On the size of a double blocking set in $PG(2, q)$

Simeon Ball
University of Sussex, Falmer, East Sussex, U.K.

Aart Blokhuis
Techn. University Eindhoven, P.O. Box 513,
5600 MB Eindhoven, The Netherlands

Simeon Ball
MAPS Building
University of Sussex,
Falmer,
East Sussex,
U.K.

Telephone: 44-273-678080
Fax: 44-273-678097

E-mail: S.M.Ball@sussex.ac.uk

Abstract

We obtain lower bounds for the size of a double blocking set in the Desarguesian projective plane $PG(2,q)$. These bounds are best possible for $q < 11$ and in the case q is a square. With the same technique we also exclude certain values for the size of an ordinary minimal blocking set.

1. Introduction

A *double blocking set* in a projective plane Π is a set S of points with the property that every line contains at least two points of S. They are also known as generating sets, a notion due to Laskar and Sherk, who investigated the situation for small planes [11]. Double blocking sets, with the additional condition that they do not contain a line, were introduced and studied by Bruen in [6]. A fundamental combinatorial tool in the study of point sets with restrictions on the possible line intersections are the relations between the numbers of lines intersecting the set in a given number of points. Let τ_i denote the number of i-secants of the set S of cardinality s. Then counting the total number of lines, incident pairs (P, l) with $P \in S$, and triples (P, Q, l) with $P, Q \in S$, we obtain what shall be referred to as the *standard equations*. Here q is the order of the plane, and $m = q + 1$:

$$\begin{aligned} \sum_{i=0}^{m} \tau_i &= q^2 + q + 1; \\ \sum_{i=0}^{m} i\tau_i &= s(q+1); \\ \sum_{i=0}^{m} i(i-1)\tau_i &= s(s-1). \end{aligned}$$

Using the standard equations Bruen obtained the general lower bound $2q + \sqrt{2q} + 2$ for a double blocking set in a projective plane of order $q > 5$.

In the desarguesian plane $PG(2, q)$ it is always possible to obtain a double blocking set of size $3q$, by taking the points on three non-concurrent lines. In the special case that the double blocking set contains a full line, it is impossible to do better. In this case we have that the points outside this line form an ordinary blocking set in the affine plane $AG(2, q)$, obtained by deleting this line (and the points on it) from the plane, and by a well known theorem of Jamison [10], and independently Brouwer and Schrijver [5], such a blocking set has at least $2q - 1$ points. If q is a square, a blocking set of size $2q + 2\sqrt{q} + 2$ can be formed, by taking the union of the point sets of two disjoint Baer subplanes. For $q \neq 4$ this blocking set is smaller than the previous one.

In [14] it was stated that $2q+2\sqrt{q}+2$ is a lower bound for the size of a double blocking set in any (not necessarily desarguesian) plane of order $q > 7$, but the proof is known to be incorrect. It is generally believed that the result is true however, and in this note we prove it for the case of desarguesian planes.

If q is not a square we get an even better bound, in particular when q is prime, but here we seriously doubt that the bound obtained is sharp. The

essential tool in the proof is a theorem about lacunary polynomials. This will be discussed in the next section.

2. Lacunary polynomials

A polynomial in $GF(q)[x]$ is called *fully reducible* if it factors completely into linear factors over $GF(q)$. If in the sequence of coefficients of a polynomial a long run of zeros occurs we call this polynomial *lacunary*. In [13] Rédei studied properties of lacunary polynomials that are fully reducible. The following theorem that we copy together with the proof from [3] is really just a slight generalization of Theorem 24′ in [13]. In the following $q = p^n$, where p is prime.

Theorem 2.1 *Let $f_1 \in GF(q)[x]$ be fully reducible, and suppose that $f_1(x) = x^q g_1(x) + h_1(x)$, where g_1 and h_1 have no common factor. Let $k_1 < q$ be the maximum of the degrees of g_1 and h_1. Let e be maximal such that f_1 (and hence g_1 and h_1) is a p^e-th power. Then we have one of the following:*

1. *$e = n$ and $k_1 = 0$;*
2. *$e \geq n/2$ and $k_1 \geq p^e$;*
3. *$e < n/2$ and $k_1 \geq p^e \lceil (p^{n-e}+1)/(p^e+1) \rceil$;*
4. *$e = 0$, $k_1 = 1$ and $f_1(x) = a(x^q - x)$.*

Note that in particular when q is prime, and $k_1 > 1$ then $k_1 \geq (q+1)/2$.

