achieved by the projective triangle of side (p + 3)/2. By taking the union of two disjoint such triangles we obtain a proper double blocking set of size 3p + 3 for p > 3. While sporadic examples of proper double blocking sets of size less than 3p + 3 are known for small primes p, it appears that no infinite families of such examples are known presently. The objective of this paper is to provide a construction of proper double blocking sets of size 3p + 1 for all primes p ≡ 3 (mod 4), p ≥ 11, and of size 3p + 2 for all primes p ≥ 7.

No example (sporadic or not) of a twofold blocking set (proper or not) in PG(2, p), p prime, with size less than 3p is known presently, with the exception of a 38-point set in PG(2, 13) discovered recently [3].

At some level our first construction (Theorem 2.2) can be viewed as a certain generalization of the classical construction of the projective triangle of side (p + 3)/2, see for example [4, Lemma 13.6], to the case where the set is created on four lines.

* Corresponding author.

E-mail addresses: plisonek@math.sfu.ca (P. Lisoněk), jwallis@math.sfu.ca (J. Wallis).

1 Research partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).
2. The constructions

Throughout this section, let \( p \) be an odd prime.

For \( x \in \mathbb{F}_p \), we say that \( x \) is a square if \( x = s^2 \) for some \( s \in \mathbb{F}_p \). Otherwise, \( x \) is a non-square. By \( \square_p \), we denote the set of all non-zero squares of \( \mathbb{F}_p \) and by \( \bigcirc \) we denote the set of all non-squares of \( \mathbb{F}_p \). Note that 0 does not appear in either set. Recall that for \( x \in \mathbb{F}_p \) the Legendre symbol \((x/p)\) is defined by \((0/p) = 0\), \((x/p) = 1\) if \( x \in \square_p \) and \((x/p) = -1\) if \( x \in \bigcirc \). For \( p \equiv 3 \pmod{4} \) we have \((-x/p) = -(x/p)\). Other properties of the Legendre symbol which we will use later are \( \sum_{x \in \mathbb{F}_p} (x/p) = 0 \) and \((ab/p) = (a/p)(b/p)\) for all \( a, b \in \mathbb{F}_p \).

**Proposition 2.1.** If \( p \) is a prime such that \( p \equiv 3 \pmod{4} \), then the set

\[
S_p := \{ x \in \mathbb{F}_p \mid x \in \square_p \text{ or } x + 1 \in \bigcirc \}
\]

has cardinality \( \frac{1}{4}(3p - 5) \).

**Proof.** Consider the set

\[
S'_p := \left\{ x \in \mathbb{F}_p \left\| \frac{x}{p} = -1 \text{ and } \frac{x + 1}{p} = 1 \right\} \right.
\]

and note that \( \mathbb{F}_p = S_p \cup S'_p \cup \{0, -1\} \), where \( \cup \) denotes disjoint union.

For \( x \in \mathbb{F}_p \), consider the function

\[
\kappa(x) := \frac{1}{4} \left( 1 - \left( \frac{x}{p} \right) \right) \left( 1 + \left( \frac{x + 1}{p} \right) \right).
\]

For each \( x \in \mathbb{F}_p \setminus \{0, -1\} \) we have \( \kappa(x) = 1 \) if \( x \in S'_p \) and \( \kappa(x) = 0 \) if \( x \notin S'_p \). Since \( S'_p \subset \mathbb{F}_p \setminus \{0, -1\} \), we simply have

\[
|S'_p| = \sum_{x \in \mathbb{F}_p \setminus \{0, -1\}} \kappa(x).
\]

We can evaluate this sum as

\[
\sum_{x \in \mathbb{F}_p \setminus \{0, -1\}} \kappa(x) = \sum_{x \in \mathbb{F}_p \setminus \{0, -1\}} \frac{1}{4} \left( 1 - \left( \frac{x}{p} \right) \right) \left( 1 + \left( \frac{x + 1}{p} \right) \right)
\]

\[
= \frac{1}{4} \left( (p - 2) + (-1) - 1 - \sum_{x \in \mathbb{F}_p \setminus \{0, -1\}} \left( \frac{x}{p} \right) \left( \frac{x - (x + 1)}{p} \right) \right)
\]

\[
= \frac{1}{4} \left( (p - 4) - \sum_{x \in \mathbb{F}_p \setminus \{0, -1\}} \left( \frac{1 + x - 1}{p} \right) \right) = \frac{1}{4}(p - 3).
\]

