Can. J. Math., Vol. XXX, No. 3, 1978, pp. 483–489

MAXIMAL STRICTLY PARTIAL SPREADS

GARY L. EBERT

1. Introduction. Let $\Sigma = PG(3, q)$ denote 3-dimensional projective space over $GF(q)$. A *partial spread* of Σ is a collection W of pairwise skew lines in Σ. W is said to be *maximal* if it is not properly contained in any other partial spread. If every point of Σ is contained in some line of W, then W is called a *spread*. Since every spread of $PG(3, q)$ consists of $q^2 + 1$ lines, the *deficiency* of a partial spread W is defined to be the number $d = q^2 + 1 - |W|$. A maximal partial spread of Σ which is not a spread is called a *maximal strictly partial spread* (msp spread) of Σ.

In [**3**] Bruen showed that if W is an msp spread of $PG(3, q)$, then $q + \sqrt{q} + 1 \leqq |W| \leqq q^2 - \sqrt{q}$. In the same paper Bruen also showed that if $q > 2$, there exist msp spreads W of $PG(3, q)$ with $|W| = q^2 - q + 1$ and hence deficiency $d = q$. This shows that the upper bound for $|W|$ is reasonably good for large q, but very little is known about the existence of msp spreads with relatively "large" deficiency. The purpose of this paper is to construct such examples. In doing this a rather interesting connection between geometry and number theory is pointed out.

When $q \equiv 1(4)$, msp spreads in $PG(3, q)$ are constructed with deficiency $d \geqq (2/3)(q + 1)[1/2(\sqrt{1 + 4\log_2(q)} - 1)]$. Moreover, if q is an odd prime raised to an even power, it is shown that Bruen's lower bound for $|W|$ is also reasonably good. Thanks are given to Marshall Hall, Jr. for bringing reference [**8**] to the author's attention. The author would also like to thank the referee for his many helpful suggestions.

2. The construction technique. The reader is referred to [**2**] for a complete explanation of spreads and reguli. In [**3**] Bruen constructed an msp spread W of $PG(3, q)$ with deficiency $d = q$ in the following way. Letting R_1 and R_2 denote two reguli of a regular spread S_0 that have precisely one line m in common, the set of lines

$$S = [S_0 \backslash (R_1 \cup R_2)] \cup (R_1 \backslash m) \cup R_2'$$

can easily be shown to be a spread. Here R_2' denotes the opposite regulus to R_2. If l is the unique line of R_1' through any chosen point of m, then the set of lines A of S meeting l have exactly one transversal. It can then be shown that the set of lines $W = (S \backslash A) \cup l$ is an msp spread of deficiency q.

We now generalize the above construction. Let $q > 2$ be a prime power and let t be a positive integer such that $t < (q + 1)/3$. If S_0 is a regular spread of

Received December 20, 1976 and in revised form, October 8, 1977 and January 17, 1978.

$\Sigma = PG(3, q)$, choose mutually disjoint reguli $R_1, \ldots, R_t$ and distinct reguli $T_1, \ldots, T_t$ of S_0 such that

$$R_i \cap T_i = \{l_i\} \quad \text{for } i = 1, \ldots, t$$
$$R_i \cap T_j = \phi \quad \text{for } i \neq j.$$

The question of existence for such reguli when $t > 1$ will be discussed in the remaining sections. Letting B denote the set of lines in

$$S_0 \backslash (R_1 \cup \ldots \cup R_t \cup T_1 \cup \ldots \cup T_t),$$

the set of lines

$$S = B \cup (T_1 \backslash l_1) \cup R_1' \cup \ldots \cup (T_t \backslash l_t) \cup R_t'$$

is easily seen to be a spread of Σ. Next choose lines $l_i' \in T_i'$ for $i = 1, \ldots, t$ so that $l_1', \ldots, l_t'$ are pairwise disjoint. Let A_i denote the set of lines in S meeting l_i' for $i = 1, \ldots, t$. Then the set of lines

$$W = \left[S \backslash \left(\bigcup_{i=1}^{t} A_i \right) \right] \cup l_1' \ldots \cup l_t'$$

can be shown to be an msp spread of Σ with deficiency

(1) $\quad d \geqq t(q + 1 - t) \geqq (2t/3)(q + 1).$

The restriction $3t < (q + 1)$ is used in several places, primarily to insure that any line extending W must meet at least three lines of $T_i \backslash l_i$ for some i.