Proof : Assume $e < n/2$, for the first two possibilities are easily checked. Write $E = p^e$. Let $f_1(x) = f_2(x)^E$ and define g_2 and h_2 similarly. Then extracting E-th roots we get

$$f_2 = x^{q/E} g_2 + h_2.$$

Now write $f_2(x) = s(x)r(x)$ where $s(x)$ contains all different linear factors of f_2 exactly once, and $r(x)$ the rest. The divisibilities $s \mid x^q - x$ and $s \mid f_1 = x^q g_1 + h_1$ imply

$$s \mid x g_1 + h_1.$$

Let f' represent the formal derivative of f. Since $r \mid f_2'$ and $r \mid f_2$ it follows that $r \mid f_2' g_2 - g_2' f_2$, whence since $(x^{q/E})' = 0$

$$r \mid h_2' g_2 - g_2' h_2.$$

Note that since $(g_1, h_1) = 1$ and g_2 and h_2 are not both p-th powers, the right-hand-side does not vanish. Combining these two divisibility relations we get

$$f_2(= rs)|(xg_1 + h_1)(h_2'g_2 - g_2'h_2).$$

Now if $xg_1 + h_1 = 0$ then we get $k_1 = 1$, since $(g_1, h_1) = 1$, and f_1 has the desired form. Otherwise the degree of the left hand side is at most equal to that of the right hand side. Consider first the case that $\deg g_1 = k_1 = Ek_2$. This implies that

$$q/E + k_2 \leq 1 + Ek_2 + 2k_2 - 2.$$

Note that the highest order term of $h_2'g_2 - h_2g_2'$ always cancels if $\deg h_2 = \deg g_2 = k_2$. Hence

$$k_2 \geq \frac{q/E + 1}{E + 1}.$$

The other case ($\deg g_1 < \deg h_1 = k_1$) is similar and gives the same conclusion. (Only the case $\deg g_1 \geq \deg h_1$ will be used in later proofs.) □

We now consider in a bit more detail the case that $q = p^{2d}$ is a square, and $e = d = n/2$. Note that in this case either $k_1 = p^e = \sqrt{q}$, or $k_1 \geq 2\sqrt{q}$. For the first case, the situation arising after extracting the p^e-th root is considered in the following theorem.

Theorem 2.2 *Let $f(x) \in GF(q)[x]$ be of the form $x^{\sqrt{q}}(x+b)+(cx+d)$, with $d \neq bc$. Then f is fully reducible if and only if $c = b^{\sqrt{q}}$ and $d \in GF(\sqrt{q})$.*

Proof : Assume first that f is fully reducible. Now we show that f has no multiple factors. Indeed, $f'(x) = x^{\sqrt{q}} + c$, so that $f(x) - (x + b)f'(x) = d - bc \neq 0$. It follows that f divides

$$f^{\sqrt{q}} \bmod (x^q - x) = x(x^{\sqrt{q}} + b^{\sqrt{q}}) + c^{\sqrt{q}}x^{\sqrt{q}} + d^{\sqrt{q}}.$$

Consequently since the degrees of f and $f^{\sqrt{q}} \bmod (x^q - x)$ are equal the implication in the lemma follows.

To see the converse, assume $f = x^{\sqrt{q}}(x+b)+xb^{\sqrt{q}}+d = N(x+b)-N(b)+d$, where N be the norm function from $GF(q)$ to $GF(\sqrt{q})$. N is a $\sqrt{q}+1 \to 1$ function from $GF(q)^*$ to $GF(\sqrt{q})^*$. Since f has order $\sqrt{q}+1$ and x is a zero of f precisely when $N(x+b) = N(b) - d \neq 0$, the inverse implication follows. □

Some remarks about this situation are in order. The field $GF(q) \cup \{\infty\}$ can be identified with the projective line $PG(1, q)$. It contains the Baer subline $GF(\sqrt{q}) \cup \{\infty\}$. The other Baer sublines are images of this subline under the

group $PGL(2,q)$. The collection of all Baer sublines forms a 3-$(q+1, \sqrt{q}+1, 1)$ design (also known as a Möbius plane, or an inversive plane). The zeros of a function f as above form a Baer subline not through the point ∞, and conversely, to every Baer subline l not containing ∞ correspond $b \in GF(q)$ and $a \in GF(\sqrt{q})^*$, such that

$$l = \{x \in GF(q) \mid N(x+b) = a\}.$$

This can all be checked by direct calculations.

