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

Simeon Ball
University of Sussex

Simeon Ball
School of Mathematical and Physical Sciences,
University of Sussex,
Brighton BN1 9QH,
U.K.

SIMEON BALL: TRIPLE BLOCKING SETS

Abstract

Lower bounds are obtained for the size of a triple blocking set in the Desarguesian projective plane $PG(2,q)$. These bounds are best possible for $q < 11$ and in the case $q > 121$ is an odd square.

1. Introduction

A *t-fold blocking set* in a projective plane Π is a set S of points with the property that each line contains at least t points of S. A 1-fold blocking set is known as a blocking set and is defined with the extra condition that it should contain no line. If $t = 2$ or 3 such sets are known as double or triple blocking sets respectively. Multiple blocking sets are simply complements of (k, n)-arcs in projective planes with $n + t = q + 1$. There is a direct link between (k, n)-arcs and optimal linear codes and hence a link between multiple blocking sets and optimal linear codes. Indeed there exists a projective $[s, 3, d]$ code over $GF(q)$ if and only if there exists a $(s, s - d)$-arc in $PG(2, q)$ if and only if there exists a $q^2 + q + 1 - s$ point $(q + 1 - s + d)$-fold blocking set in $PG(2, q)$.

Blocking sets have been well studied previously and a survey of results can be found in [3]. Double blocking sets have not been studied as much but lower bounds on their existence, some of which are sharp, appear in [1].

This paper, however, is concerned with the case $t = 3$. Some properties of triple blocking sets of type $(3, n)$ were derived by de Resmini [8]. Hill and Mason [5] provided examples of triple blocking sets of size $4q - 1$ for q even and $4q$ for q odd. In the case when q is square then the union of three disjoint Baer subplanes forms a triple blocking set in $PG(2, q)$ of size $3q + 3\sqrt{q} + 3$ which is smaller for $q > 16$. It will be shown that for $q > 121$, an odd square, triple blocking sets in $PG(2, q)$ must have at least $3q + 3\sqrt{q} + 3$ points. If q is not a square then an even better bound is obtained in most cases but this is unlikely to be sharp. As in [1], [2] the theory of lacunary polynomials is used to obtain these results.

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 [7] Rédei studied properties of lacunary polynomials that are fully reducible. The following theorem copied together with its proof from [3] is really just a slight generalization of Theorem 24$'$ in [7]. In the following $q = p^h$, where p is prime.

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

1. *$e = h$ and $m = 0$;*

2. *$e \geq h/2$ and $m \geq p^e$;*

3. *$e < h/2$ and $m \geq p^e \lceil (p^{h-e}+1)/(p^e+1) \rceil$;*

4. *$e = 0$, $m = 1$ and $f(x) = a(x^q - x)$.*

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

Proof : Assume $e < h/2$, for the first two possibilities are easily checked. Write $E = p^e$. Let $f(x) = f_1(x)^E$ and define v_1 and w_1 similarly. Then extracting E-th roots we get

$$f_1 = x^{q/E} v_1 + w_1.$$

Now write $f_1(x) = s(x)r(x)$ where $s(x)$ contains all different linear factors of f_1 exactly once, and $r(x)$ the rest. Since $s \mid x^q - x$ and $s \mid f = x^q v + w$ these imply

$$s \mid xv + w.$$

Since $r \mid f_1'$ and $r \mid f_1$ these imply $r \mid f_1' v_1 - v_1' f_1$ or

$$r \mid w_1' v_1 - v_1' w_1.$$

Note that $(v, w) = 1$ and v_1 and w_1 are not both p-th powers, so the right hand side does not vanish. Combining these two divisibility relations we get

$$f_1 (= rs) | (xv + w)(w_1' v_1 - v_1' w_1).$$

Now if $xv + w = 0$ then $m = 1$ since $(v, w) = 1$, and f has the desired form. Otherwise the degree of the left hand side is at most equal to that of the right hand side. First consider the case that $\deg v = m = Em_1$. In this case

$$q/E + m_1 \leq 1 + Em_1 + 2m_1 - 2.$$

Hence

$$m_1 \geq \frac{q/E + 1}{E + 1}.$$

The other case ($\deg v < \deg w = m$) is similar and gives the same conclusion. $\square$

Now consider in a bit more detail the case that $q = p^{2d}$ and $e = d = h/2$. Note that in this case either $m_1 = 1$, $m_1 = 2$ or $m \geq 3\sqrt{q}$. For the first case when $m_1 = 1$, f_1 is a polynomial of the same type as in the following theorem. This theorem also appears in [1].