The above bound is obtained as follows. For each i the lines of A_i are the q lines of $T_i \backslash l_i$ plus one line of R_i'. Since T_i and T_j have at most two lines in common for $i \neq j$,

$$\left| \bigcup_{i=1}^{t} (T_i \backslash l_i) \right| \geqq q + (q - 2) + \ldots + (q - 2t + 2) = t(q + 1 - t).$$

Hence

$$\left| \bigcup_{i=1}^{t} A_i \right| \geqq t + t(q + 1 - t) = t(q + 2 - t)$$

and

$$|W| \leqq q^2 + 1 - t(q + 2 - t) + t = q^2 - tq + (t^2 - t + 1).$$

It should be noted that if the reguli $T_1, \ldots, T_t$ are also chosen to be pairwise disjoint, then

(2) $\quad d = qt.$

3. Inversive planes. We are now faced with the problem of finding the maximum t for a given prime power q (subject to the restriction $t < (q + 1)/3$) for which there exist reguli $R_1, \ldots, R_t$ and $T_1, \ldots, T_t$ in S_0 satisfying the above stated conditions. In [**2**, Theorem 4.5] R. H. Bruck showed that the search for reguli in a regular spread of $PG(3, q)$ can be transformed into the search for circles in a miquelian inversive plane of order q, which we will denote by $IP(q)$. Thus we are concerned with the existence of certain configurations of circles in $IP(q)$.

The interested reader is referred to [**6**, Chapter 6] for a detailed discussion of $IP(q)$. As a point of notation, for any two distinct points P and Q of $IP(q)$, the set of all circles which pass through both P and Q will be called the *bundle with carriers* P *and* Q. A maximal set of mutually tangent circles at a point P will be called a *pencil with carrier* P. A *flock* K will be a set of pairwise disjoint circles such that, with the exception of precisely two points (called the *carriers* of K), every point of $IP(q)$ lies on precisely one circle of K.

Our problem is to find pairwise disjoint circles $C_1, \ldots, C_t$ and distinct circles $D_1, \ldots, D_t$ in $IP(q)$ such that C_i and D_i are tangent for $i = 1, \ldots, t$ but C_i and D_j are disjoint for $i \neq j$. Of course we are trying to maximize t subject to these restrictions and the additional constraint $t < (q + 1)/3$. We first take a combinatorial approach and then an algebraic approach.

4. The combinatorial approach. Slightly different arguments must be used for the cases q even and q odd. Since the technique is essentially the same in both cases, we will assume throughout that q is an even prime power. Choose C_1, D_1 to be two tangent circles of $IP(q)$, and we first answer the question of how many circles there are in $IP(q)$ that miss both C_1 and D_1. To this end, let $s(i, j)$ denote the number of circles that meet C_1 in i points and meet D_1 in j points, where i and j are integers satisfying $0 \leqq i, j \leqq 2$. We would like to compute $s(0, 0)$.

LEMMA 1. (i) $s(1, 0) = q(q - 2)/2 = s(0, 1)$.
(ii) $s(1, 1) = q - 2$.
(iii) $s(1, 2) = q^2/2 = s(2, 1)$.

Proof. Let P denote the point of intersection for the circles C_1 and D_1. Choose Q to be any point of C_1 other than P, and let $L(Q; C_1)$ denote the pencil of q circles with carrier Q containing the circle C_1. Since q is even, it can be shown (see [**6**, page 265]) that a circle not incident with the carrier of a pencil is tangent to precisely one circle of the pencil. Thus the $q - 1$ circles of $L(Q; C_1)\backslash\{C_1\}$ are either disjoint or secant to D_1. Since the $q + 1$ points of D_1 are covered by the circles of $L(Q; C_1)$, D_1 is disjoint from $(q - 2)/2$ circles of $L(Q; C_1)$. Allowing Q to vary and using symmetry, (i) now follows,

Since the only circles tangent to both C_1 and D_1 are those of the common pencil $L(P; C_1)$, (ii) follows immediately. Using the fact that the total number of circles tangent to D_1 is $q^2 - 1$, a little arithmetic and symmetry together give us (iii).

