Special Issue (2003), S245–S253

Advances in Geometry

Blocking sets in PG(2, p) for small p, and partial spreads in PG(3, 7)

Aart Blokhuis, Andries E. Brouwer and Henny A. Wilbrink

Dedicated to Professor Adriano Barlotti on the occasion of his 80th birthday

Abstract. We find all minimal blocking sets of size $\frac{3}{2}(p+1)$ in PG$(2,p)$ for $p<41$. There is one new sporadic example, for $p=13$. We find all maximal partial spreads of size 45 in PG$(3,7)$.

1 Minimal nontrivial blocking sets in PG(2, p)

A *blocking set* in a projective plane is a set of points meeting all lines. It is called *nontrivial* when it does not contain a line. An *m-secant* of a set is a line meeting the set in precisely m points.

Blokhuis [2] shows that in a Desarguesian projective plane PG$(2,p)$ of prime order p, a nontrivial blocking set has size at least $\frac{3}{2}(p+1)$, and, moreover, that in case of equality each point of the blocking set lies on precisely $\frac{1}{2}(p-1)$ tangents (1-secants).

Nontrivial blocking sets of size $\frac{3}{2}(p+1)$ exist for all p. Indeed, an example is given by the *projective triangle*: the set consisting of the points $(0,1,-s^2)$, $(1,-s^2,0)$, $(-s^2,0,1)$ with $s\in\mathbb{F}_p$.

No nontrivial blocking set of size $q+m$ in PG$(2,q)$ can have a k-secant for $k>m$, and in particular such a set of size $\frac{3}{2}(p+1)$ in PG$(2,p)$ cannot have a k-secant with $k>\frac{1}{2}(p+3)$. The *triangle* has three $\frac{1}{2}(p+3)$-secants. Conversely, Lovász and Schrijver [10] show that any nontrivial blocking set of size $\frac{3}{2}(p+1)$ with a $\frac{1}{2}(p+3)$-secant must be projectively equivalent to the *triangle*. (They put the given secant at infinity and show that the remaining p affine points can be taken to be the points $(a,a^{(p+1)/2})$ for $a\in\mathbb{F}_p$.)

A blocking set S in PG$(2,q)$ is called *of Rédei type* when there is a line L such that $|S\backslash L|=q$. Thus, we know the blocking sets of Rédei type meeting the Blokhuis bound in PG$(2,p)$, p prime. Let us call a nontrivial blocking set in PG$(2,p)$ that meets the Blokhuis bound *sporadic* if it is not of Rédei type. A single sporadic blocking set (in PG$(2,7)$) was known. Here we find a second sporadic blocking set (in PG$(2,13)$) and show that no other sporadic blocking sets exist in PG$(2,p)$, $p<41$.

2 The Blokhuis bound

Theorem 2.1 ([2]). *Let S be a nontrivial blocking set in* $\mathrm{PG}(2,p)$, *p prime. Then* $|S| \geqslant \frac{3}{2}(p+1)$. *If equality holds, then each point of S lies on precisely* $\frac{1}{2}(p-1)$ *tangents.*

Proof. Let $S = \{(a_i, b_i, c_i) \mid i = 1, \ldots, q+m\}$ be a minimal blocking set in $\mathrm{PG}(2,q)$, where q is a power of the prime p. The polynomial $F(X,Y,Z) = \prod_i (a_i X + b_i Y + c_i Z)$ vanishes in all points (x,y,z), hence can be written as

$$F(X,Y,Z) = A(X,Y,Z)(X^q - X) + B(X,Y,Z)(Y^q - Y) + C(X,Y,Z)(Z^q - Z).$$

Since $F(X,Y,Z)$ is homogeneous, all low degree terms cancel, and we have $F(X,Y,Z) = A_0(X,Y,Z)X^q + B_0(X,Y,Z)Y^q + C_0(X,Y,Z)Z^q$, where F has degree $q+m$ and A_0, B_0, C_0 have degree m. Assume that $|S| < 2q$, so that no cancellation takes place between the terms on the right hand side.