The following properties of a Baer subline will be used as well.

1. The intersection of a dual Baer subline with a line is a Baer subline.
2. Two Baer sublines intersect in at most 2 points.
3. If one has two points and two dual Baer sublines through these points so that the line joining the two points belongs to both dual Baer sublines, then the intersection of the lines of these Baer sublines contain a Baer subplane.

3. Double blocking sets

Using the results in the previous section we are now able to prove the following.

Theorem 3.1 *Let S be a double blocking set in $PG(2,q)$.*

1. *If $q > 16$ is a square then $|S| \geq 2q + 2\sqrt{q} + 2$.*
2. *If $3 < q = p^{2d+1}$ then $|S| \geq 2q + p^d \lceil (p^{d+1}+1)/(p^d+1) \rceil + 2$.*

Proof : (Compare with [2].) We construct a polynomial that satisfies the conditions of Theorem 2.1, and then consider each of the four cases arising from it.

Construction of the polynomial. Without loss of generality take the points $U_0 = (1,0,0)$ and $U_1 = (0,1,0)$ to be in S. Moreover assume that the line l_∞ with equation $z = 0$ is a 2-secant of S. Every point lies on a 2-secant since, as we are trying to prove lower bounds, we take S to be minimal. Let $|S| = 2q + k + 2$. Let $B = S \setminus \{U_0, U_1\}$. Write $B = \{(a_i, b_i) \mid i = 1, \ldots, 2q+k\} \subset AG(2,q)$.

The set B has at least two points on every non-horizontal or non-vertical line (the horizontal lines are blocked once by $(1,0,0)$, the verticals once by

$(0,1,0)$). So for every $u,t \in GF(q)$, $u \neq 0$, the equation $x+uy+t=0$ has two solutions in B; that is, for two i we have $a_i+ub_i+t=0$. For $u=0$ there is always at least one solution. It follows that the polynomial

$$F(t,u) = u\prod_{i=1}^{2q+k}(t+a_i+ub_i).$$

vanishes "twice" for all $t,u \in GF(q)$. Theorem 1.3 in [8] implies that F is in the ideal generated by $(t^q-t)^2$, $(t^q-t)(u^q-u)$ and $(u^q-u)^2$.

So it can be written in the form

$$F(t,u) = (t^q-t)^2G(t,u) + (t^q-t)(u^q-u)H(t,u) + (u^q-u)^2J(t,u).$$

Here G, H and J are of total degree $k+1$ in t and u. Let F_0 denote the part of F that is homogeneous of total degree $2q+k+1$, and let G_0, H_0 and J_0 denote the parts of G, H and J respectively, that are homogeneous of total degree $k+1$.

Restricting to those terms of total degree $2q+k+1$ implies

$$F_0 = t^{2q}G_0 + t^qu^qH_0 + u^{2q}J_0,$$

where

$$F_0(t,u) = u\prod_{i=1}^{2q+k}(t+ub_i).$$

The variable u does not play any further role since the equation is homogeneous. So put $u=1$ and define $f(t)=F_0(t,1)$, $g(t)=G_0(t,1)$, $h(t)=H_0(t,1)$ and $j(t)=J_0(t,1)$. Hence $f(t)=\prod(t+b_i)$ and $f=t^{2q}g+t^qh+j$. By definition each factor of f corresponds to a point on a horizontal line. Note that g has degree only k in t and j has degree at most $k+1$. Since there is at least one point of B on every horizontal line, we get that f is divisible by t^q-t, so we must have (assuming $k<q-2$)

$$f(t) = (t^q-t)(t^qg(t) - \frac{j(t)}{t}).$$

The polynomial $t^qg(t)-j(t)/t$ satisfies the conditions in Theorem 2.1, after dividing through by the greatest common divisor of g and j/t, if necessary (this possibly reduces k). So let us divide by this greatest common divisor and let the result be $f_1 = t^qg_1+h_1$, with $k \geq k_1 = \deg g_1 \geq \deg h_1$.

