ON A BOUND USEFUL IN THE THEORY OF FACTORIAL DESIGNS AND ERROR CORRECTING CODES[1]

By R. C. Bose and J. N. Srivastava

University of North Carolina

0. Summary. Consider a finite projective space $PG(r-1, s)$ of $r-1$ dimensions, $r \geqq 3$, based on the Galois field GF_s, where $s = p^h$, p being a prime. A set of distinct points in $PG(r-1, s)$ is said to be a non-collinear set, if no three are collinear. The maximum number of points in such a non-collinear set is denoted by $m_3(r, s)$. It is the object of this paper to find a new upper bound for $m_3(r, s)$. This bound is of importance in the theory of factorial designs and error correcting codes. The exact value of $m_3(r, s)$ is known when either $r \leqq 4$ or when $s = 2$. When $r \geqq 5$, $s > 3$, the best values for the upper bound on $m_3(r, s)$ are due to Tallini [10] and Barlotti [1]. Our bound improves these when $s = 3$ or when s is even.

1. Introduction. R. A. Fisher [4], [5] showed that the maximum number of factors, which can be accommodated in a symmetrical factorial design in which each factor is at s levels and the blocks are of size s^r (where s is prime), without confounding any main effect or two factor interaction is $(s^r - 1)/(s - 1)$.

Bose [2], generalizing Fisher's result proved the following: Let $m_t(r, s)$ denote the maximum number of points which can be chosen in the finite projective space $PG(r-1, s)$, where s is a prime or the power of a prime, so that no t of the points are dependent. Then $m_t(r, s)$ is the maximum number of factors which we can accommodate in a symmetrical factorial design in which each factor is at s levels and the blocks are of size s^r, so that no t factor or lower order interaction is confounded. Fisher's result follows at once by noting that for the case $t = 2$, $m_t(r, s)$ is simply the number of distinct points in $PG(r-1, s)$.

For a fractionally replicated design $1/s^k \times s^n$, consisting of a single block with s^r plots or experimental units, $n = r + k$, a slight modification of Bose's argument shows that if it is required that no d-factor or lower order interaction, should be aliased with a d-factor or a lower order interaction, then the maximum possible value of n is $m_{2d}(r, s)$. On the other hand if it is required that no d-factor or lower order interaction should be aliased with a $(d+1)$-factor or a lower order interaction, then the maximum value of n would be $m_{2d+1}(r, s)$.

The number $m_t(r, s)$ also turns out to be important in information theory. If there is an s-ary channel, i.e. a channel capable of transmitting s distinct symbols, then for an (n, k) group code, with k information symbols and fixed redundancy $r = n - k$, the maximum value of n for which d errors can be corrected with

Received 27 May 1963.

[1] This research was supported in part by the Mathematics Division of the Air Force Office of Scientific Research under Grant No. AF-AFOSR-84-63.

certainty is $m_{2d}(r, s)$. Similarly the maximum value of n for which d errors can be corrected with certainty and $d + 1$ errors can be detected is $m_{2d+1}(r, s)$. This parallelism between the theory of fractional replications and error correcting codes has been brought out by Bose [3].

Thus the problem of finding the maximum value of $m_t(r, s)$, and of obtaining by a constructive method the corresponding points of $PG(r - 1, s)$ is of some importance. This problem may be called the packing problem. Only partial solutions to this problem are at present known. In the absence of a complete solution a good bound on $m_t(r, s)$ is desirable. In this paper we shall consider the case $t = 3$. For this case the packing problem reduces to finding the maximum number of points in $PG(r - 1, s)$ so that no three are collinear. Such a set may be called a *non-collinear set*, and $m_3(r, s)$ is then the maximum number of points in a non-collinear set in $PG(r - 1, s)$.

Bose [2] showed that for the case $r = 3$, (i.e. for a finite projective plane)

$$m_3(3, s) = s + 1 \qquad \text{when } s \text{ is odd,} \tag{1.1}$$

$$m_3(3, s) = s + 2 \qquad \text{when } s \text{ is even.} \tag{1.2}$$

For the case $r > 3$, $s = 2$, Bose [2] showed that

$$m_3(r, 2) = 2^{r-1} \tag{1.3}$$

and the same result was obtained independently by Hamming [6], in connection with binary group codes correcting one error and detecting two errors.

For $r = 4$, Bose [2] showed that when s is odd

$$m_3(4, s) = s^2 + 1, \qquad s > 2 \tag{1.4}$$

and the same result was proved to hold true for the case when s is even ($s > 2$) by Qvist [7], the particular case $s = 4$ having been obtained earlier by Seiden [9].

