Available online at www.sciencedirect.com
ScienceDirect
Discrete Mathematics 308 (2008) 4052–4056
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

# Small proper double blocking sets in Galois planes of prime order

Petr Lisoněk*, Joanna Wallis[1]

*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 $\mathrm{PG}(2, p)$ is a set $B$ of points such that $2 \leqslant |B \cap l| \leqslant (p+1) - 2$ for each line $l$. The smallest known example of a proper double blocking set in $\mathrm{PG}(2, p)$ 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 $p \geqslant 11$ such that $p \equiv 3 \pmod 4$ we construct a proper double blocking set with $3p+1$ points, and for each prime $p \geqslant 7$ we construct a proper double blocking set with $3p+2$ points.


*Keywords:* Blocking set; Double blocking set; Galois plane

## 1. Introduction

Let $\mathrm{PG}(2, q)$ denote the projective plane over $\mathbb{F}_q$, the finite field of order $q$. A set of points $B \subseteq \mathrm{PG}(2, q)$ is called a *t-fold blocking set* if $t \leqslant |B \cap l|$ for each line $l$ of $\mathrm{PG}(2, q)$.

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 $B \subset \mathrm{PG}(2, q)$ is a *proper t-fold blocking set* if $t \leqslant |B \cap l| \leqslant (q+1) - t$ for each line $l$ of $\mathrm{PG}(2, q)$. 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 $\mathrm{PG}(2, p)$ 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 $p \equiv 3 \pmod 4$, $p \geqslant 11$, and of size $3p+2$ for all primes $p \geqslant 7$.

No example (sporadic or not) of a twofold blocking set (proper or not) in $\mathrm{PG}(2, p)$, $p$ prime, with size less than $3p$ is known presently, with the exception of a 38-point set in $\mathrm{PG}(2, 13)$ 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), jlwallis@math.sfu.ca (J. Wallis).
[1] Research partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

0012-365X/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2007.07.103

## 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 $\not\square_p$ 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 $x \in \not\square_p$. 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*

$$S_p := \{x \in \mathbb{F}_p \mid x \in \square_p \text{ or } x + 1 \in \not\square_p \} \tag{1}$$

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

**Proof.** Consider the set

$$S'_p := \left\{x \in \mathbb{F}_p \,\middle|\, \left(\frac{x}{p}\right) = -1 \text{ and } \left(\frac{x+1}{p}\right) = 1\right\}$$

and note that $\mathbb{F}_p = S_p \sqcup S'_p \sqcup \{0, -1\}$, where $\sqcup$ 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 $x \in \mathbb{F}_p\backslash\{0, -1\}$ we have $\kappa(x) = 1$ if $x \in S'_p$ and $\kappa(x) = 0$ if $x \notin S'_p$. Since $S'_p \subset \mathbb{F}_p\backslash\{0, -1\}$, we simply have

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

We can evaluate this sum as

$$\begin{aligned}\sum_{x\in\mathbb{F}_p\backslash\{0,-1\}} \kappa(x) &= \sum_{x\in\mathbb{F}_p\backslash\{0,-1\}} \frac{1}{4}\left(1 - \left(\frac{x}{p}\right)\right)\left(1 + \left(\frac{x+1}{p}\right)\right)\\ &= \frac{1}{4}\left((p-2) + (-1) - 1 - \sum_{x\in\mathbb{F}_p\backslash\{0,-1\}} \left(\frac{x}{p}\right)\left(\frac{x}{p}\right)\left(\frac{x^{-1}(x+1)}{p}\right)\right)\\ &= \frac{1}{4}\left(p - 4 - \sum_{x\in\mathbb{F}_p\backslash\{0,-1\}} \left(\frac{1+x^{-1}}{p}\right)\right) = \frac{1}{4}(p-3).\end{aligned}$$

Thus

$$|S_p| = |\mathbb{F}_p| - |S'_p| - |\{0, -1\}| = p - \tfrac{1}{4}(p-3) - 2 = \tfrac{1}{4}(3p-5). \qquad \square$$

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 *four* 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 $p \geqslant 11$ be a prime such that $p \equiv 3 \pmod 4$. There is a proper double blocking set $B$ in* PG(2, $p$) *such that $|B| = 3p + 1$ and each line of* PG(2, $p$) *intersects $B$ in at most $\frac{1}{4}(3p + 7)$ points.*