Case 1 of Theorem 2.1. f_1 contains a factor of the form $t^q-a=(t-a)^q$, in addition to the factor $t-a$ already present in t^q-t. This however gives too many factors $t-a$ in f.

Case 4 of Theorem 2.1. Since in our situation the degree of g_1 is not less than the degree of h_1, this case cannot occur.

Case 3 of Theorem 2.1. If q is not a square, that is $q = p^{2d+1}$, then $e \leq d$ and the desired bound is obtained. If q is a square, $q = p^{2d}$, we want to prove that $k \geq 2p^d$. In case 3 $e \leq d-1$, and

$$k_1 \geq p^{d-1}\lceil \frac{p^{d+1}+1}{p^{d-1}+1} \rceil.$$

And so $k_1 \geq 2\sqrt{q}$ unless $(p^{d+1}+1)/(p^{d-1}+1) \leq 2p-1$, and one immediately verifies that this can only happen for $q = 4, 9$ or 16. In these cases one only gets $k \geq 3$, 5, and 6 respectively (we will come back to this problem in the next section).

Case 2 of Theorem 2.1. If q is not a square, that is $q = p^{2d+1}$, then $k \geq p^{d+1}$ which is better than the desired bound. So let q be a square, $q = p^{2d}$.

If $e > d$ then $k_1 \geq 2\sqrt{q}$; so we may assume $e = d$. We repeat the remark preceding Theorem 2.2, that is, either $k_1 = p^d$ or $k_1 \geq 2p^d$. It suffices now to show that $k_1 = p^d = \sqrt{q}$ is impossible.

If $e = d$ and $k = p^e$ then after extracting the p^e-th root from $t^q g_1 + h_1$, a fully reducible function of the form $t^{\sqrt{q}}(t+b) + (ct+d)$ is obtained. Theorem 2.2 implies that this function is of the form $N(t+b) - N(b) + d$. The zeros of this are precisely the points of a Baer subline of $GF(q) \cup \{\infty\}$, not containing ∞. This means that among the lines through $(1,0,0)$ having more than 2 points of S there are $\sqrt{q}+1$ having at least $\sqrt{q}+2$ points, forming a dual Baer subline. There is however nothing special about the point $(1,0,0)$, so this situation occurs in every point.

Call the lines meeting S in at least $\sqrt{q}+2$ points *long lines*. Notice that two long lines meet in a point of S, for otherwise we get by counting points of S on the lines through the intersection point that $|S| \geq 2(q-1) + 2(\sqrt{q}+2) = 2q + 2\sqrt{q} + 2$.

Next observe that the intersection of S with a long line l contains a Baer subline. Indeed, let P be any point of S not on l. The long lines on P contain a dual Baer subline, and they all meet l in a point of S. In fact a much stronger property holds: if Q is an arbitrary point of S on l then l contains a Baer subline in S not containing Q. To see this it suffices to take for P any point such that PQ is a 2-secant.

Now two Baer sublines meet in at most 2 points. So a little reflection shows that (for $q \geq 9$) all long lines have at least $2\sqrt{q}$ points, and this implies $|S| \geq 1 + (\sqrt{q}+1)(2\sqrt{q}-1) + (q-\sqrt{q}) = 3q$; this is certainly bigger than $2q + 2\sqrt{q} + 2$. □

4. Small planes

In Theorem 3.1 the condition $q > 16$ was imposed and the obvious question is whether this restriction is really necessary. The problem here is that for q equal to 9 and 16 the lower bound on k in Theorem 2.1, case 3, is not large enough to carry us beyond $2\sqrt{q}$. In this section we shall investigate the small planes more closely. The following observation will be crucial in our considerations:

Suppose S is a double blocking set of size $2q+k+2$ where k equals $p^e\lceil(p^{n-e}+1)/(p^e+1)\rceil$, where $e = d$ if $n = 2d+1$ and $e = d-1$ if $n = 2d$ (and in this case $q \leq 16$). Then all lines intersect S in 2 (mod p^e) points, moreover, if no round-off error has been made, then every point of S is on exactly $q-k$ two-secants.

