COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA **14** (1) (1994) 111–114

NOTE

ON THE SIZE OF A BLOCKING SET IN $PG(2,p)$

AART BLOKHUIS

Received March 29, 1993
Revised June 12, 1993

We show that the size of a non-trivial blocking set in the Desarguesian projective plane $PG(2,p)$, where p is prime, is at least $3(p+1)/2$. This settles a 25 year old conjecture of J. di Paola.

A *blocking set* in a linear space is a set S of points, such that each line intersects S in at least one point. In the case that the linear space is a projective plane, the blocking set S is called *non-trivial* if no line is completely contained in S. Note that in $PG(2,2)$ every blocking set is trivial. It is well known, and due to Bruen [4], that a non-trivial blocking set in a projective plane of order q has at least $q+\sqrt{q}+1$ points, and this result is best possible in the case that q is a square. If q is not a square and the plane is Desarguesian this bound has been improved independently by Bruen and Silverman [5], and by Brouwer and the author [1] to $q+\sqrt{2q}+1$.

If $q = p$ is an odd prime, then the smallest known examples of non-trivial blocking sets have $3(p+1)/2$ points. An example of such a blocking set is provided by the set of points having homogeneous coordinates $(0,1,-s)$, or a cyclic permutation of this, where s is zero or a square in $GF(p)$. Note that these points all lie on a triangle. In [6] the cardinality of the smallest blocking sets is determined for desarguesian planes of order at most 9. Concerning the above example it is remarked: "It is anticipated that such a triangle is not a minimum blocking coalition for $PG(2,p^n)$ with $n>1$ but may possibly be a minimum for planes of prime order". It was shown in [4, 1] that also for $PG(2,p)$, with $p=11$ or 13, this is true, that is a minimal blocking set has size $3(p+1)/2$ in these cases.

In this note I will show that di Paola's carefully stated conjecture is in fact true for all p.

Theorem. *Let S be a non-trivial blocking set in $PG(2,p)$, where p is an odd prime. Then*

$$|S| \geq 3(p+1)/2.$$

Proof. Let $S = B \cup \{(1,0,0)\}$ be a blocking set of size $p+k+1$, in $PG(2,p)$. We may assume that there is a line meeting S in a single point, since otherwise we may

AMS subject classification code (1991): 05 B 25

delete one or more points from S and still have a blocking set. We take l_∞ (the line with equation $z=0$) to be a tangent of S, so that B is in the affine plane.

Let $B=\{(a_i,b_i)\,|\,i=1,\ldots,p+k\}\subset AG(2,p)$. The set B has at least one point on every non-horizontal line (the horizontal lines are blocked by $(1,0,0)$), so for every $u,t\in GF(p)$ the equation $x+uy+t=0$ has a solution in B, that is, for some i we have $a_i+ub_i+t=0$. It follows that the polynomial

$$F(t,u)=\prod_{i=1}^{p+k}(t+a_i+ub_i).$$

vanishes for all $t,u\in GF(p)$. This implies that F is in the ideal generated by (t^p-t) and (u^p-u), so let us write

$$F(t,u)=(t^p-t)G(t,u)+(u^p-u)H(t,u),$$

where G and H are of total degree k in the variables t and u. Let F_0 denote the part of F that is homogeneous of total degree $p+k$, and let G_0 and H_0 denote the parts of G and H respectively, that are homogeneous of total degree k.

Restricting to the terms of total degree $p+k$ we get

$$F_0=t^pG_0+u^pH_0.$$

where

$$F_0(t,u)=\prod_{i=1}^{p+k}(t+ub_i),$$

The variable u does not play any role anymore since the equation is homogeneous, so let us put $u=1$ and define $f(t)=F_0(t,1)$, $g(t)=G_0(t,1)$ and $h(t)=H_0(t,1)$.

So $f(t)=\prod(t+b_i)$ and $f=t^pg+h$. For a typical factor $t+b_i$ of f we infer that in fact

$$(t+b_i)\mid tg+h.$$

This follows from the fact that $b_i\in GF(p)$ and hence $(t+b_i)\,|\,t^p-t$.