Theorem 2.2 *Let $f(x) \in GF(q)[x]$, q a square, 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

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

Since the degrees of left-hand-side and right-hand-side are equal the statement follows.

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

Next consider the case when $m_1 = 2$. If f_1 has no multiple factors then the following theorem gives a useful form the polynomial must take.

Theorem 2.3 *Let $f(x) \in GF(q)[x]$ be of the form $x^{\sqrt{q}}(x^2+bx+c) + dx^2 + ex + a$. If f is a fully reducible polynomial with no multiple factors then one of the following holds:*

1. $f(x) = (x^2+bx+c)(x^{\sqrt{q}} + d)$;
2. $f(x) = (x+b)(x^{\sqrt{q}+1} + e)$;
3. $f(x) = (x + cd^{-\sqrt{q}})[N(x + d^{\sqrt{q}}) + d^{\sqrt{q}}(ac^{-1} - d)]$.

Note that in all cases this implies that if $f(x) = x^{\sqrt{q}}v(x) + w(x)$ where $f(x)$ has no multiple factors and is fully reducible, $v(x)$ is of degree two and $w(x)$ is of degree at most two, then $v(x)$ and $w(x)$ have a common factor. In the latter case $(x + cd^{-\sqrt{q}})$ is a factor of $v(x)$ since $b = d^{\sqrt{q}} + cd^{-\sqrt{q}}$ and hence is also a factor of $w(x)$.

Proof : Since f is fully reducible and contains no multiple factors it follows that

$$f | f^{\sqrt{q}} \bmod (x^q - x) = x(x^{2\sqrt{q}} + b^{\sqrt{q}}x^{\sqrt{q}} + c^{\sqrt{q}}) + d^{\sqrt{q}}x^{2\sqrt{q}} + e^{\sqrt{q}}x^{\sqrt{q}} + a^{\sqrt{q}}.$$

By long division form a polynomial $\theta(x)$ where
$f\theta = f^{\sqrt{q}} \bmod (x^q - x)$. Then

$$\theta(x) = x^{\sqrt{q}-1} + (d^{\sqrt{q}} - b)x^{\sqrt{q}-2} - (b(d^{\sqrt{q}} - b) + c)x^{\sqrt{q}-3} +$$

$$(b^2(d^{\sqrt{q}} - b) + bc - c(d^{\sqrt{q}} - b))x^{\sqrt{q}-4} + ... + a^{\sqrt{q}-1}$$

and by equating coefficients of terms of order $x^{\sqrt{q}-1}$ and $x^{\sqrt{q}-2}$ the following two equations are obtained.

$$a + e(d^{\sqrt{q}} - b) - db(d^{\sqrt{q}} - b) - dc = 0 \qquad (1)$$

$$(d^{\sqrt{q}} - b)(a - eb + db^2 - dc) - ec + dbc = 0 \qquad (2)$$

It can be deduced from these that $c = 0$ if and only if $d = 0$ and this implies $f(x) = (x + b)(x^{\sqrt{q}+1} + e)$.

So assume that cd is non-zero. By substituting $(d^{\sqrt{q}} - b)(e - bd) = dc - a$ from (1) into (2) deduce that $e = c^{-1}(ba + (d^{\sqrt{q}} - b)(a - dc))$.

Substituting for e back into (1) implies that either $a = dc$ or $b = d^{\sqrt{q}} + cd^{-\sqrt{q}}$. If $a = dc$ then (2) implies that $e = bd$ and hence that $f(x) = (x^2+bx+c)(x^{\sqrt{q}}+d)$. The latter case implies that $e = ad^{\sqrt{q}}c^{-1} + dcd^{-\sqrt{q}}$ and it can then be deduced that $f(x)$ is of the form $f(x) = (x+cd^{-\sqrt{q}})[N(x+d^{\sqrt{q}})+d^{\sqrt{q}}(ac^{-1}-d)]$. $\square$

3. Triple blocking sets

The following lemmas will also be needed in the case when q is a square.