LEMMA 2. (i) $s(2, 0) = q^2(q - 2)/4 = s(0, 2)$.

https://doi.org/10.4153/CJM-1978-043-0 Published online by Cambridge University Press

(ii) $s(2, 2) = q^2(q + 2)/4$.
(iii) $s(0, 0) = q(q - 2)(q - 4)/4$.

Proof. Once again let P denote the point of intersection for C_1 and D_1. Choose R, S to be two points of C_1 other than P such that R, S are not conjugate with respect to D_1. Let $J(R, S)$ denote the bundle of $q + 1$ circles with carriers R and S. Then every circle of $J(R, S)\backslash\{C_1\}$ is either secant to or disjoint from D_1 since q is even. The $q + 1$ points of D_1 are covered by the bundle $J(R, S)$ and therefore $q/2$ circles in $J(R, S)\backslash\{C_1\}$ are disjoint from D_1. Allowing R, S to vary, we obtain $q^2(q - 2)/4$ distinct circles secant to C_1 and disjoint from D_1. All such circles are counted in this fashion, yielding (i) by symmetry. The rest of the lemma now follows from lemma (1) by simple counting arguments.

Next we would like to find tangent circles C_2 and D_2 that are disjoint from both C_1 and D_1. This would yield a desirable configuration as discussed in sections 2 and 3 with $t = 2$ and having the additional property that D_1 is disjoint from D_2.

THEOREM 1. *Let q be an even prime power such that $q \geqq 16$. Then there exist circles C_1, C_2, D_1, D_2 in $IP(q)$ such that C_1 is tangent to D_1; C_2 is tangent to D_2; and each of C_1, D_1 is disjoint from both C_2, D_2.*

Proof. Choose C_1, D_1 to be tangent circles in $IP(q)$. Let Ω denote the collection of circles in $IP(q)$ that are disjoint from both C_1 and D_1 and assume that no two circles in Ω are tangent by way of contradiction. Then there are at most $q + 1$ circles in Ω that are tangent to any circle not in Ω. Lemma (2) (iii) now gives us at least $q(q - 1)(q - 2)(q - 4)/4$ distinct circles that are tangent to at least one circle in Ω and hence are not in Ω. This is in contradiction to the total number of circles in $IP(q)$ when $q \geqq 16$, proving the theorem.

Remarks. A slight modification of the above counting techniques yields the odd order analogue of Theorem 1 when $q \geqq 11$. Direct computation shows that the theorem is also true for $q = 5, 7, 8, 9$. Such a configuration is impossible in $IP(4)$ since there are not enough points.

COROLLARY. *Let q be any prime power such that $q \geqq 7$. Then there exist msp spreads W of $PG(3, q)$ with deficiency $d = 2q$ and $|W| = q^2 - 2q + 1$.*

Proof. Since $t < (q + 1)/3$ when $t = 2$ and $q \geqq 7$, the result follows immediately from the construction and equation (2) given in Section 2.

Unfortunately, this combinatorial approach cannot be easily (if at all) extended to yield msp spreads of deficiency greater than $2q$. Hence we take a new approach.

5. The algebraic approach. We now give a model for $IP(q)$ that was discussed by W. F. Orr in [**7**]. Most of the tools we will be using are only valid when q is odd, and hence we *assume throughout this section that q is an odd prime power.* The elements of $GF(q^2) \cup \{\infty\}$ will be regarded as the points of $IP(q)$, and a circle of $IP(q)$ will be represented as a one-dimensional vector space over $GF(q)$ with basis element a 2 by 2 matrix of the form

$$\begin{bmatrix} x & a \\ b & -x^q \end{bmatrix},$$

where $x \in GF(q^2)$; $a, b \in GF(q)$; and $x^{q+1} + ab \neq 0$. Such a circle will have as its inversion the mapping

$$z \rightarrow \frac{xz^q + a}{bz^q - x^q} \quad \text{for all } z \text{ in } GF(q^2) \cup \{\infty\}.$$

For the remainder of this paper we will represent circles by matrices of the above form with the understanding that the circle is really a one-dimensional vector space over $GF(q)$.