When $r \geqq 5$, $s > 2$, the exact value of $m_3(r, s)$ is not known. The best upper bounds currently known are due to Tallini, and Barlotti. Thus Tallini [10] has shown that

$$m_3(r, s) < s^{r-2} + 1, \qquad s > 2, \quad r \geqq 4 \tag{1.5}$$

the result holding both for odd and even s. When $s > 3$, Barlotti [1], has improved the bound given above. He shows that:

$$m_3(r, s) \leqq s^{r-2} - (s - 5)\sum_{i=0}^{r-5} s^i + 1, \qquad r \geqq 5, \quad s \geqq 7 \text{ and odd,} \tag{1.6}$$

$$m_3(5, s) \leqq s^3 - 1, \qquad s = 5, \tag{1.7}$$

$$m_3(r, s) \leqq s^{r-2} - 2s\sum_{i=0}^{r-6} s^i - 1), \qquad s = 5, \quad r \geqq 6, \tag{1.8}$$

$$m_3(5, s) \leqq s^3, \qquad s \text{ even,} \tag{1.9}$$

$$m_3(r, s) \leqq s^{r-2} - s\sum_{i=0}^{r-6} s^i, \qquad s \text{ even } r \geqq 6. \tag{1.10}$$

We obtain in Theorem 2, Section 4, a new bound which is an improvement over these results when $s = 3$, or s is even ($s > 2$). For $s = 5, r = 5$ our bound is the same as Barlotti's. In other cases Barlotti's bound is better. For lower bounds on $m_3(r, s)$ and other important results on non-collinear sets reference may be made to Segre [8].

2. Symmetric representation for $t = 3$. A set of points in finite projective space $PG(r - 1, s)$ of $r - 1$ dimensions, based on the Galois field GF_s where $s = p^h$ (p being a prime), is said to be a *non-collinear set* if no three of the points are collinear. The set is said to be complete if we cannot add any new point to the set, so that it still retains the property of non-collinearity. The maximum number of points in a non-collinear set in $PG(r - 1, s)$ may be denoted by $m_3(r, s)$. The same number in the notation used by Barlotti [1] would be denoted by $M_{r-1,s}$. Let

$$S = A_1, A_2, \cdots, A_m, \tag{2.1}$$

be a complete non-collinear set in $PG(r - 1, s)$. Since there are

$$N_r = (s^r - 1)/(s - 1), \tag{2.2}$$

distinct points in $PG(r - 1, s)$, there are $n = N_r - m$ points

$$B_1, B_2, \cdots B_n, \qquad n = N_r - m \tag{2.3}$$

not contained in the set S given by (2.1). We will denote by $\bar{S}$ the set of points (2.3).

From the property of non-collinearity no line in $PG(r - 1, s)$ can intersect the set S in more than two points. A line will be said to be a *secant* of S, if it intersects S in two distinct points, it will be said to be a *tangent* to S if it intersects S in a single point, and will be said to be a *non-intersector* if it contains no point of S.

Through each of the points B_i in (2.3) there must pass at least one secant of S. If not $A_1, A_2, \cdots A_m, B_i$ would be a non-collinear set contradicting the property of completeness. Let u_i be the number of secants through B_i ($i = 1, 2, \cdots, n = N_r - m$), $1 \leqq u_i \leqq [m/2]$, where $[x]$ denotes the largest integer not exceeding x. On every secant there must occur exactly $s - 1$ of the points B, since each line of $PG(r - 1, s)$ has exactly $s + 1$ points.

The secants can be exhibited in a tabular form as follows, where the ith row shows the secants passing through B_i.

$$\begin{array}{llll}
B_1A_{111}A_{112}, & B_1A_{121}A_{122}, & \cdots, & B_1A_{1u_11}A_{1u_12} \\
B_2A_{211}A_{212}, & B_2A_{221}A_{222}, & \cdots, & B_2A_{2u_21}A_{2u_22} \\
\cdots, & \cdots, & \cdots, & \cdots \\
B_iA_{i11}A_{i12}, & B_iA_{i21}A_{i22}, & \cdots, & B_iA_{iu_i1}A_{iu_i2} \\
B_nA_{n11}A_{n12}, & B_nA_{n21}A_{n22}, & \cdots, & B_nA_{nu_n1}A_{nu_n2}.
\end{array} \tag{2.4}$$

Here the points A_{ijk}

$$1 \leqq i \leqq m, \qquad 1 \leqq j \leqq u_i, \qquad 1 \leqq k \leqq 2$$

belong to the non-collinear set $S = A_1, A_2, \cdots, A_m$, and the points $B_1, B_2, \cdots, B_n$ belong to the complementary set $\bar{S}$.