To see this, note that the lower bound on k always comes from Theorem 2.1, case 2 or 3. First of all, g and j/t have no common divisor. This means that really all factors of f have multiplicity 1 (mod p^e) and hence all lines through $(1,0,0)$ have 2 (mod p^e) points of S.

If no round-off error has been made, then equality also implies that the degree of s in the proof of Theorem 2.1 equals $1+k$. But this tells us that the number of different factors in $t^q g - j/t$ is exactly $1+k$. Hence there are precisely this number of lines through $(1,0,0)$ that are not 2-secants. So we have precisely $q-k$ two-secants through $(1,0,0)$ and hence through every point.

An important additional observation is the following. Suppose that k differs from the above lower bound by exactly one. Then g and j/t have precisely one common linear factor. This implies that all lines through a fixed point of S, apart from precisely one, have 2 (mod p^e) points.

Now let us look at small planes. For orders 2 and 3 the bounds for S are 6 and 9. For the plane of order 4 the complement of a unital is a double blocking set of size 12, and this again is best possible. For $q = 5$ we get the bound $|S| \geq 15$ from the theorem and this is best possible. For $q = 7$ however we only get $|S| \geq 20$, but it is known that in fact 21 is a lower bound in this case. This was first proved in [9]. Let us show how it follows from our observations.

If S is a double blocking set in $PG(2,7)$ of size 20, then no round-off error has been made; so we see that every point of S is on precisely 3 two-secants. This gives us a total of 30 two-secants. Let l be a line intersecting S in the maximal number, t say, of points. If $t = 8$ or 7 then S has to have at least 21 points. If $t = 6$ or 5 we can count the number of 2-secants exactly, this number being $6\times3+2\times7 = 32$ and $5\times3+3\times6 = 33$ respectively, in both cases more than 30. If $t = 4$ in the same way the lower estimate $4\times3+4\times5 = 32$ is obtained, so $t = 3$ and we can again count exactly and obtain $5\times4+3\times3 = 29$.

For $PG(2,8)$ we get $|S| \geq 22$. In [12] it was shown that in fact $|S| > 22$ and $|S| \geq 24$ was obtained in [1] by using the binary code generated by the plane (and this is of course realizable).

We can obtain the same bound by using the following argument. If the size of S is 22 then every line intersects S in an even number of points. The standard equations give only one solution that is $\tau_2 = 54$, $\tau_4 = 12$ and $\tau_6 = 7$. By considering the degree of s in Theorem 2.1 we have that each point of S is on either 4 or 5 bisecants. This implies that each point of S is on either one or two 6-secants. Since $\tau_6 = 7$ and two 6-secants must meet in a point of S, we have that S has 21 points, a contradiction.

If $|S| = 23$, then our additional observation gives us that through every point S there is exactly one line with an odd number of points. At most 7 such lines exist altogether, but since $|S|$ is odd, all points outside S are also on an odd-secant. The odd-secants therefore form a dual blocking set, but there are too few of them.

The next case is $PG(2,9)$. From the proof of Theorem 3.1 it follows that S has size at least 25, but we want to show that it has at least 26 points. Now $|S| = 25$ implies $k = 5$ and we have equality in the bound (without round-off error). Therefore every point of S lies on exactly $q-k = 4$ two-secants. In the same way as for $q = 7$ a contradiction will be obtained. The total number of 2-secants equals $25 \times 4/2 = 50$. Let l be a t-secant of S, with t maximal. We immediately get $t \leq 7$. If t is 7 or 6 the number of 2-secants can be computed exactly; counting them on every point of the line l we get $7 \times 4 + 3 \times 9 = 55$ and $6 \times 4 + 4 \times 8 = 56$. If $t = 5$ or 4 we get lower bounds for the number of 2-secants, 55 and 52 respectively. Hence $t = 3$ and we can compute everything using the standard equations. Again we get a contradiction.