Lemma 3.1 *($q > 9$ a square) Let B be a triple blocking set in $PG(2, q)$ such that through each of its points there are $\sqrt{q} + 1$ lines, containing at least $\sqrt{q} + 3$ points of B and forming a dual Baer subline. Then B has at least $3q + 2\sqrt{q} + 3$ points.*

Proof : Call the lines meeting B in $\sqrt{q} + 3$ or more points *long lines.* If two long lines meet outside of B then B has at least $2(\sqrt{q} + 3) + 3(q - 1) = 3q + 2\sqrt{q} + 3$ points and the desired bound is obtained. So assume two long lines meet in B.

Take l, a long line, and P, a point of B not on l. Then the long lines through P contain a dual Baer subline and meet l in a Baer subline. Let Q be a point on this Baer subline. Consider long lines through a point on a 3-secant to Q. These meet l in another Baer subline not containing Q. Two Baer sublines meet in at most 2 points and so l has at least $2\sqrt{q}$ points. Since l was arbitrary, every long line has at least $2\sqrt{q}$ points and it follows that B has at least $1 + (\sqrt{q} + 1)(2\sqrt{q} - 1) + 2(q - \sqrt{q}) = 4q - \sqrt{q}$ points. $\square$

Lemma 3.2 *($\sqrt{q} > 12$, q a square) Let B, a triple blocking set in $PG(2, q)$, have through every point at least $\sqrt{q}+1$ lines, containing at least $\sqrt{q}+3$ points* *of B and forming a dual Baer subline. Then B has at least $3q+3\sqrt{q}+3$ points.*

Proof : Assume that B has less than $3q+3\sqrt{q}+3$ points. Call the lines meeting B in $\sqrt{q}+3$ or more points *long lines*. Take nine points of B all lying on a long line l. There are at least $9\sqrt{q}(\sqrt{q}+2)$ points of $B\setminus l$ lying on the long lines through these nine points, counting with multiplicity. Since $B\setminus l$ has less than $3q+2\sqrt{q}$ points there exist more than $9\sqrt{q}(\sqrt{q}+2)-3(3q+2\sqrt{q})=12\sqrt{q}$ points on four or more of the long lines through these nine points, counting with multiplicity.

Let P_i be a point of $B\setminus l$ joined to at least four of these nine points of l by long lines. Let S_i be the points of l where the long lines through P_i meet l. The set S_i has at most $\sqrt{q}+2$ points otherwise P_i lies on at least $\sqrt{q}+3$ long lines and B has at least $(\sqrt{q}+3)(\sqrt{q}+2)+2(q-\sqrt{q}-2)+1=3q+3\sqrt{q}+3$ points. Also S_i contains a Baer subline b_i by hypothesis.

Since there exists $12\sqrt{q}$ points of $B\setminus l$ (counting with multiplicity) meeting at least 4 of the nine points, there exists $12\sqrt{q}$ points whose corresponding b_i meet at least 3 of the nine points.

There are 84 different sets of three points among these nine points and so there are points P_1 and P_2 whose corresponding b_1 and b_2 meet in at least three points. Since two Baer sublines meet in at most two points, b_1 and b_2 are the same.

If three long lines meet in a point outside of B then B has at least $3(\sqrt{q}+3)+3(q-2)=3q+3\sqrt{q}+3$ points. So at most 2 long lines meet in a point outside of B. This implies that the long lines through P_1 and P_2 meet l in at most one point outside of B and that point lies on the long line joining P_1 and P_2.

Let S be the set of points of $l\cap B$ where $b_1=b_2$ meet $l\cap B$, then S has $\sqrt{q}$ or $\sqrt{q}+1$ points.

We shall now prove that l has at least $\sqrt{q}+5$ points. Assume firstly that it has less than $\sqrt{q}+5$ points. Let T be the set of points in $B\setminus l$ that lie on a non-long line meeting S. By considering the points on non-long lines through a point of S it follows that there are at least $2(q-\sqrt{q}-1)$ points in T.