The coordinates of B_i can be represented by the vector

$$\mathbf{b}_i = (b_{i1}, b_{i2}, \cdots, b_{ir}) \qquad i = 1, 2, \cdots, n = N_r - m \tag{2.5}$$

and the coordinates of A_t by the vector

$$\mathbf{a}_t = (a_{t1}, a_{t2}, \cdots, a_{tr}) \qquad t = 1, 2, \cdots, m. \tag{2.6}$$

The relations between these vectors then can be exhibited as

$$\mathbf{b}_i = \lambda_{i1}(\mathbf{a}_{i11} + \rho_i \mathbf{a}_{i12}) = \lambda_{i2}(\mathbf{a}_{i21} + \rho_i \mathbf{a}_{i22}) = \cdots = \lambda_{iu_i}(\mathbf{a}_{iu_i1} + \rho_{iu_i}\mathbf{a}_{iu_i2}), \tag{2.7}$$

where λ's and ρ's are non-zero elements of GF_s and the $\mathbf{a}$'s belong to the set of vectors $\mathbf{a}_1, \mathbf{a}_2, \cdots \mathbf{a}_m$ representing the points of S, $(i = 1, 2, \cdots, n)$.

The scheme (2.4) or its vector equivalent (2.7) may be called the symmetric representation for $t = 3$. It specifies the structure of the complete non-collinear set $S = A_1, A_2, \cdots, A_m$. We shall use this scheme for obtaining an upper bound on $m_3(r, s)$. This scheme can also be used for constructing non-collinear sets, but this will be considered in a separate paper.

3. Proper and improper non-collinear sets. Consider the complete non-collinear set S given by (2.1). A plane Π cannot contain more than $s + 2$ points of S when s is even, and more than $s + 1$ points when s is odd, from the result due to Bose [2] mentioned in the introduction, since the points of S contained in Π must themselves form a non-collinear set.

We shall call the non-collinear set S, *improper* if there is at least one plane Π which contains $s + 2$ points of S. In this case s must be even. We shall call the non-collinear set S proper if there is no plane Π which contains $s + 2$ points of S. In this case s may be odd or even.

Let the complete non-collinear set $S = A_1, A_2, \cdots, A_m$ be improper, and let Π be a plane which contains $s + 2$ points of S, which may without loss of generality be taken to be $A_1, A_2, \cdots A_{s+2}$. Through the plane Π there pass $N_{r-3} = (s^{r-3} - 1)/(s - 1)$, 3-spaces of $PG(r - 1, s)$. Now from the result of Qvist [7] mentioned in the Introduction, no 3-space can contain more than $s^2 + 1$ points of S. Hence each 3-space contains $s^2 - s - 1$ or less points other than $A_1, A_2, \cdots, A_{s+2}$. We therefore have the theorem:

THEOREM 1. *The number of points m in an improper non-collinear set in $PG(r - 1, s)$, $s > 2$, satisfies the inequality*

$$m \leqq (s + 2) + (s^2 - s - 1)N_{r-3}. \tag{3.1}$$

4. Some useful lemmas. The number u_i of the secants of S, passing through B_i may be called the weight of B_i. We may write

$$u_i = w(B_i). \tag{4.1}$$

Each of the points A, contained in a secant through B_i may be supposed to contribute a weight $\frac{1}{2}$ to B_i. The weight of B_i is then the sum of the weights of all the points A, lying on secants through B_i, i.e. the weight of all the points A occurring in the ith row of the scheme (2.4).

LEMMA 1. $\sum_{i=1}^{n} u_i = \frac{1}{2}m(m-1)(s-1)$, $n = N_r - m$.

The number of distinct secants of the set S is exactly $m(m-1)/2$ since any secant must contain exactly two points of S. Consider the secant passing through the points A_i and A_j. There are exactly $s-1$ of the points B, on A_iA_j. The points A_i and A_j each contribute a weight $\frac{1}{2}$ to each of these $s-1$ points, and to no other points B. Hence the total weight of the points B is $m(m-1)(s-1)/2$. This proves the Lemma.

We shall define the weight of a secant A_iA_j as the sum of weights of all the $s-1$ points B, contained in A_iA_j, and denote this weight by $w(A_iA_j)$

LEMMA 2. $\sum_{i<j} w(A_iA_j) = \sum_{i=1}^{n} u_i^2$, $i, j = 1, 2, \cdots, m$.