Let the line $Z = 0$ contain l points of S, and assume that $(1,0,0) \in S$. Now divide by X and substitute $X = 0$, $Y = 1$ to get $f(Z) = b(Z) + c(Z)Z^q$ where f has degree $q + m - l$ and factors completely, and c has degree $m - l$ and b has degree at most $m - 1$. Write $f(Z) = s(Z) \cdot r(Z)$ where s contains every irreducible factor of f just once, and r contains the repeated factors. Then $s \mid (b + cZ^q)$ and $s \mid (Z^q - Z)$ so $s \mid (b + cZ)$. And $r \mid f' = b' + c'Z^q$, so that $f = rs \mid (b + cZ)(b' + c'Z^q)$, and hence $f \mid (b + cZ)(b'c - bc')$.

If the factors on the right are nonzero, it follows that $q + m - l \leqslant 2(m-1) + m - l - 1$ that is, $m \geqslant (q+3)/2$. And in case of equality the degree of s equals the degree of $b + cZ$ so that $(1,0,0)$ lies on precisely $(q-1)/2$ tangents.

If $b + cZ = 0$ then $f = c \cdot (Z^q - Z)$ and it follows that $(1,0,0)$ does not lie on a tangent, i.e., S is not minimal, contradiction.

If $b'c - bc' = 0$ then b and c differ by a p-th power. In the particular case $q = p$ (and $m < q$) it follows that they differ by a constant factor, say $b(Z) = a \cdot c(Z)$, and $f(Z) = c(Z) \cdot (a + Z)^q$ so that S contains (and hence is) a line.

3 Lacunary polynomials

We see that the blocking set problem leads one to search for polynomials $f(x)$, $g(x)$, $h(x)$, where f factors completely into linear factors and g and h have degree at most $\frac{1}{2}(q+1)$ such that $f = x^q g + h$.

(Indeed, in the proof above we found such an f given a small blocking set S, a point P inside, and a line L passing through that point. An e-fold linear factor of f corresponds to a line on P distinct from L meeting S in $e+1$ points. The line L meets S in $|S| - \mathrm{degree}(f)$ points. Below we take $|S| = \frac{3}{2}(q+1)$.)

This equation has solutions that need not correspond to blocking sets. We give a few examples.

a) (For odd q, say $q = 2r+1$.) Take $f(x) = x\prod(x-a)^3$ where the product is over the nonzero squares a. Then f satisfies $f(x) = x(x^r - 1)^3 = x^q g + h$ with $g(x) = x^r - 3$, $h(x) = 3x^{r+1} - x$. This would correspond to line intersections (with frequen-

cies written as exponents) $1^r 2^2 4^r$. For $q = 7$ this is the function for the blocking set $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, $(a,b,1)$ with $a,b \in \{1,2,4\}$.

b) (For $q = 4t+1$.) Take $f(x) = x\prod(x-a)\prod(x-b)^4$ where the product is over the nonzero squares a and fourth powers b. Here $f(x) = x(x^{2t}-1)(x^t-1)^4 = x^q g + h$ with $g(x) = x^{2t} - 4x^t + 5$ and $h(x) = -5x^{2t+1} + 4x^{t+1} - x$. This would correspond to line intersections $1^{2t}2^{t+2}6^t$.

c) (For $q = 4t+1$.) Take $f(x) = x^{t+1}\prod(x-a)\prod(x-b)^2$ where the product is over the nonzero squares a and fourth powers b. Here $f(x) = x^{t+1}(x^{2t}-1)(x^t-1)^2 = x^q g + h$ with $g(x) = x^t - 2$ and $h(x) = 2x^{2t+1} - x^{t+1}$. This would correspond to line intersections $1^{2t}2^t4^t(t+2)^2$. For $q = 13$ this is a function for the blocking set $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, $(1,a,0)$, $(0,1,a)$, $(a,0,1)$, $(b,c,1)$ with $a^3 = -1$, $b^3 = c^3 = 1$.

d) (For $q = 13$.) Take $f(x) = x\prod(x-a)^4\prod\left(x-\frac{1}{2}a\right)$ where the product is over all a with $a^3 = 1$. Here $f(x) = x(x^3-1)^4\left(x^3-\frac{1}{8}\right) = x^q g + h$ with $g(x) = x^3 + 4$ and $h(x) = 5x^7 - 5x^4 - 5x$. This would correspond to line intersections $1^6 2^4 5^4$, and indeed this occurs.