Suppose that l has exactly $\sqrt{q}+3$ points of B. The long lines through a point of T can meet at most 2 points of S and so at most 5 points of $l\cap B$. This follows from the fact that two different Baer sublines meet in at most 2 points. Let n be maximal such that n points of T are collinear. Each point of B lies on at least $\sqrt{q}+1$ long lines and so each point of T has at least

$\sqrt{q}-4$ long lines meeting $l \setminus B$. There are $q+1-(\sqrt{q}+3)$ points in $l \setminus B$ and so $n(\sqrt{q}-4) \le q-\sqrt{q}-2$ which implies $n \le \sqrt{q}+4$ for $\sqrt{q} > 9$.

Now since every point of T has at least $\sqrt{q}-4$ long lines meeting l outside B and at most $\sqrt{q}+4$ of them are collinear it follows that

$$2(q-\sqrt{q}-1)\frac{(\sqrt{q}-4)}{(\sqrt{q}+4)} \le q-\sqrt{q}-2 < q-\sqrt{q}-1.$$

For $\sqrt{q} > 12$, since l was arbitrary, every long line contains at least $\sqrt{q}+4$ points of B. Now if $\sqrt{q}+2$ of these long lines meet in a point then $|B| \ge 1+(\sqrt{q}+2)(\sqrt{q}+3)+2(q-\sqrt{q}-1) = 3q+3\sqrt{q}+5$. So assume every point of B lies on exactly $\sqrt{q}+1$ long lines.

Let l be a line meeting exactly $\sqrt{q}+4$ points of B. Define S, T and n as before. A point of T has at most 2+3 of its long lines meeting $l \cap B$, since two points of T cannot have their long lines agreeing on l. (Of course it is possible for one of the points of T to have long lines meeting all 4 points of $(l \cap B) \setminus S$ but then all the other points of T have at most 2+2 long lines meeting $l \cap B$ and future bounds would be even better).

Therefore $n(\sqrt{q}-4) \le q-\sqrt{q}-2$ as before and

$$2(q-\sqrt{q}-1)\frac{(\sqrt{q}-4)}{(\sqrt{q}+4)} \le q-\sqrt{q}-3 < q-\sqrt{q}-1.$$

For $\sqrt{q} > 12$, since l was arbitrary, it has now been shown that every long line has at least $\sqrt{q}+5$ points. By counting the points of B on lines through a point of B it follows that $|B| \ge 1+(\sqrt{q}+1)(\sqrt{q}+4)+2(q-\sqrt{q}) = 3q+3\sqrt{q}+5$ and the result follows.

$\square$

Lemma 3.3 ($\sqrt{q} > 12$, *q a square*) *Let B be a triple blocking set in $PG(2,q)$ such that each of its points is one of the following:*

1. *The meet of a secant of length $2\sqrt{q}+3$ or more and $\sqrt{q}$ secants of length at least $\sqrt{q}+3$.*
2. *The meet of two secants of length $2\sqrt{q}+3$ or more and $\sqrt{q}-2$ secants of length at least $\sqrt{q}+3$.*
3. *The meet of at least $\sqrt{q}+1$ lines, that meet B in at least $\sqrt{q}+3$ points, and contain a dual Baer subline.*

Then B has at least $3q + 3\sqrt{q} + 3$ points.

Proof : Call the points of type *3 special points*, secants of length $2\sqrt{q} + 3$ or more *very long lines* and secants of length at least $\sqrt{q} + 3$ *long lines.* If every point of B is a special point then Lemma 3.2 implies B has at least $3q + 3\sqrt{q} + 3$ points. So assume β, the number of very long lines, is non-zero and hence that B has at least $3q + 2\sqrt{q} + 3$ points. Assume B has less than $3q+3\sqrt{q}+3$ points, which immediately implies that very long lines meet long lines and other very long lines in B.

Assume that every very long line has exactly $2\sqrt{q}+3$ points. There exists at least $3q + 2\sqrt{q} + 3 - (2\sqrt{q} + 3)\beta + \beta(\beta - 1)/2$ special points. Consider l a very long line and P a special point. We will show that l has at least $2\sqrt{q}+4$ points.

The long lines through P meet $l \cap B$ in a set containing a Baer subline. For each Q on this Baer subline there exists another Baer subline in $l \cap B$ not containing Q. This is since there exists a special point on a 3-secant through Q. Indeed, the long lines through Q contain at most $\sqrt{q}(\sqrt{q} + 2 - \beta/2)$ special points and this is always less than the total number of special points. Therefore $l \cap B$ splits into 2 disjoint Baer sublines and a point or l has at least $3\sqrt{q} - 3$ points. So by assumption $l \cap B$ splits into 2 disjoint Baer sublines and a point.