Consider any point B_i. There are u_i secants passing through it. Hence in counting the weight of all the secants, the weight of B_i is counted u_i times. This proves the result.

LEMMA 3. *If the non-collinear set* $S = A_1, A_2, \cdots, A_m$ *is proper*

$$w(A_iA_j) \leqq (s-1) + \tfrac{1}{2}(m-2)(s-2). \tag{4.2}$$

Let $B_{ij1}, B_{ij2}, \cdots, B_{ij,s-1}$ be the points of $\bar{S}$ lying on A_iA_j. By definition

$$w(A_iA_j) \leqq \sum_{k=1}^{s-1} w(B_{ijk}). \tag{4.3}$$

Let A_t be a point of S distinct from A_i and A_j. If A_k contributes a weight $\frac{1}{2}$ to B_{ijk}, there exists a point A_k of S (distinct from A_i, A_j, A_t) such that the line A_tA_k passes through B_{ijk}. If A_t contributes a weight $\frac{1}{2}$ to each of the points $B_{ij1}, B_{ij2}, \cdots, B_{ij,s-1}$, then there exist distinct points $A_1, A_2, \cdots A_{s-1}$ (distinct from A_i, A_j, A_t) of S, lying in the plane $A_iA_jA_t$. Hence this plane has $s+2$ points of S, which contradicts the fact that S is proper. Hence A_t can contribute a weight $\frac{1}{2}$ to utmost $s-2$ of the points B on A_iA_j. Hence the total weight contributed by the $m-2$ points of S not lying on A_iA_j to points of $\bar{S}$ on A_iA_j does not exceed $(m-2)(s-2)/2$. On the other hand each of the points A_i and A_j contributes a weight $\frac{1}{2}$ to each of the points $B_{1j1}, B_{1j2}, \cdots, B_{1j,s-1}$. Hence

$$\sum_{k=1}^{s-1} w(B_{ijk}) \leqq (s-1) + \tfrac{1}{2}(m-2)(s-2). \tag{4.4}$$

This proves the Lemma.

5. Upper bound on the number of points contained in a non-collinear set in $PG(r-1, s)$, where $s > 2$. First let the non-collinear set $S = A_1, A_2, \cdots, A_m$ be proper and complete. Then from Lemmas 2, and 3,

$$\tfrac{1}{2}m(m-1)\{\tfrac{1}{2}(m-2)(s-2) + (s-1)\} \geqq \sum u_i^2. \tag{5.1}$$

Also from Lemma 1

$$(5.2)\quad \sum u_i^2 \geqq (1/n)(\sum u_i)^2 = m^2(m-1)^2(s-1)^2/4(N_r - m).$$

$$n = N_r - m$$

Hence from (5.1) and (5.2) we have

$$(5.3)\quad m^2(s^2 - s - 1) - m\{(s^2 - 2s - 1) + N^r(s-2)\} - 2N_r \leqq 0.$$

Hence m cannot exceed the positive root of the quadratic equation

$$(5.4)\quad x^2(s^2 - s - 1) - x\{(s^2 - 2s - 1) + N_r(s-2)\} - 2N_r = 0.$$

If the non-collinear set S is improper and $s > 2$, then $s = 2^n$, where $n \geqq 2$. One can check after some calculation that in this case the result of replacing x in the left hand side of (5.4) by $(s+2) + (s^2 - s - 1)N_{r-3}$ is negative if $r \geqq 4$. Hence the upper bound on m given by (3.1) is smaller than the upper bound on m given by (5.5). The later bound is therefore valid in all cases where $s > 2$, $r \geqq 4$. If we have a non-collinear set which is incomplete then we can add more points to it to make it a complete non-collinear set. Hence we have the theorem:

THEOREM 2. *If $m_3(r, s)$ denotes the maximum possible number of points in any non-collinear set in $PG(r-1, s)$, then $m_3(r, s)$ cannot exceed the positive root of the equation* (5.3), *if $s > 2$, $r \geqq 4$.*

Hence if $s > 2, r \geqq 4$, $m_3(r, s) \leqq \psi(r, s)$ where $\psi(r, s)$ is given by

$$(5.5)\quad \psi(r, s) \leqq \{N_r(s-2) + (s^2 - 2s - 1) + [N_r^2(s-2)^2 + 2N_r(s^3 - s - 2) + (s^2 - 2s - 1)^2]^{\frac{1}{2}}\}/2(s^2 - s - 1)$$

where $N_r = (s^r - 1)/(s-1)$.