These lacunary polynomials are just weighted subsets of the projective line, and in particular $\mathrm{PGL}(2,q)$ acts. For example, $x \mapsto \frac{1}{x}$ sends $x^q g + h$ to $x^q \tilde{h} + \tilde{g}$ where $\tilde{k}(x) = x^{(q+1)/2} k(x^{-1})$.

For completeness we describe the lacunary polynomials that correspond to the Rédei type blocking set:

e) Take $f(x) = x^q - x^{(q+1)/2} = x^{(q+1)/2}\prod(x-a)$ where the product is over the nonzero squares a.

f) Take $f(x) = x^q - 2x^{(q+1)/2} + x = x\prod(x-a)^2$ where the product is over the nonzero squares a.

4 Search setup

We search for lacunary polynomials as described above over the prime field $\mathbb{F}_p$ by exploiting the equation

$$f = x^p g + h = a(xg+h)(gh' - g'h)$$

for some constant a, where f factors into linear factors, and $xg+h$ factors into distinct linear factors, and g and h have degree at most $\frac{1}{2}(p+1)$.

If we guess $xg+h$ and the constant of proportionality a and the constant term of g then this relation gives a recurrence that allows us to compute all other coefficients of g, and thus to find f. If we take $l = 1$, then $xg+h$ is a product of $m = (p+3)/2$ distinct linear factors, and there are $\binom{p}{m}$ possible choices for the set of roots of $xg+h$. We tried all possibilities for $p < 41$, where $\mathrm{PGL}(2,p)$ was used to divide the computation time by roughly p^3. This yields all possibilities for f, and in particular the multiplicities of the roots of f, so that we know the sizes of the intersection of lines on some arbitrary point $(1,0,0)$ with S. This suffices to classify the possible solutions. In fact, except for example d) in the previous section we only find solutions if $xg + h = x^{(q+1)/2} - x$. In a seperate section we will completely classify this special case.

Looking at $p = 31$ took 80 minutes CPU time on an old Pentium running Linux, and $p = 37$ took four days.

5 Results

The results are as follows. First of all there are possibilities with a factor of multiplicity $\frac{1}{2}(p+1)$, i.e., a $\frac{1}{2}(p+3)$-secant, and we have a Rédei example, unique by Lovász and Schrijver.

For the primes $p = 7, 11, 19, 23, 31$ there is a unique non-Rédei intersection pattern, namely $1^{(p-1)/2}2^2 4^{(p-1)/2}$ (corresponding to the lacunary polynomial found under a) above). Counting the total number of lines on these points we see that this can be a blocking set only for $p = 7$. It remains to investigate the cases $p = 7, 13, 17, 29, 37$.

5.1 $p = 7$. For $p = 7$ there is a unique intersection pattern $1^3 2^2 4^3$ (and no computer search is required to see that). It gives rise to a unique sporadic blocking set (of size 12) (see also [4]).

It arises as follows. The affine plane $\mathrm{AG}(2,3)$ can be embedded into $\mathrm{PG}(2,q)$ if and only if $q = 0, 1 \pmod 3$, as one easily checks by assigning coordinates to the 9 points of $\mathrm{AG}(2,3)$ (for more details see [9] and [1]). This embedding is unique up to isomorphism. The three lines in a parallel class of $\mathrm{AG}(2,3)$ are concurrent in $\mathrm{PG}(2,q)$ if and only if $q = 0 \pmod 3$. For $q = 1 \pmod 3$ this 9-set can be found as the set of inflections of a nondegenerate cubic. Dualizing we find a dual affine plane $\mathrm{DAG}(2,3)$ with 12 points, 9 4-lines (3 on each point) and 12 2-lines (2 on each point) embedded in $\mathrm{PG}(2,q)$ for $q = 1 \pmod 3$. It has $(q^2+q+1) - 12(q+1-5) - 9 - 12 = (q-4)(q-7)$ 0-secants, and hence is a blocking set for $q = 4, 7$ and for $q = 4$ even a 2-fold blocking set.