(Note if the long lines through Q have more than $\sqrt{q} + 3$ points then they could meet more special points, but this would simply imply that B is equally larger and so the difference between the total number of special points and the number of special points that the long lines through Q can meet remains constant.)

Take Q_1, a point of type *1*, and Q_2, a point of type *2*, in seperate Baer sublines in $l \cap B$. If every point is of type *1* then $\beta = 1$ and take two points of type *1*. If every point is of type *2* then $\beta = 2\sqrt{q} + 4$ and take two points of type *2*.

The long lines through Q_1 meet at most $\sqrt{q}(\sqrt{q}+2-(\beta-1)/2)$ special points. The long lines through Q_2 meet at most $(\sqrt{q}-2)(\sqrt{q}+3-\beta/2)$ special points. This implies, by subtraction from the total number of special points, there are $\frac{1}{2}(\beta - \sqrt{q} - \frac{9}{2})^2 + \frac{1}{2}q - 6\sqrt{q} - \frac{9}{8}$ special points joined to Q_1 and Q_2 by 3-secants. This number is greater than zero for $\sqrt{q} > 12$. By considering the intersection of the long lines through one of these special points with l it follows that l has at least $3\sqrt{q} - 3$ points, since they meet $l \cap B$ in a Baer subline not containing Q_1 or Q_2 and 2 different Baer sublines meet in at most 2 points.

In the extreme cases $\beta = 1$ and $\beta = 2\sqrt{q} + 4$ similar arguments hold and we have that there are $q - 4\sqrt{q}$ and $q - 7\sqrt{q} - 7$ special points, respectively, joined to Q_1 and Q_2 by 3-secants.

We have now shown there exists a very long line with more than $2\sqrt{q} + 3$ points. This implies there are at least $(2\sqrt{q}+4)\sqrt{q}-2(\beta-1)$ long lines. Long lines meet in at most $\sqrt{q}+2$ in a point otherwise $|B| \geq 1+(\sqrt{q}+3)(\sqrt{q}+2)+2(q-\sqrt{q}-2) = 3q+3\sqrt{q}+3$. If a long line has $\sqrt{q}+3$ points it meets at most $(\sqrt{q}+3)(\sqrt{q}+1)+q-\sqrt{q}-2-2(\beta-1) = (2\sqrt{q}+4)\sqrt{q}-2(\beta-1)-\sqrt{q}+1$ long lines. So every long line has at least $\sqrt{q}+4$ points. Counting the points of B on the lines through a point of type *1* or *2* implies B has more than $3q + 3\sqrt{q} + 3$ points. □

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

Theorem 3.4 *Let B be a triple blocking set in $PG(2,q)$.*

1. *If $121 < q$ is an odd square then $|B| \geq 3q + 3\sqrt{q} + 3$.*
2. *If $8 < q = p^{2d+1}$ then $|B| \geq 3q + p^d\lceil(p^{d+1}+1)/(p^d+1)\rceil + 3$.*
3. *If $16 < q$ is an even square or $q = 25$, 49, 81 or 121 then $|B| \geq 3q + 2\sqrt{q} + 3$.*

Proof : (Compare with [2] and [1].) 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. Let l, the line $z = 0$ be a 3-secant to a triple blocking set B. Assume $(1,0,0) \in B$ and that B has $3q + m + 3$ points. Let $S = B \setminus l$ and note that S has $3q + m$ points. Assume $m < q - 3$ since otherwise $|B| \geq 4q$. In coordinates

$$S = \{(a_i, b_i) | i = 1, ..., 3q + m\} \subset AG(2,q) = PG(2,q) \setminus l.$$

Let d_1 and d_2 be the directions determined by the points in $B \cap (l \setminus (1,0,0))$. That is, for each $P_j \in B \cap (l \setminus (1,0,0))$, let d_j be the negative reciprocal of the slope of the lines meeting in P_j, $(j = 1,2)$. Then each line $x + uy + t = 0$ has three solutions in S whenever $u \neq d_1$ or d_2 and two solutions otherwise. So the function

$$F(t,u) = (u - d_1)(u - d_2) \prod_{i=1}^{3q+m} (t + a_i + b_i u)$$

has zeros of degree three for all t and u and therefore lies in the ideal generated by $(t^q-t)^3$, $(t^q-t)^2(u^q-u)$, $(t^q-t)(u^q-u)^2$ and $(u^q-u)^3$.