Thus

\[
|S_p| = |\mathbb{F}_p| - |S'_p| - |\{0, -1\}| = p - \frac{1}{4}(p - 3) - 2 = \frac{1}{4}(3p - 5) \quad \square
\]

Our construction of the proper double blocking set presented in the proof of Theorem 2.2 exhibits parallels to one classical example of a onefold blocking set, namely the projective triangle of side \((p + 3)/2\) (see e.g. [4, Lemma 13.6]). In our case, each point of the set lies on one of 4 lines in a general position. A second similarity consists of exploiting the properties of squares and non-squares in \( \mathbb{F}_p \) in order to achieve the desired blocking property of the set.

By \([a : b : c]\) we will denote the line consisting of the points \((x : y : z)\) such that \(ax + by + cz = 0\).

**Theorem 2.2.** Let \( p \geq 11 \) be a prime such that \( p \equiv 3 \pmod{4} \). There is a proper double blocking set \( B \) in \( \text{PG}(2, p) \) such that \(|B| = 3p + 1\) and each line of \( \text{PG}(2, p) \) intersects \( B \) in at most \( \frac{1}{4}(3p + 7) \) points.
Proof. Let \( I_0 = [1 : 0 : 0], I_1 = [0 : 1 : 0], I_2 = [0 : 0 : 1] \) and \( I_3 = [1 : 1 : 1] \), with indices viewed as elements of \( \mathbb{Z}_4 \).

We will construct \( B \) as a subset of \( I_0 \cup I_1 \cup I_2 \cup I_3 \). Let \( M \) be the projectivity of \( \text{PG}(2, p) \) that maps \( I_i \to I_{i+1} \), \( i \in \mathbb{Z}_4 \).

We have

\[
M = \begin{pmatrix}
1 & 1 & 1 \\
-1 & 0 & 0 \\
0 & -1 & 0
\end{pmatrix}.
\]

The subgroup \( G := \langle M \rangle \) of \( \text{PGL}(3, p) \) is isomorphic to \( Z_4 \). For any point \( u \in \text{PG}(2, p) \) let \( G(u) \) denote the \( G \)-orbit of \( u \). For a point \( (0 : 1 : a) \in I_0 \) we have

\[
G(0 : 1 : a) = \{(0 : 1 : a), (a + 1 : 0 : -1), (a : -(a + 1) : 0), (-1 : -a : a + 1)\}.
\]

Let

\[
B_V := \{I_i \cap I_j \mid 0 \leq i < j \leq 3\}
\]

and notice that

\[
B_V = G(0 : 1 : 0) \cup G(0 : 1 : -1).
\]

For \( a \neq 0 \) we have \( |G(0 : 1 : a)| = 4 \).

Let

\[
B_I := \bigcup_{a \in S_p} G(0 : 1 : a),
\]

where \( S_p \) was defined in (1). Note that \( B_I \cap B_V = \emptyset \). The set \( B \) is now defined as

\[
B := B_I \cup B_V.
\]

Points in \( B_V \) will be called the vertices of \( B \). Throughout this proof it will be useful to write each point of \( B_I \) in the form implied by (2) in order to explicitly determine the \( G \)-orbit to which the point belongs. By Proposition 2.1,

\[
|B| = |B_I| + |B_V| = 4 \cdot \frac{1}{4}(3p - 5) + 6 = 3p + 1.
\]

Next we prove that \( B \) is a proper double blocking set, that is,

\[
2 \leq |l \cap B| \leq (p + 1) - 2
\]

for each line \( l \). We will split this proof into cases according to \( |l \cap B| \).