The next plane is $PG(2,11)$. The bound in Theorem 3.1 gives 30, but again it is possible to improve this to 31 using the fact that in this case every point is on exactly 5 two-secants (this is done exactly as before). To know the truth in this case would be very interesting, because one of the authors conjectures that a double blocking set in $PG(2,p)$ has at least $3p$ points, and this is the first open case.

The reader may amuse himself by verifying that also for $q = 13, 17$ and 19 the lower bound can be increased by 1.

Finally we consider $PG(2,16)$. The arguments from Theorem 3.1 give a lower bound of size 40 only, corresponding to $k = 6$ and $e = 1$. In this case every line has an even number of points, and every point of S is on 10 two-secants. Reasoning as before we get that S has at most 6 collinear points, and now the standard equations do not have a (non-negative) solution. This raises the

bound to 41, and we proceed as in the case of $PG(2,8)$. By our additional observation every line contains an even number of points, apart from exactly one through each point of S. Now since S has odd size, the lines intersecting S in an odd number of points form a dual blocking set. On the other hand, since every point of S is on exactly one such line, and all of them have more than 2 points, there are at most 13 lines like this. This is far too few lines to form a dual blocking set.

5. Ordinary blocking sets

In this final section we look at the implication of Theorem 2.2 for the possible sizes of (ordinary) minimal blocking sets in desarguesian planes of square order. Apart from the line (the trivial blocking set) a blocking set S in $PG(2,q)$ has size at least $q+\sqrt{q}+1$ and equality occurs if and only S consists of the points of a Baer subplane.

It was shown by Bruen and Silverman [7], that other minimal blocking sets are substantially larger. We are able to improve their bound, but this is certainly not the best possible result.

Theorem 5.1 *Let S be a minimal blocking set in $PG(2,q)$, $16 < q = p^{2d}$ a square, S not a line nor a Baer subplane. Then*

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

Proof : We start the proof similarly to that of Theorem 3.1, or better, as in [2]. So, assume that $U_0 = (1,0,0)$ is in S, that the line l_∞ with equation $z = 0$ is a tangent, and that S has size $q+k+1$. Let B be the set of points in S that are in the affine plane $PG(2,q) \setminus l_\infty$.

$$B = \{(a_i, b_i) \mid i = 1, \ldots, q+k\}.$$

The set B has at least one point on every non-horizontal line (the horizontal lines are blocked by $(1,0,0)$). It follows that the polynomial

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

vanishes for all $t, u \in GF(q)$, and we may write

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

Let F_0 denote the part of F that is homogeneous of total degree $q+k$, and let G_0 and H_0 denote the parts of G and H that are homogeneous of total degree k.

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

$$F_0 = t^q G_0 + u^q H_0.$$

where

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

We 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 $f(t)=\prod(t+b_i)$; that is, f is fully reducible, and $f=t^q g+h$. So divide again by the greatest common divisor of g and h to obtain $f_1 = t^q g_1 + h_1$. We wish to prove that $k \geq 2p^d$.

The situation is now exactly the same as at the end of the proof of Theorem 3.1. We skip the details and arrive at the conclusion immediately:

If $k < 2p^d = 2\sqrt{q}$, then among the lines through $(1,0,0)$ there are $\sqrt{q}+1$ having at least $\sqrt{q}+1$ points, and they form a dual Baer subline. In fact we have this situation in every point.

Let us now call lines meeting S in at least $\sqrt{q}+1$ points *long lines*. Again, two long lines meet in a point of S, for otherwise we get by counting points of S on the lines through the intersection points, that $|S| \geq (q-1)+2(\sqrt{q}+1) = q+2\sqrt{q}+1$.

We observe again that the intersection of S with a long line l contains a Baer subline. Indeed, let P be any point of S not on l. The long lines on P contain a dual Baer subline, and they all meet l in a point of S. We now use property 3 of Baer sublines given after the proof of Theorem 2.2 to conclude that S contains a complete Baer subplane. Since S is minimal S in fact equals this subplane. □