6. Discussion of special cases, and comparison with previously known bounds.

(a) Consider the special case $s = 3$, $r \geqq 5$. Let $f(x)$ denote the left hand side of (5.4). Then $f(x) = 5x^2 - x(2 + N_r) - 2N_r$, where $N_r = (3^r - 1)/2$. Let $u = (2 + N_r)/5$. Then $f(u+1) = 7 - N_r < 0, f(u+2) = 24 > 0$. Hence $\psi(r, s)$ lies between $u+1$ and $u+2$. Thus

$$m_3(r, s) \leqq \psi(r, s) < (N_r + 12)/5 = (3^r + 23)/10.$$

The best previously known bound due to Tallini [10] is given by (1.5) which in this case reduces to $m_3(r, s) \leqq 3^r/9$.

Hence for this case the bound given by (5.5) is always better than the bound given by (1.5).

(b) Consider the special case $s > 3$, $r = 5$. Denoting the left hand side of (5.4) by $f(x)$ we have $f(x) = x[x(s^2 - s - 1) - (s^2 - 2s - 1) - N_5(s-2)] - 2N_5$. Let

$$u = [(s^2 - 2s - 1) - N_5(s-2)]/(s^2 - s - 1) = s^5 - \{3(s+1)/(s^2 - s - 1)\}.$$

For any c

$$f(u + c) = (u + c)c(s^2 - s - 1) - 2N_5$$
$$= N_5[c(s - 2) - 2] + c(s^2 - 2s - 1) + c^2(s^2 - s - 1).$$

Taking $c = 3(s + 1)/(s^2 - s - 1)$, we see that $f(s^3) > 0$. Taking $c = -1 + [3(s + 1)/(s^2 - s - 1)]$, we find that $f(s^3 - 1) < 0$. Hence $\psi(r, s)$ lies between $s^3 - 1$ and s^3. We therefore have $m_3(5, s) \leqq s^3 - 1$.

This equals the Barlotti's bound given by the Equation (1.7) for the case $s = 5$, and improves Barlotti's bound given by the Equation (1.9) when s is even.

(c) Consider the case when s is even, $s > 2$, $r \geqq 6$. As before let $f(x)$ denote the left hand side of (5.4) and let

$$u = [(s^2 - 2s - 1) - N_r(s - 2)]/(s^2 - s - 1).$$

Then

$$f(u) = -2N_r < 0, \qquad f(u + 1) = (s - 4)N_r + (s - 2)(2s + 1).$$

Hence $\psi(r, s)$ lies between u and $u + 1$. Thus $m_3(r, s) \leqq \psi(r, s) < u + 1$.

It is easy to check that in this case $u + 1$ is less than the right hand side of the Equation (1.10), so that our bound is an improvement over that given by Barlotti.

REFERENCES

[1] BARLOTTI, A. (1957). Una limitazione superiore per il numero di punti appartenenti a una calotta $\mathcal{C}(k, o)$ di uno spazio lineare finito. *Boll. Un. Mat. Ital.* **12** 67–70.

[2] BOSE, R. C. (1947). Mathematical theory of the symmetrical factorial design. *Sankhyā* **8** 107–166.

[3] BOSE, R. C. (1961). On some connections between the design of experiments and information theory. *Bull. de l'Institute International de Statist.* **38** 4e 257–271.

[4] FISHER, R. A. (1942). The theory of confounding in factorial experiments in relation to the theory of groups. *Ann. Eugen. London* **11** 341–353.

[5] FISHER, R. A. (1945). A system of confounding for factors with more than two alternatives giving completely orthogonal cubes and higher powers. *Ann. Eugen. London* **12** 283–290.

[6] HAMMING, R. W. (1950). Error detecting and error correcting codes. *Bell System Tech. J.* **29** 147–160.

[7] QVIST, B. (1952). Some remarks concerning curves of the second degree in a finite plane. *Ann. Acad. Sci. Fenn. Ser. A, I.* No. 134.

[8] SEGRE, B. (1957). Le geometrie di Galois. *Ann. of Math.* **48** 1–97.

[9] SEIDEN, E. (1950). A theorem in finite projective geometry and an application to statistics. *Proc. Amer. Math. Soc.* **1** 282–286.

[10] TALLINI, G. (1956). Sulla k-calotta di uno spazio lineare finito. *Ann. of Math.* **42** 119–164.