Note that if \( l \) is not one of the lines \( I_i \) (\( i \in \mathbb{Z}_4 \)) defined above, then from \( B \subset (I_0 \cup I_1 \cup I_2 \cup I_3) \) it follows that \( |l \cap B| \leq 4 < (p + 1) - 2 \). Hence, in each subcase for which \( l \notin \{I_0, I_1, I_2, I_3\} \) it only remains to prove \( |l \cap B| \geq 2 \).

Case (i): \( |l \cap B_V| \geq 2 \). We have \( |l \cap B| \geq 2 \) since \( B_V \subset B \). If \( l \) is one of \( I_i \), then \( |l \cap B| = \frac{1}{4}(3p - 5) + 3 = \frac{1}{4}(3p + 7) \leq (p + 1) - 2 \) since \( p \geq 11 \) by assumption.

In the remaining cases we have \( |l \cap B_V| < 2 \). Since \( |l \cap B_V| = 3 \) for each \( i \in \mathbb{Z}_4 \), for each remaining case we have \( l \notin \{I_0, I_1, I_2, I_3\} \).

Case (ii): \( |l \cap B_V| = 1 \).

Due to (3) and the \( G \)-symmetry of the set \( B \) it is enough to consider the two cases \( l \cap B_V = (0 : 1 : 0) \) and \( l \cap B_V = (0 : 1 : -1) \).

If \( P_{02} := l \cap B_V = (0 : 1 : 0) = I_0 \cap l_2 \), then denote \( P_1 := I_1 \cap l_1 = (b + 1 : 0 : -1) \) and \( P_3 := I_3 \cap l_3 = (-1 : -d : d + 1) \).

If \( P_1 \in B \) then we are done. Otherwise, it must be that \( b \notin S_p \), so \( b \notin \overline{p} \) and \( b + 1 \notin \overline{p} \), since \( b \notin \{-1, 0\} \). From \( \{P_{02}, P_1, P_3\} \subset I \) we get \( d = -b/(b + 1) \) so that \( d \notin \overline{p} \). Thus \( P_3 \in B \).

Similarly if \( l \cap B_V = (0 : 1 : -1) = I_0 \cap l_3 \), then denote \( P_1 := (b + 1 : 0 : -1) = I_1 \cap l_1 \) and \( P_2 := (c : -(c + 1) : 0) = I_2 \cap l_2 \).

If \( P_1 \in B \) then we are done. Otherwise, \( c = -(b + 1)/b \notin \overline{p} \). Thus \( P_2 \in B \).

Case (iii): \( |l \cap B_V| = 0 \).

Let \( P = \{P_0, P_1, P_2, P_3\} \) where \( P_i := I_i \cap l_i \) (\( i \in \mathbb{Z}_4 \)). Due to the \( G \)-symmetry of the set \( B \) it is enough to prove the following two implications: (a) \( P_0, P_1 \notin B \Rightarrow P_2, P_3 \in B \). (b) \( P_0, P_2 \notin B \Rightarrow P_1, P_3 \in B \).
Case (iii)(a): Let $P_0 = (0 : 1 : a)$ and $P_1 = (b + 1 : 0 : -1)$ where $a, b \notin S_p$. Thus $a \in \mathbb{F}_p, a + 1 \in \mathbb{F}_p$, $b \notin \mathbb{F}_p$, and $b + 1 \in \mathbb{F}_p$. Let $P_2 = (c : -(c + 1) : 0)$, $P_3 = (-1 : -d : d + 1)$. From $\{P_0, P_1, P_2\} \subset l$ we get $c = -a(b + 1)/(ab + a + 1)$; note that $ab + a + 1 \neq 0$ since $ab \notin \mathbb{F}_p$ and $-(a + 1) \notin \mathbb{F}_p$. We want to show that $c \in S_p$. If $c \in \mathbb{F}_p$ then we are done. Otherwise, $c \notin \mathbb{F}_p$ and $a(b + 1) \notin \mathbb{F}_p$ together imply $1/(ab + a + 1) \notin \mathbb{F}_p$.

Since $c + 1 = (ab + a + 1)$, we conclude that $c + 1 \notin \mathbb{F}_p$ and so $c \in S_p$ which implies $P_2 \in B$.