The projective triangle in $\mathrm{PG}(2,7)$ can also be viewed as a modification of $\mathrm{AG}(2,3)$: it arises by taking the 9 points of $\mathrm{AG}(2,3)$ and adding the 3 points of intersection of the lines of one parallel class.

There are no other possibilities: Suppose the blocking set S has n_i i-secants, $1 \leqslant i \leqslant 4$. Then $\sum n_i = 57$, $\sum i n_i = 96$, $\sum \binom{i}{2} n_i = 66$ by standard counting. And $n_1 = 36$ since we have equality in the Blokhuis bound. Hence $n_2 = 12$, $n_3 = 0$, $n_4 = 9$. If there are m_i i-secants on a fixed point $s \in S$, then $\sum m_i = 8$, $\sum (i-1)m_i = 11$, $m_1 = 3$ so that $m_2 = 2$, $m_4 = 3$. This yields the $\mathrm{DAG}(2,3)$ structure.

More generally, Gács et al. showed in [6] that if a nontrivial blocking set S of size $\frac{3}{2}(p+1)$ in $\mathrm{PG}(2,p)$ has a k-secant for $k \geqslant \frac{1}{2}(p+1)$ then it is of Rédei type, unless $p = 7$ and we have this dual affine plane.

5.2 $p = 11$. We already saw that for $p = 11$ nothing of interest happens. More generally, Gács [5] showed that a k-secant with $k = \frac{1}{2}(p-1)$ only occurs for sets of Rédei type, and simple counting then shows that for $p = 11$ the set S must be of Rédei type.

5.3 $p = 13$. For $p = 13$ there is a nice example again that is not of Rédei type. Let $q = 1 \pmod 3$ and take in $\mathrm{PG}(2,q)$ the 9 points of an embedded $\mathrm{AG}(2,3)$ together with the 12 points of intersection of lines that are parallel in $\mathrm{AG}(2,3)$. This yields a

self-dual configuration. Indeed, these 21 points together with the 21 lines that contain more than two of the points have a structure that is that of PG(2, 4) in which the incidences between the 9 points of a unital (AG(2, 3)) and the tangent at these points has been removed. There are 12 5-secants, 9 4-secants, 36 2-secants, $21(q+1-8)$ 1-secants and $(q^2+q+1)-21(q+1-8)-36-9-12=(q-7)(q-13)$ 0-secants, so that this is a blocking set for $q=7,13$, and for $q=7$ even a 2-fold blocking set.

For $p=13$ we have $|S|=21$. The search shows that there are four possible intersection patterns: a) $1^6 2^2 4^6$, b) $1^6 2^5 6^3$, c) $1^6 2^3 4^3 5^2$, d) $1^6 2^4 5^4$. Let there be N_a points of type a, etc., and n_i i-secants.

If $N_b > 0$, then there is a 6-secant, and it meets another 12 6-secants, so $13 \leqslant n_6 = 3N_b/6$ and $N_b > |S|$, contradiction.

So $N_b = 0$. If also $N_a = 0$ then $N_c + N_d = 21$, $n_1 = 126$, $n_2 = \frac{3}{2}N_c + 2N_d$, $n_4 = \frac{3}{4}N_c$, $n_5 = \frac{2}{5}N_c + \frac{4}{5}N_d$, $\sum n_i = 13^2 + 13 + 1 = 183$, with unique solution $N_c = 12$, $N_d = 9$, $n_2 = 36$, $n_4 = 9$, $n_5 = 12$. Each 4-secant meets the remaining eight, that is, the 4-secants meet pairwise (in points of type c)), and the points of type c) form a DAG(2, 3). A 5-secant meets the DAG(2, 3) in at most two points, so has at least three points of type d), and the points of type d) together with the 5-secants form an AG(2, 3). Now everything is determined, and this indeed yields a solution.

