Using theorems of Rédei, and of Brouwer and Schrijver, and Jamison, it is proved that a non-trivial blocking set in a desarguesian projective plane of order $q$ has at least $q + \sqrt{2q} + 1$ points, if $q$ is at least 7, odd and not a square and $q \neq 27$. Further one can show that non-trivial blocking sets in the desarguesian planes $PG(2, 11)$ and $PG(2, 13)$ have at least 18 resp. 21 points, and this is best possible. In addition a nice description of a blocking set of size $q^t + q^{t-1} + 1$ in the desarguesian plane $PG(2, q^t)$ is given, where $q$ is some prime power.

**Introduction**

A blocking set in a linear space is a set $S$ of points, such that each line intersects $S$ in at least one point. $S$ is called *non-trivial*, if no line is completely contained in $S$, in the case of a projective plane. In this note we want to derive lower bounds for the cardinality of $S$.

**Two useful theorems**

The following construction yields interesting blocking sets in the desarguesian plane $PG(2, q)$:

Let $f: GF(q) \to GF(q)$ be any non-linear function. Form a blocking set consisting of

(i) the $q$ points forming the graph of $f$ in $AG(2, q)$,

(ii) the directions determined by $f$ on the line at infinity, say $m$ points.

**Example 1.** Let $q = p$ be a prime, $f(x) = x^{(p+1)}$. This yields a blocking set of $\frac{q(q+1)}{2}$ points, which is conjectured to be best possible ([7], see also [6]).

2. Let $q = q_1^t$ ($t > 1$), then $GF(q_1)$ is a subfield of $GF(q)$. Let $f$ be the trace map from $GF(q)$ to $GF(q_1)$. Then $S = q + q/q_1 + 1$. This is also the best known, if $q_1$ is chosen maximal (compare [2, 4]).

The following theorem gives lower bounds for $m$, where $q = p^n$, $p$ prime.

**Theorem.** ([8, p. 237], see also [6]).

$$m \geq \frac{q}{p^n + 1} + 1, \quad \text{and} \quad m \geq \frac{p + 3}{2} \quad \text{if } n = 1.$$

**Corollary.** Let $X$ be a set of $q$ points in the desarguesian affine plane of order $q$, determining $m$ directions. Then $m$ satisfies the above inequalities.

**Proof.** Either $X$ determines all directions, or there is a parallel class all of whose lines contain exactly 1 point of $X$. 

---

Received 1 June 1984.

1980 *Mathematics Subject Classification* 05B25.

Let $S$ be a minimal blocking set; then each point of $S$ is on at least one tangent. Let $p \in S$ be a point on $t$ tangents, call one tangent $l$, and form a blocking set of $AG(2, q) = PG(2, q) \setminus l$ with $|S| = t + 1 - 1 = t$ points in the obvious way.

**Theorem ([1, 5]).** A blocking set of a desarguesian affine plane $AG(2, q)$ has at least $2q - 1$ points.

As a consequence of this, one has that $t \geq 2q + 1 - |S|$ for each point in $S$. Using these two results it is now a trivial exercise to show that a blocking set in the desarguesian plane $PG(2, 11)$ has at last 18 points, and a rather tedious one to prove $|S| \geq 21$ for $PG(2, 13)$.

**Blocking sets in the desarguesian plane PG(2, q)**

It is well known, and due to Bruen [2], that $|S| \geq q + \sqrt{q} + 1$, with equality if and only if $q$ is a square and $S$ a Baer-subplane. When $q$ is not a square this bound can be improved.

Let $S$ be a blocking set of size $|S| = q + m$. If $S$ contains an $m$-secant the corollary gives a lower bound for the cardinality of $S$. The next theorem treats the remaining case.

**Theorem.** Let $S$ be a blocking set of size $q + m$ without an $m$-secant. Then

$$|S| \geq q + \sqrt{(2q) + 1}.$$  

**Proof.** Since each line contains at most $m - 1$ points of $S$, it follows that each point is on at most $q - 1$ tangents. Counting incident pairs (tangent, point not in $S$) in two ways, using the second theorem, one gets

$$q(q + m)(q - m + 1) \leq (q^2 - m + 1)(q - 1)$$

or, rewriting,

$$2q \leq (m - 1)^2 + (m - 1)/q, \quad \text{whence } m \geq \sqrt{(2q) + 1}.$$  

**Corollary.** Suppose $q$ is odd, not a square, at least 7 and not 27. Let $S$ be an arbitrary non-trivial blocking set of the desarguesian plane $PG(2, q)$. Then $|S| \leq q + \sqrt{(2q) + 1}$.

**Final remarks**

If $q < 7$ everything is known; if $q = 27$ we only get $|S| \geq 35$; if $q = 2^{2t+1}$ one obtains $|S| \geq 2^{2t+1} + 2^{2t+1}$.

The first paper relating Redei’s theorem to blocking sets seems to be [3]. We wonder whether Redei’s theorem can be improved to $m \geq 1 + q/q_1$, where $q_1$ is the order of maximal subfield of GF($q$).

**References**


Techn. University Eindhoven
P.O. Box 513
5600 MB Eindhoven
Netherlands

C.W.I.
Kruislaan 413
1098 SJ Amsterdam
Netherlands