From $\{P_0, P_1, P_3\} \subset l$ we get $d = -b/[(b + 1)(a + 1)]$. From $b \notin \mathbb{F}_p$ and $b + 1, a + 1 \in \mathbb{F}_p$ we get $d \in \mathbb{F}_p$. Therefore, $d \in S_p$ and $P_3 \in B$.

Case (iii)(b): Let $P_0 = (0 : 1 : a)$, $P_2 = (c : -(c + 1) : 0)$ where $a, c \notin S_p$. Thus $a \in \mathbb{F}_p, a + 1 \in \mathbb{F}_p, c \in \mathbb{F}_p$, and $c + 1 \in \mathbb{F}_p$. Let $P_1 = (b + 1 : 0 : -1)$ and $P_3 = (-1 : -d : d + 1)$. We want to show that $P_1, P_3 \in B$. From $\{P_0, P_1, P_2\} \subset l$ we get $b = -(c + ac + a)/[a(c + 1)]$ and thus $b + 1 = -c/[a(c + 1)] \notin \mathbb{F}_p$. Therefore, $b \in S_p$ and $P_1 \in B$.

Similarly, we find $d = -(c + ac + a)/(c(a + 1))$. Interchanging $a$ and $c$, the argument is the same as in the previous paragraph. □

The following theorem removes the condition that $p \equiv 3 \pmod{4}$ imposed in the previous theorem; the cardinality of the set increases by 1.

**Theorem 2.3.** Let $p \geq 7$ be a prime. There is a proper double blocking set in $\text{PG}(2, p)$ of size $3p + 2$.

**Proof.** Let $l_0 = [1 : 0 : 0], l_1 = [0 : 1 : 0], l_2 = [0 : 0 : 1]$ and let $H \cong S_3$ be the subgroup of $\text{PGL}(3, p)$ consisting of the six $3 \times 3$ permutation matrices. As in the previous proof, $H(x : y : z)$ will denote the $H$-orbit of the projective point $(x : y : z)$. By $H([a : b : c])$ we will denote the $H$-orbit of the line $[a : b : c]$.

Let

$$T := l_0 \cup l_1 \cup l_2.$$ 

Further let

$$B' := (T \setminus H(0 : 1 : 2)) \cup H(1 : 2 : 3) \cup H(1 : -2 : -2)$$

and

$$B := B' \setminus \{(-2 : -2 : 1)\}.$$ 

We have $|B| = 3p - 6 + 6 + 3 - 1 = 3p + 2$.

We will first show that $B'$ is a proper double blocking set. By noticing the $H$-symmetry of the set $B'$ one quickly realizes that there are exactly four cases (up to symmetry) of lines $l$ such that $|(T \setminus H(0 : 1 : 2)) \cap l| < 2$. These four cases are listed in Table 1. Each row of that table corresponds to one $H$-orbit of lines affected by the removal of $H(0 : 1 : 2)$ from $T$. Each such $H$-orbit is indicated by one representative line $l$ written in the first column; in the second column we verify that $|B' \cap l| \geq 2$ for that line. The proof for the remaining lines in the same orbit follows by symmetry.

Finally, it is clear from the table that the set $B := B' \setminus \{(-2 : -2 : 1)\}$ is still a double blocking set. The fact that $B$ is a proper double blocking set follows from $|B \cap l_i| = p + 1 - 2$ for $i = 0, 1, 2$ and from an easy observation that for each $p \geq 7$ and each $l \notin \{l_0, l_1, l_2\}$ we have $|B \cap l| \leq 5 < (p + 1) - 2$. □

<table>
<thead>
<tr>
<th>$l$</th>
<th>$l \cap B'$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$[2 : 0 : -1]$</td>
<td>$[(1 : 3 : 2), (0 : 1 : 0)]$</td>
</tr>
<tr>
<td>$[1 : 1 : -2]$</td>
<td>$[(1 : 3 : 2), (3 : 1 : 2), (1 : -1 : 0)]$</td>
</tr>
<tr>
<td>$[4 : 1 : -2]$</td>
<td>$[(1 : 2 : 3), (1 : -4 : 0)]$</td>
</tr>
</tbody>
</table>

Table 1

Intersections of $B'$ with lines in special orbits
References