If $N_a > 0$ then at most two points do not lie on a 4-secant, so $N_d \leqslant 2$. If $N_c = N_d = 0$, then $N_a = 21$ and $n_4 = 6N_a/4$ is not integral. Contradiction. So, $n_5 = \frac{2}{5}N_c + \frac{4}{5}N_d > 0$. We have $n_4 = \frac{6}{4}N_a + \frac{3}{4}N_c$, so N_c is even, and $4 \mid n_5$. Each 5-secant meets at least five more, so $n_5 \geqslant 8$, i.e., $N_c + 2N_d \geqslant 20$, $N_c + N_d \geqslant 18$, $N_a \leqslant 3$. If $n_5 \geqslant 12$ then $N_c + 2N_d \geqslant 30$, $N_c + N_d \geqslant 28$, contradiction. So $n_5 = 8$. Now $n_4 = \frac{6}{4}N_a + \frac{3}{4}N_c = \frac{3}{2}(N_a + N_c + N_d) - \frac{3}{4}(N_c + 2N_d) = \frac{3}{2}\cdot 21 - \frac{3}{4}\cdot 20$ is not integral. Contradiction.

So, up to isomorphism there is a unique minimal blocking set in PG(2, 13) of size 21 that is not of Rédei type.

5.4 $p = 17$. For $p=17$ we have $|S|=27$. There are three possible intersection patterns: a) $1^8 2^2 4^8$, b) $1^8 2^6 6^4$, c) $1^8 2^4 4^4 6^2$.

We have $N_a + N_b + N_c = 27$ and $n_1 = 8 \cdot 27 = 216$, and $n_2 = N_a + 3N_b + 2N_c$, $n_4 = 2N_a + N_c$, so $n_2 + n_4 = 3 \cdot 27 = 81$ and $n_6 = 17^2 + 17 + 1 - 216 - 81 = 10$. $2N_b + N_c = 3n_6 = 30$, so $N_b \geqslant 3$. Now three points of type b) see twelve 6-secants, but there are only ten, so there is a 6-secant with at least two points of type b). But such a 6-secant meets at least $3+3+1+1+1+1=10$ other 6-secants, contradiction.

So, no non-Rédei sets occur for $p=17$.

5.5 $p = 29$. For $p=29$ we have $|S|=45$. There are three possible intersection patterns: a) $1^{14} 2^2 4^{14}$, b) $1^{14} 2^9 6^7$, c) $1^{14} 2^7 4^7 9^2$.

If type c) occurs then there are 9-secants, and each 9-secant meets another nine, so $10 \leqslant n_9 = 2N_c/9$ and $N_c \geqslant 45$ so that all points are of type c). But then $n_4 = 7N_c/4$ is not integral. Contradiction.

So $N_c = 0$. There are $14N_a/4$ 4-secants, so N_a is even. There are $7N_b/6$ 6-secants, so N_b is even. But $N_a + N_b = 45$. Contradiction.

So, no non-Rédei sets occur for $p=29$.

5.6 $p = 37$ and larger p. For $p = 37$ we have $|S| = 57$. There are three possible intersection patterns: a) $1^{18}2^24^{18}$, b) $1^{18}2^{11}6^9$, c) $1^{18}2^94^911^2$, and as before no non-Rédei set can exist.

Let us prove more generally that no sporadic blocking set exists in $\mathrm{PG}(2, p)$, $p = 4t + 1 \geqslant 37$, when only the three patterns a) $1^{2t}2^24^{2t}$, b) $1^{2t}2^{t+2}6^t$ and c) $1^{2t}2^t4^t(t+2)^2$ do occur. We have $|S| = 6t + 3$.