Letting C, D be matrices representing circles of $IP(q)$ and letting $||C||$ denote the determinant of C, we define

$$h(C, D) = ||C + D|| - ||C|| - ||D||$$
$$C \cdot D = h(C, D)/2$$
$$C \times D = (C \cdot D)^2 - ||C||||D||.$$

Orr has shown (see [**7**, Lemma 2.1]) that C and D are disjoint, tangent, or secant accordingly as $C \times D$ is a non-zero square, zero, or non-square in $GF(q)$.

Choose $P = 0$ and $Q = \infty$ as two distinct points of $IP(q)$, and let $K(0, \infty)$ denote the linear flock of $q - 1$ circles with carriers 0 and ∞. Pick $C_1, \ldots, C_t$ to be circles represented by matrices of the form

$$C_i = \begin{bmatrix} 0 & a_i \\ 1 & 0 \end{bmatrix},$$

where $a_1, \ldots, a_t$ are distinct non-zero elements of $GF(q)$. These circles are all in $K(0, \infty)$ and hence are pairwise disjoint. Choose $D_1, \ldots, D_t$ to be circles represented by matrices of the form

$$D_i = \begin{bmatrix} x_i & 0 \\ 1 & -x_i^q \end{bmatrix},$$

where $x_1, \ldots, x_t$ are elements of $GF(q^2)$ such that $x_i^{q+1} = a_i/4$. Since $C_i \times D_i = 0$, D_i is tangent to C_i for each i. It should be also noted that each D_1 passes through the point 0 and

$$C_i \times D_j = a_i(a_i - a_j)/4.$$

According to the msp spread construction given in sections 2 and 3, we would like C_i and D_j to be disjoint for $i \neq j$ and therefore want $C_i \times D_j$ to be a non-zero square in $GF(q)$ for $i \neq j$. Hence we would like to find a collection of distinct non-zero squares $a_1, \ldots, a_t$ in $GF(q)$ such that the difference of any two is a square. The problem of finding the largest possible collection of this type is old and difficult. Of course $(a_1 - a_2)/(a_2 - a_1) = -1$ is required to be a non-zero square in $GF(q)$, and hence we must assume that $q \equiv 1\ (4)$. Some partial results and their consequences are now given.

THEOREM 2. *Let p be an odd prime and let $q = p^{2n}$ for some positive integer n. Then there exist msp spreads W of $PG(3, p^{2n})$ with deficiency $d \geqq (2/3)(p^n - 1)(p^{2n} + 1)$.*

Proof. Every element of $GF(p^n)$ is a square in $GF(p^{2n})$. Thus we can choose $t = p^n - 1$ non-zero squares in $GF(p^{2n})$ such that the difference of any two is a square in $GF(p^{2n})$; namely, choose the non-zero elements of $GF(p^n)$. The reader should note that $q \equiv 1\ (4)$ since $q = p^{2n}$ where p is odd. Clearly $t < (q + 1)/3$. The result now follows from the construction and equation (1) given in Section 2.

It should be noted that the deficiency guaranteed by Theorem 2 is of the order $q^{3/2}$ while the maximum possible deficiency from Bruen's result is of the order q^2. Hence, in this case, Bruen's lower bound for $|W|$ is reasonably good for large q.

THEOREM 3. *Let $p \geqq 29$ be a prime such that $p \equiv 1\ (4)$. Then there exist msp spreads W of $PG(3, p)$ with deficiency $d \geqq 2(p + 1)$.*

Proof. As shown in [**1**, Theorem 10-4], $GF(p)$ has at least one triple of consecutive non-zero squares so long as $p \geqq 29$. Let $a - 1, a, a + 1$ denote non-zero squares of $GF(p)$. Clearly $a \neq \pm 1$. Since -1 is a square in $GF(p)$, it is easy to see that $1, a, a^{-1}$ denote three distinct non-zero squares such that the difference of any two is a square. With $t = 3$ and $p \geqq 29$, clearly $t < (p + 1)/3$. The result now follows as in Theorem 2.