There is an alternative combinatorial arguement for the last part of the proof, suggested by Tamas Szönyi. Assume that we have a minimal blocking set with cardinality less than $q+2\sqrt{q}+1$. From the lacunary polynomial approach it follows that the point-degrees (with respect to long lines) are $\sqrt{q}+1$. Counting the long lines using a long line we get that the total number of long lines is $|D|\sqrt{q}+1$, where $|D|$ is the size of a long line. Hence all long lines have the same cardinality, and this is $\sqrt{q}+1$, since there are lines having this cardinality. Then, by counting incident point-line pairs, we get that the number of long lines is equal to the number of points. Hence the number of points is $(\sqrt{q}+1)\sqrt{q}+1$, i.e. we have a Baer-subplane. The same idea also works for double blocking sets. There the point degrees are $\sqrt{q}+1$ and the cardinality of the long lines is $\sqrt{q}+2$, if we start from a double blocking set with cardinality less than $2q+2\sqrt{q}+2$. Now counting incident point-line pairs gives a contradiction.

We finish by looking at the small planes. For $q = 4$ minimal blocking sets exist of sizes 7,8 and 9 and for $q = 9$ there does not exist a blocking set of size 14, by a result of Bruen and Silverman. Size 15 is possible however. For $q = 16$ the bound of the theorem can be obtained; that is, a blocking set, not a Baer subplane or a line, in $PG(2, 16)$ has size at least 25. To see this we have to rule out the possible sizes 23 and 24. If the size is 23, then $k = 6$ and we are in case 3 of Theorem 2.1 with equality (and $e = 1$). It follows that all lines intersect the blocking set in an odd number of points, and that there are precisely 230 tangents. If there is a 7-secant then all the numbers turn out to be correct; however in this case the blocking set is of so-called Rédei type, and it was shown in [4] that this is not possible. So we only have 1,3 and 5-secants, and using the standard equations, we can solve everything. It turns out that the number of tangents is 233 in the solution, but we know already that the number should be exactly 230.

Size 24 is dealt with using the same trick as before. In this case we must again be in case 3 of Theorem 2.1, and now we have lost a linear factor in dividing by the greatest common divisor. This implies that through every point of S there is a unique line intersecting S in an even number of points. Since S has even size, the lines meeting S in an even number of points form a dual blocking set, and we see that there are at most 12 of them. This is again way too small.

□

References

[1] J. Bierbrauer, (k, n)-arcs of maximal size in the plane of order 8. Unpublished manuscript, (1988).

[2] A. Blokhuis, On the size of a blocking set in $PG(2, p)$. *Combinatorica*, **14** (1994), 111–114.

[3] A. Blokhuis, Blocking sets in Desarguesian planes, *in* "Paul Erdös is Eighty", Vol. 2 (eds: D. Miklós, V.T. Sós and T. Szönyi), Bolyai Soc. Math. Studies, (1993), 1–20.

[4] A. Blokhuis, A.E. Brouwer and T. Szőnyi, The number of directions determined by a function f on a finite field. *J. Combin. Theory Ser.A*, to appear.

[5] A.E. Brouwer and A. Schrijver, The blocking number of an affine space. *J. Combin. Theory Ser.A* **24** (1978), 251–253.

[6] A.A. Bruen, Arcs and multiple blocking sets. *Combinatorica, Symposia Mathematica* **28**, Academic Press, (1986), 15–29.

[7] A.A. Bruen and R. Silverman, Arcs and Blocking Sets II. *European. J. Combin* **8** (1987), 351–356.

[8] A.A. Bruen, Polynomial multiplicities over finite fields and intersection sets. *J. Combin. Theory Ser.A* **60** (1991), 19–33.

[9] Z. Ciechanowicz, PhD Thesis. University of London, (1980).

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

[11] R.C. Laskar and F.A. Sherk, Generating sets in finite projective planes, *in* "Finite geometries", (eds.: C.A. Baker and L.M. Batten), Lecture notes in pure and applied mathematics 103, Marcel Dekker, New York, Basel, (1985), 183–197.

[12] J.R.M. Mason, On the maximum sizes of certain (k, n)-arcs in finite projective geometries. *Math. Proc. Cambridge. Philos. Soc.* **91** (1982) 153–169.

[13] L. Rédei, "Lückenhafte Polynome über endlichen Körpern. " Birkhäuser Verlag, Basel, 1970.

[14] M.J. de Resmini, On 2-blocking sets in projective planes. *Ars Combin* **20B** (1985), 59–69.