If type c) occurs then there are $(t+2)$-secants, and each meets $t+2$ more, so $t + 3 \leqslant n_{t+2} = 2N_c/(t+2) \leqslant 2|S|/(t+2) < 12$, contradiction. So $N_c = 0$. Now $N_a + N_b = |S|$ and $n_1 + n_2 + n_4 + n_6 = p^2 + p + 1$ determines all values: $N_a = 12$, $N_b = 6t - 9$, $n_1 = 12t^2 + 6t$, $n_2 = 3t^2 + \frac{3}{2}t + 3$, $n_4 = 6t$, $n_6 = t^2 - \frac{3}{2}t$. Now a 4-line meets $4(2t-1)$ other 4-lines, contradicting $n_4 = 6t$.

So, for a new sporadic blocking set we need a new factorizing lacunary polynomial.

6 The special case $xg + h = x^{(p+1)/2} - x$

In this section we consider the modular differential equation

$$x^p g + h = a(xg + h)(g'h - h'g),$$

where $xg + h$ factors into distinct linear factors, and $g, h \in \mathbb{F}_p[x]$ are both of degree at most $(p+1)/2$, not both zero, and a is a nonzero constant. Write $s := xg + h$ and $t := (x^p - x)/s$. Then $h = s - xg$ and $s't + st' = -1$. Rewrite the original equation as

$$(x^p - x)g = s(ag's - ags' + ag^2 - 1).$$

Division by s gives

$$tg = ag's - ags' + ag^2 - 1 = ag's - ags' + ag^2 + st' + s't.$$

This may be rewritten as

$$s(ag' + t') = -(ag - t)(g - s').$$

We now consider the special case $s = x^{n+1} - x$, where $n := (p-1)/2$. Then $t = x^n + 1$, and our equation simplifies to

$$(x^n - 1)\left(xag' - \frac{1}{2}x^n\right) = (x^n + 1 - ag)\left(g + 1 - \frac{1}{2}x^n\right).$$

If u is a square in $\mathbb{F}_p^*$ (so that $u^n - 1 = 0$) then $g(u) \in \{-\frac{1}{2}, \frac{2}{a}\}$. Comparing degrees we see that g has degree at most n. Modulo x^n this equation reduces further to

$$xg' = \left(g - \frac{1}{a}\right)(g+1) \mod x^n.$$

Note that $\left(g(0) - \frac{1}{a}\right)(g(0) + 1) = 0$.

Consider more generally the equation $xg' = (g - b)(g - c) \bmod x^n$, say with $g(0) = b$. Then we get $g = c + (b - c)/(1 - Cx^{b-c}) \bmod x^n$ for some constant C.

(Indeed, the equation $xg' = (g - b)(g - c)$ suffices to determine all coefficients of g in terms of earlier coefficients, except the coefficient of x^i where $i = b - c$.)

In the above, $1/(1 - Cx^d)$ was to be interpreted in $\mathbb{F}[[x]]$. We get a solution in polynomial form by replacing it by $(1 - C^m x^{dm})/(1 - Cx^d)$, for some m such that $dm \geqslant n$.

Thus, in our case,

$$g = c + d\frac{1 - C^m x^{dm}}{1 - Cx^d} + ex^n,$$

for certain constants c, d, e, where either $d = 0$ and the middle term is absent, or $C \neq 0$, $0 < d < p$, $m \geqslant 2$, $d(m - 1) < n \leqslant dm$.

Since g takes at most two values on nonzero squares, the same holds for $\frac{1-C^m x^{dm}}{1-Cx^d}$ (when $d \neq 0$). Thus, there are constants A, B such that $x^n - 1$ divides $(1 - C^m x^{dm} - A(1 - Cx^d))(1 - C^m x^{dm} - B(1 - Cx^d))$. This remains true if we replace x^{dm} by x^{dm-n}, so either $n \leqslant 2d$, $m = 2$, $d = n/2$, or the right hand side vanishes and $A = 0$, $dm = n$, $C^m = 1$.