So it can be written in the form

$$F(t,u)=(t^q-t)^3G(t,u)+(t^q-t)^2(u^q-u)I(t,u)+$$
$$(t^q-t)(u^q-u)^2J(t,u)+(u^q-u)^3K(t,u).$$

The polynomials G, I, J and K are of total degree at most $m+2$ in t and u. Let F_0 denote the part of F that is homogeneous of total degree $3q+m+2$, and define G_0, I_0, J_0 and K_0 similarly.

Restricting to terms of total degree $3q+m+2$ only implies

$$F_0=t^{3q}G_0+t^{2q}u^qI_0+t^qu^{2q}J_0+u^{3q}K_0,$$

where

$$F_0(t,u)=u^2\prod_{i=1}^{3q+m}(t+ub_i).$$

The variable u does not play any further role since the equation is homogeneous. So put u=1 and define $f(t)=F_0(t,1)$ and define g and k similarly. Note that g has degree only m in t. Since there are at least two points of S on every horizontal line, f is divisible by $(t^q-t)^2$ and hence

$$f(t)=(t^q-t)^2(t^qg(t)+h(t)+\frac{k(t)}{t^2}).$$

The degree of $h(t)$ is at most $m+2<q-1$. The divisibility $t^q|(f(t)-k(t))$ implies that $t^{q-2}|h(t)$ and therefore $h(t)=\alpha t^{q-2}$. If α is non-zero then $F(t,u)$ has a term of order $t^{3q-2}u^q$ and so $|S|\geq 4q-4$ and $|B|\geq 4q-1$. Also if q is odd then $F(t,u)$ has a term $t^{2q-1}u^{2q}$ and so $|S|\geq 4q-3$ and $|B|\geq 4q$.

So assume α is zero and define $z(t)$ to be the polynomial formed after dividing $t^qg(t)+k(t)/t^2$ by the greatest common divisor of g and k/t^2, this possibly reduces m.

Case 1 of Theorem 2.1. $z(t)$ contains a factor of the form $t^q-a=(t-a)^q$. In addition to the $(t-a)^2$ present in the $(t^q-t)^2$, this gives too many factors $t-a$ in $f(t)$.

Case 4 of Theorem 2.1. Since the degree of g is not less than the degree of k/t^2 this case cannot occur.

Case 3 of Theorem 2.1. If q is not a square, then $q=p^{2d+1}$, $e\leq d$ and so the bound is obtained. If q is a square then $q=p^{2d}$, $e\leq d-1$, and

$$m\geq p^{d-1}\lceil(p^{d+1}+1)/(p^{d-1}+1)\rceil.$$

This implies $m \geq 3\sqrt{q}$ unless $(p^{d+1}+1)/(p^{d-1}+1) \leq 3p-1$ which can only occur if q is even or $q = 9$, 25 or 81.

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

If $e > d$ then $m \geq 2\sqrt{q}$ for q even and $m \geq 3\sqrt{q}$ otherwise; so assume $e = d$. This implies $m = \sqrt{q}$, $m = 2\sqrt{q}$ or $m \geq 3\sqrt{q}$. Since $m \geq 3\sqrt{q}$ implies the desired bound is obtained assume $m = \sqrt{q}$ or $m = 2\sqrt{q}$.

If $m = \sqrt{q}$ then Theorem 2.2 implies that $z(t)$ is a $\sqrt{q}$-th power of a function of the form $N(t+b) - N(b) + d$. The zeros of this are precisely the points of a Baer subline. This means among the lines through (1,0,0) having more than 3 points of B there are $\sqrt{q}+1$ of them, having at least $\sqrt{q}+3$ points, forming a dual Baer subline.