THEOREM 4. *Let p be a prime such that $p \equiv 1\ (4)$. Then there exist msp spreads W of $PG(3, p)$ with deficiency $d \geqq [(1/3) \ln (p)](p + 1)$, where $[r]$ denotes the greatest integer less than or equal to r.*

Proof. As shown in [**5**], for any prime $p \equiv 1\ (4)$, the largest collection of non-zero squares in $GF(p)$ such that the difference of any two is a square always has cardinality at least $(1/2) \ln (p)$. The result now follows as in Theorem 2.

THEOREM 5. *Let q be a prime power such that $q \equiv 1\ (4)$. Then there exist msp spreads W of $PG(3, q)$ with deficiency*

$$d \geqq (2/3)(q + 1)[1/2(\sqrt{1 + 4 \log_2 (q)} - 1)].$$

Proof. As shown in [**8**, Theorem 3], so long as $q \equiv 1\ (2)$ and $q > 2^{r(r+1)}$, there exists an $(r + 1)$-tuple $a_1, \ldots, a_{r+1}$ of elements in $GF(q)$ such that $a_j - a_i$ is a non-zero square for $1 \leqq i < j \leqq r + 1$. Setting

$$t = [1/2(\sqrt{1 + 4 \log_2 (q)} - 1)],$$

it is easy to see that $q > 2^{t(t+1)}$. Hence we can choose elements $a_1, \ldots, a_{t+1}$ in $GF(q)$ satisfying the above condition. Setting $b_i = a_{i+1} - a_1$ for $i = 1, \ldots, t$ and using the fact that -1 is a square in $GF(q)$, we obtain a set of t non-zero squares in $GF(q)$ such that the difference of any two is a square. The result now follows as in Theorem 2.

Among other things, Theorem 5 shows that for any constant c, msp spreads of deficiency $d \geqq cq$ exist whenever q is a sufficiently large prime power such that $q \equiv 1$ (4). Thus our construction technique does produce msp spreads of $PG(3, q)$ with reasonably large deficiency; in fact, with deficiency of the order $q\sqrt{\log_2(q)}$.

6. Concluding remarks. To obtain maximum mileage from our construction technique for msp spreads of large deficiency, a complete solution to the non-zero squares problem should first be found. This has not yet been accomplished.

In the search for circles $C_1, \ldots, C_t$ and $D_1, \ldots, D_t$ of $IP(q)$ satisfying the conditions stated at the end of Section 3, the case when $C_1, \ldots, C_t$ do not form a linear set has not yet been studied. On the other hand, if $C_1, \ldots, C_t$ do form a linear set, it might be profitable to consider circles D_i that do not pass through one of the carriers for this linear set. In any case, when q is even, it seems apparent that some new approach must be found to produce msp spreads of deficiency greater than $2q$.

It should also be pointed out that in a recent paper [**4**], Bruen and Hirschfeld use a twisted cubic to construct a msp spread of size $\frac{1}{2}(q^2 + q + 2)$ whenever 3 does not divide $q + 1$.

REFERENCES

1. G. E. Andrews, *Number theory* (W. B. Saunders, Philadelphia, London, Toronto, 1971)

2. R. H. Bruck, *Construction problems of finite projective planes*, Combinatorial Mathematics and Its Applications, ed. R. C. Bose and T. A. Dowling, The University of North Carolina Press, Chapel Hill (1969), 426–514.

3. A. Bruen, *Partial spreads and replaceable nets*, Can. J. Math. *23* (1971), 381–391.

4. A. A. Bruen and J. W. P. Hirschfeld, *Applications of line geometry over finite fields I. The twisted cubic*, Geometriae Dedicata, to appear.

5. D. A. Buell and K. S. Williams, *Maximal residue difference sets modulo p*, Proc. Amer. Math. Soc., to appear.

6. P. Dembowski, *Finite geometries* (Springer-Verlag, Berlin, 1968).

7. W. F. Orr, *The miquelian inversive plane IP(q) and the associated projective planes*, Dissertation, University of Wisconsin, Madison, Wisconsin, 1973.

8. R. M. Wilson, *Cyclotomy and difference families in elementary abelian groups*, J. Number Theory *4* (1972), 17–47.

Texas Tech University,
Lubbock, Texas;
University of Delaware,
Newark, Delaware