Let us write $f(t)=s(t)r(t)$, where s contains the different linear factors of f each exactly once, and r the rest. We then get $s\,|\,tg+h$ and

$$r\mid f'(t)=t^pg'+h'.$$

Multiplying these two divisibility relations and using $f=s.r$ and also multiplying the right hand side by an additional factor g we get

$$f(t)\mid(tg+h)(t^pg'g+h'g).$$

We may replace the term t^pg in the second factor of the right hand side with $t^pg-f=-h$ without affecting the divisibility property, and after doing that we obtain

$$f\mid(tg+h)(h'g-g'h).$$

The t-degree of the right hand side is at most $1+k+2k-2=3k-1$ (because the coefficient of t^{2k-1} in $h'g$ and $g'h$ is the same) while the t-degree of f equals $p+k$.

It follows that we get $3k-1 \geq p+k$, unless the right hand side vanishes identically. Now $3k-1 \geq p+k$ of course means $k \geq (p+1)/2$ giving the result we want, that is $|S| = p+k+1 \geq 3(p+1)/2$.

Since $tg+h$ is of degree exactly $k+1$ in t it is not zero, so the only way for the right hand side to vanish identically is that $h'g = g'h$. Since p is prime and the degrees of h and g are less than p, the only solution of this differential equation is $h = \alpha g$ for some $\alpha \in GF(p)$. But this implies that

$$f(t) = (t^p + \alpha)g = (t+\alpha)^p g.$$

So there are p b_i's equal to α. But this just means that the horizontal line with equation $y = \alpha$ is part of B, so that S is trivial. ∎

The fact that p is prime is only used to conclude that $h = \alpha g$. The above approach also yields interesting information in the case that the order of the plane is not a prime, namely that $h'g = g'h$. In the case that $q = p^3$ for example this is just enough to conclude that a non-trivial blocking set has size at least p^3+p^2+1, and this is also best possible. This bound was conjectured in [4].

One also obtains some information about the structure of non-trivial blocking sets having the minimal cardinality $3(p+1)/2$. It follows from the divisibility relation, that in this case every point of the blocking set is on exactly $(p-1)/2$ tangents.

Another interesting detail is the fact that the divisibility relation $s \mid tg+h$ implies that the (arbitrary) point $(1,0,0)$ is on at least $q-k$ tangents (assuming it is on at least one tangent). This can be used to give an alternative proof for the result of Jamison and of Brouwer–Schrijver, that a blocking set of the affine plane $AG(2,q)$ has at least $2q-1$ points [7, 3]. Indeed, let S be a blocking set of $AG(2,q)$ of size $q+m$ say. Then adding the point $P = (1,0,0)$ produces a blocking set of $PG(2,q)$, and P is on just one tangent. So $q-m \leq 1$ or $m \geq q-1$.

The methods I have used are very much inspired by ideas in Rédei's book on Lacunary Polynomials [9], and an unpublished manuscript of the author together with Andries Brouwer and Tamás Szőnyi on these matters [2]. In fact this results generalizes Rédei's theorem on the number of directions (or difference quotients) determined by a function $GF(q) \to GF(q)$ in the case that q is prime. This special case of Rédei's theorem was also proved in an elementary way by Lovász and Schrijver [8].

In a sequel to this paper by Brouwer, Szőnyi and the author, the general case, that leads to far more technicalities and where only partial results are available will be discussed, as well as implications of this approach to related problems such as maximal partial spreads and small maximal arcs.

References

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

[2] A. Blokhuis, A. E. Brouwer, and T. Szőnyi: The number of directions determined by a function f on a finite field, *manuscript*.

[3] A. E. BROUWER, and A. SCHRIJVER: The blocking number of an affine space, *J. Combin. Theory (A)* **24** (1978), 251–253.

[4] A. A. BRUEN: Blocking sets in finite projective planes, *SIAM J. Appl. Math.* **21** (1971), 380–392.

[5] A. A. BRUEN, and R. SILVERMAN: Arcs and blocking sets II, *Europ. J. Combin.* **8** (1987), 351–356.

[6] J. DI PAOLA: On minimum blocking coalitions in small projective plane games, *SIAM J. Appl. Math.* **17** (1969), 378–392.

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

[8] L. LOVÁSZ, and A. SCHRIJVER: Remarks on a theorem of Rédei, *Studia Scient. Math. Hungar.* **16** (1981), 449-454.

[9] L. RÉDEI: Lückenhafte Polynome über endlichen Körpern, *Birkhäuser Verlag, Basel (1970).*

Aart Blokhuis

Tech. University Eindhoven
P. O. Box 513,
5600 MB Eindhoven
The Netherlands
aartb@win.tue.nl