In the former case we have (with new constants) $g = c + dx^{n/2} + ex^n$ with $c = -1$ or $c = 1/a$. Substitution and comparison of coefficients gives $(a, c, d, e) = (-2, -1, 0, 1/2)$ or $(a, c, d, e) = (-2, -1, 0, 0)$ or $(a, c, d, e) = (-4/3, -1, \pm 1/2, 0)$ or $(a, c, d, e) = (-2, -1/2, 0, 0)$ or $(a, c, d, e) = (-4/3, -3/4, 0, 1/4)$ or $(a, c, d, e) = (-4/5, -5/4, \pm 1, -1/4)$, and these correspond to the examples f), e), c), f), a), b), respectively.

In the latter case we have $g = c + d\frac{1-x^n}{1-Cx^d} + ex^n$, where $n = dm$, $C^m = 1$ and without loss of generality $m \geqslant 3$. The two values taken by g on the set of nonzero squares differ by $\frac{2}{a} + \frac{1}{2} = \pm n = \mp\frac{1}{2}$, so that $a = -2$ and $c + e = -1/2$. Comparing leading coefficients we find $e \in \{0, -1/4\}$. Comparing constants we find $c + d \in \{-1, -1/2\}$. The four possible values of d turn out to be $0, n/2, n, 3n/2$, and we already handled those.

Altogether the conclusion is that if $x^p g + h = a(xg + h)(g'h - h'g)$ and $xg + h = x^{n+1} - x$, with g, h both of degree at most $n + 1$, then we have one of the examples from Section 3.

7 Partial spreads in PG(3, 7)

A *spread* in a point-line geometry is a partition of the point set into lines. A *partial spread* is a collection of pairwise disjoint lines. Given a partial spread in a point-line geometry, we shall call a point not covered by one of its lines a *hole*.

Hirschfeld [8] (Section 17.6) shows that PG(3, q) has a maximal partial spread of size $q^2 - q + 2$ for $q > 3$ (and a maximal partial spread of size 7 for $q = 3$). No larger maximal partial spreads (that are not spreads) are known, except for $q = 7$, where Heden [7] constructed a maximal partial spread of size 45.

The relation with blocking sets in $\mathrm{PG}(2,q)$ is as follows: *Given a maximal partial spread of size* $q^2+1-\delta$ *in* $\mathrm{PG}(3,q)$, *where* $\delta>0$, *we find a nontrivial blocking set of size* $q+\delta$ *in* $\mathrm{PG}(2,q)$.

(Indeed, we find such a blocking set by taking the set of holes in a plane that does not contain a line of the partial spread.)

Since nontrivial blocking sets in $\mathrm{PG}(2,7)$ have size at least 12, it follows that a partial spread in $\mathrm{PG}(3,7)$ that is not a full spread has at most 45 lines, that is, has at least 40 holes.

We did a complete search for partial spreads with 40 holes and find that there are precisely 879 nonisomorphic such partial spreads. The table below gives group order, number of isomorphism classes and total number of partial spreads.

order	#	total
1	174	4 510 080
2	383	4 963 680
3	7	60 480
4	175	1 134 000
6	35	151 200
8	39	126 360
10	9	23 328
12	40	86 400
20	1	1 296
24	11	11 880
60	1	432
120	4	864
total	879	11 070 000

Soicher [11] had already determined the partial spreads with 40 holes and an automorphism group of order 5.

The geometry of the set H of 40 holes (complement of the union of a maximal partial spread $\mathscr{S}$ of size 45) is uniquely determined, as was already remarked by Heden. Indeed, each plane must meet H in either 5 or 12 points (depending on whether it contains a line of $\mathscr{S}$ or not), and the holes form a blocking set in each plane π with 12 holes. (Otherwise there would be a line L in π disjoint from H, and looking at the 8 planes on L they must all have precisely 5 points of H, contradiction.) Thus, the planes with 12 holes are either of the triangle or of the $\mathrm{DAG}(2,3)$ type.