If $m = 2\sqrt{q}$ then the situation after taking $\sqrt{q}$-th roots in Theorem 2.1 is that in Theorem 2.3. This implies $z(t)$ must have multiple factors since any common factor has been removed from g and k/t^2. This implies (1,0,0) lies on a secant of length $2\sqrt{q}+3$ or more. The degree of s in Theorem 2.1 is $q/E + 2 - m_1 = \sqrt{q}$ so there are this many non 3-secants through (1,0,0). Therefore (1,0,0) lies on at most two secants with at least $2\sqrt{q}+3$ points of B, or we get the desired bound.

Consider a point lying on a secant of length $3\sqrt{q}+3$ or more and $\sqrt{q}-1$ secants of length at least $\sqrt{q}+3$. This implies there are at least $(3\sqrt{q}+3)(\sqrt{q}-1) = 3q-3$ long lines by counting the long lines meeting the secant of length $(3\sqrt{q}+3)$ or more. If there exists a long line with at most $\sqrt{q}+4$ points of B then it can meet at most $(\sqrt{q}+4)(\sqrt{q}+2) + q - \sqrt{q} - 3 = 2q + 5\sqrt{q} + 5$ other long lines. This, however, is too few and so every long line has at least $\sqrt{q}+5$ points of B. Now by counting the points of B on lines through a point on the secant of length $3\sqrt{q}+3$ or more implies B has at least $(3\sqrt{q}-2) + (\sqrt{q}-1)(\sqrt{q}+4) + 1 + 2(q - \sqrt{q}+1) = 3q + 4\sqrt{q} + 1$ points. Hence assume there is no secant of length $3\sqrt{q}+3$ or more.

Since there exist no secants of length $3\sqrt{q}+3$ or more and (1,0,0) was chosen arbitrarily every point of B is of type *1*, *2* or *3* of Lemma 3.3. Applying Lemma 3.3 implies that, for $\sqrt{q} > 12$, B has at least $3q + 3\sqrt{q} + 3$ points. If q is even or $\sqrt{q} < 12$ then $m = 2\sqrt{q}$ implies the desired bound immediately. So every point is of type *3* of Lemma 3.3 and by applying Lemma 3.1 we can deduce B has at least $3q + 2\sqrt{q} + 3$ points.

4. Small planes

Now consider the situation for small planes. In $PG(2,5)$ and $PG(2,7)$ it is not possible to make the initial assumption that $m < q-3$ since the latter bounds obtained for m are greater in these cases. So it follows that $m \geq q-3$ and hence B has at least $4q$ points, which is always attainable, as mentioned before. These bounds were first proved in [6] and [4] respectively.

For $q = 8$ the lower bound obtained for the size of a triple blocking set from Theorem 3.4 is 31. It was shown in [5] that a 31 point triple blocking set exists and that this is the smallest triple blocking set in $PG(2,8)$.

For $q = 9$ either $m \geq 2\sqrt{q}$, and therefore B has at least $4q = 36$ points, or we are in Case 3 of Theorem 2.1 or, Case 2 of Theorem 2.1 with $m = \sqrt{q}$. In Case 3 of Theorem 2.1 the bound obtained is $m \geq 5$. So assume $m = 5$ and that B has exactly 35 points. This implies that the degree of s in Theorem 2.1 is equal to 6 and since this is the number of non 3-secants through a point of B, there are exactly four 3-secants through each point. Hence there exist 35.4/3 such lines, but this number is not an integer.

If $m = \sqrt{q}$ and we are in Case 2 of Theorem 2.1 then each long line meets at least 6 points of B. If 5 long lines meet in a point or two long lines meet outside of B, then B has at least 36 points. So a long line with 6 points meets at most 18 other long lines. If a long line had 7 points of B it would meet at least 21 other long lines and so every long line would have at least 7 points. This implies B has more than 36 points. Each line must therefore meet B in at least 3 and at most 6 points. But the diophantine equations imply from this that B has at least 39 and at most 42 points. Hence B has at least 36 points.