Now all planes with 12 holes must be of the same type. Indeed, let an *m-line* be a line with m holes. A plane of triangle type does not have 4-lines, while a plane of $\mathrm{DAG}(2,3)$ type does not have 5-lines. In particular, a 4-line cannot meet a 5-line. Each hole in a plane of $\mathrm{DAG}(2,3)$ type is on some 4-line, so no such hole can be on a 5-line. On a 4-line there are 8 planes, four of $\mathrm{DAG}(2,3)$ type, and we find at least 36 holes on a 4-line, no room for a 5-line.

Not all planes can be of triangle type. Indeed, suppose this is the case. Each 3-line is on three planes with 12 holes and in each of these planes each of the three holes of

the 3-line lies on a unique 5-line. It follows that each hole is on precisely three 5-lines (so that there are 24 5-lines in all). On the other hand, the projective transformations that fix the set of non-holes on a 5-line have two orbits on the 5 holes, so that the two 'corners' on that line in a triangle do not depend on the choice of triangle, so that these corners would be on six 5-lines, contradiction.

Thus, all planes are dual affine planes. We have a geometry with points and 4-lines, where two intersecting 4-lines determine a plane, and each plane is dual affine of order 3. By Cuypers [3] this is the geometry of points and hyperbolic lines and dual affine planes of the Sp$(4, 3)$ geometry. This is again a self-dual configuration that lives in PG$(3, q)$ for all prime powers $q = 1 \pmod 3$. (For example, in PG$(3, 4)$ it lives as the nonisotropic points of a U$(4, 2)$ geometry.) Explicit coordinates: take the 4 points $(1, 0, 0, 0)$ and the 36 points $(0, 1, a, -b)$ where $a^3 = b^3 = 1$ and the coordinates may be permuted cyclically.

References

[1] A. Bichara, G. Korchmáros, n^2-sets in a projective plane which determine exactly $n^2 + n$ lines. *J. Geom.* **15** (1980), 175–181. MR 82j:51016 Zbl 0459.51007

[2] A. Blokhuis, On the size of a blocking set in PG$(2, p)$. *Combinatorica* **14** (1994), 111–114. MR 96b:51010 Zbl 0803.05011

[3] H. Cuypers, Symplectic geometries, transvection groups, and modules. *J. Combin. Theory Ser. A* **65** (1994), 39–59. MR 94m:51003 Zbl 0824.51003

[4] J. W. Di Paola, On minimum blocking coalitions in small projective plane games. *SIAM J. Appl. Math.* **17** (1969), 378–392. MR 40 #1140 Zbl 0191.49601

[5] A. Gács, A remark on blocking sets of almost Rédei type. *J. Geom.* **60** (1997), 65–73. MR 99e:51009 Zbl 0897.51004

[6] A. Gács, P. Sziklai, T. Szőnyi, Two remarks on blocking sets and nuclei in planes of prime order. *Des. Codes Cryptogr.* **10** (1997), 29–39. MR 97j:51015 Zbl 0874.51002

[7] O. Heden, A maximal partial spread of size 45 in PG$(3, 7)$. *Des. Codes Cryptogr.* **22** (2001), 331–334. MR 2002a:51007 Zbl 0982.51005

[8] J. W. P. Hirschfeld, *Finite projective spaces of three dimensions*. Oxford Univ. Press 1985. MR 87j:51013 Zbl 0574.51001

[9] L. M. Kelly, S. Nwankpa, Affine embeddings of Sylvester-Gallai designs. *J. Combin. Theory Ser. A* **14** (1973), 422–438. MR 47 #3207 Zbl 0282.05018

[10] L. Lovász, A. Schrijver, Remarks on a theorem of Rédei. *Studia Sci. Math. Hungar.* **16** (1983), 449–454. MR 85e:51017 Zbl 0535.51009

[11] L. Soicher, Computation of partial spreads. http://www.maths.qmw.ac.uk/~leonard/partialspreads

Received 7 January, 2003; revised 5 April, 2003

A. Blokhuis, A. E. Brouwer, H. A. Wilbrink, Dept. of Math., Techn. Univ. Eindhoven, P.O. Box 513, 5600MB Eindhoven, Netherlands
Email: {aartb, aeb, wsdwhw}@win.tue.nl