For $q = 11$ the bound in Theorem 3.4 implies that B has at least 42 points. In this case the degree of s in Theorem 2.1 is exactly 7 and so the number of 3-secants through a point of B is exactly five. Let r be the total number of 3-secants. By counting the number of 3-secants through a point it is shown that $r = 5.42/3 = 70$. Let t be the length of the longest secant to B. If $t = 12$ then counting the 3-secants intersecting this line there are exactly sixty 3-secants. If $t = 11$ or 10 then by considering a point on the longest secant not in B and counting, B must have at least 44 or 43 points respectively. If $t = 9$ then by counting 3-secants again implies that $r = (9.5) + (3.11) = 78$. If $t = 8$ then counting as before gives $r = (8.5) + (4.10) = 80$. If $t = 7$ then considering lower bounds gives $r \geq (7.5)+(5.9) = 80$. If $t = 6$; again $r \geq (6.5)+(6.8) = 78$ which is too many. If $t = 5$ then $r \geq (5.5) + (7.7) = 74$. If $t = 4$ the number of 3-secants can be calculated exactly and is $r = (4.5) + (8.6) = 68$ which is not equal to 70 and hence is a contradiction. This raises the bound to 43 but no triple blocking sets are known with less than 44 points in them.

In exactly the same way it is possible to raise the bound in Theorem 3.4 to 50 for $q = 13$ but there are no known examples of triple blocking sets with less than 52 points.

In Theorem 3.4 it was not possible to prove $m \geq 2\sqrt{q}$ for $q = 16$ since in Case 2 of Theorem 2.1 it is implied that $m_1 \geq 3$ and $e = 1$ and hence that $m \geq 6$. Assume that $m_1 = 3$ and that $m = 6$ and hence that B has 57 points. These imply that the degree of s in Theorem 2.1 is exactly 7 and so every point of B is on exactly ten 3-secants. As in the case for $q = 11$ it is possible to show that there are 190 secants of length 3 and by considering the length of the longest secant gain a contradiction.

This raises the bound to 58. Now if B has exactly 58 points then $m_1 = 3$ and $e = 1$ and since B differs from the bound these values give by exactly one, there must have been exactly one common factor removed from v and w in Theorem 2.1. This implies each point of B lies on secants of length $3 + np$ (some n) except exactly one. This is the same reasoning as was used in [1]. Each point outside of B lies on a secant of even length since there are 17 lines through a point and B has an even number of points. So the secants of even length form a dual blocking set. There are at most 58/4 of them and this is nowhere near enough. So a triple blocking set in $PG(2, 16)$ must have at least $3q + 2\sqrt{q} + 3 = 59$ points.

For $PG(2, 17)$ Theorem 3.4 gives a lower bound of 63. It is again possible to improve this by one by the same arguement as was used for $PG(2, 11)$. The bound of 64 is unlikely to be sharp however and no known examples exist with less than 68 points.

Combining the discussion in this section with Theorem 3.4 the following has been proved.

Theorem 4.1 *Let B be a triple blocking set in $PG(2, q)$.*

1. *If $q = 5$, 7 or 9 then B has at least $4q$ points and if $q = 8$ then B has at least 31 points.*
2. *If $q = 11$, 13 or 17 then $|B| \geq (7q + 9)/2$.*
3. *If $17 < q = p^{2d+1}$ then $|B| \geq 3q + p^d\lceil(p^{d+1} + 1)/(p^d + 1)\rceil + 3$.*
4. *If $4 < q$ is an even square or $q = 25$, 49, 81 or 121 then $|B| \geq 3q + 2\sqrt{q} + 3$.*
5. *If $121 < q$ is an odd square then $|B| \geq 3q + 3\sqrt{q} + 3$.*

References

[1] S. Ball and A. Blokhuis, On the size of a double blocking set in $PG(2,q)$, preprint.

[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. *Paul Erdös is Eighty, Volume 2 (eds: D. Miklós, V.T. Sós and T. Szönyi), Bolyai Soc. Math. Studies.*, to appear.

[4] Z. Ciechanowicz, Ph.D. Thesis, University of London, 1980.

[5] R. Hill and J. R. M. Mason, On (k,n)-arcs and the falsity of the Lunelli-Sce conjecture, in: London Math. Soc. Lecture Note Series 49, CUP, (1981), 153–168.

[6] L. Lunelli and M. Sce, Considerazioni arithmetiche e resultati sperimentali sui $\{k;n\}_q$ archi. *Ist Lombardo Accad. Sci. Rend.* A **98** (1964), 3–52.

[7] L. Rédei, *Lückenhafte Polynome über endlichen Körpern.* Birkhäuser Verlag, Basel, 1970.

[8] M. J. de Resmini, On 3-blocking sets in projective planes. *Ann. Discrete. Math.* **34**, (1987), 145–152.