BOUNDS FOR k-CAPS IN PG(r,q) USEFUL IN THE THEORY OF ERROR CORRECTING CODES

by

A. Barlotti*

University of North Carolina

Institute of Statistics Mimeo Series No. 484.2

August 1966

This research was supported by the Air Force Office of Scientific Research Contract No. AF-AFOSR-760-65 and also partially supported by Contract No. DA-31-124-AROD-254, U.S. Army Research Office-Durham.

DEPARTMENT OF STATISTICS

UNIVERSITY OF NORTH CAROLINA

Chapel Hill, N. C.

* On leave from the University of Florence.

The connection between information theory and finite geometries has been established in various papers by R. C. Boxe (see [4] for references). A complete introduction to the theory of these geometries can be found in the volume of B. Segre [10].

Consider a finite r-dimensional projective space PG(r,q), based on the Galois field GF(q), where $q = p^h$, p prime. A k-cap in PG(r,q) is a set of k points no three of which are collinear. If we denote by $m_s(r+1,q)$ the maximum number of points in PG(r,q) such that no s of them are dependent, $m_3(r+1,q)$ is the number of points belonging to a k-cap of PG(r,q) for which k is maximal. The usefulness of knowing the values of $m_s(r+1,q)$ in coding theory has been emphasized by R. C. Bose and I. M. Chakravarti in this volume (see [5] and [7]).

The known values of $m_3(r+1,q)$ are given below (see [3] and [8]).

$$m_3(2,q) = 2,$$

$$m_3(3,q) \begin{cases} = q + 1 & (q \text{ odd}) \\ = q + 2 & (q \text{ even}) , \end{cases}$$

$$m_3(4,q) = q^2 + 1 \qquad (\text{any } q),$$

$$m_3(r+1,2) = 2^r .$$

We shall mention some bounds on $m_3(r+1,q)$ in the cases $r > 3$, $q > 2$ in which the values of $m_3(r+1,q)$ are unknown. The first upper bound was obtained by R. C. Bose [3]:

Theorem 1. For $m_3(r+1,q)$ the following inequality holds:

$$m_3(r+1,q) \leq 1 + \frac{q^r - 1}{q - 1} .$$

If q is odd, then

$$m_3(r+1,q) \leq q^{r-1} + 1.$$

A first improvement of this was found by Tallini [9]:

Theorem 2. If $r > 3$, $q > 2$, then

$$m_3(r+1,q) < q^{r-1} + 1.$$

Further improvements on the upper bound on $m_3(r+1,q)$ were obtained by A. Barlotti [2], B. Segre [9] and Bose and Srivastava [6]. We shall give these results with some improvements for the cases in which they are the best known.

Theorem 3. In $PG(4,q)$, $q \geq 7$ odd, we have

$$m_3(5,q) \leq q^3 - q^2 + 8q - 14.$$

In geometric language: if a k-cap exists in $PG(4,q)$ $q \geq 7$ odd, then

$$k \leq q^3 - q^2 + 8q - 14.$$

Proof: For convenience of the reader we shall give here the whole proof although, apart from some initial change, it is the same as in [9], § 24.

Suppose there exists a k-cap K in $PG(4,q)$ with $k \geq q^3 - q^2 + 8q - 13$. We will prove that this leads to a contradiction.

A plane which cuts K in a $(q+1)$-arc will be called a plane of the first kind. A hyperplane which cuts K in at least $q^2 - q + 7$ points will be called a hyperplane of the first kind. The following three lemmas are required for the proof.

Lemma 1. In $PG(3,q)$, $q \geq 7$ odd, any k-cap with $k \geq q^2 - q + 7$ belongs to an elliptic quadric.

The proof is given in [1].

Lemma 2. Through any secant of K there pass at least $9q-14$ planes of the first kind.

If not, then by counting the points on the different $q^2 + q + 1$ planes through a secant, we get

$$k \leq 2 + (9q-15)(q-1) + [(q^2+q+1)-(9q-15)](q-2) =$$

$$= q^3 - q^2 + 8q - 15$$

Lemma 3. Through any plane of the first kind there pass at least five hyperplanes of the first kind.

If not, then by counting the points on the hyperplanes passing through a plane of the first kind, we have

$$k \leq (q+1) + 4[q^2+1-(q+1)] + (q-3)[q^2-q+6-(q+1)]$$

$$= q^3 - q^2 + 8q - 14$$

We now proceed to the proof of Theorem 3. Let π be a plane of the first kind and let S' and S'' be hyperplanes of the first kind passing through π. Denote the conic in which π cuts K by C, and by Q' and Q'' the elliptic quadrics containing the points of K in S' and S'', respectively. Obviously Q' and Q'' cut π in C.

Let A be a point on C and P a point of K not contained in either S' or S''. (The existence of P is easily shown by counting points). There are at least $(9q-14)-(q+1) = 8q-15$ planes of the first kind through the secant AP which do

not cut π in a line. Let ρ be one of these planes. Of the q+1 hyperplanes passing through ρ, there is at most one tangent to Q' at A. The same statement holds for Q". By Lemma 3, there are at least three hyperplanes of the first kind passing through ρ which are not tangent to either Q' or Q" at A. Let S be one of these hyperplanes, let Q be the elliptic quadric which contains the points of K in S, and denote by π' and π'' the intersections of S with S' and S", respectively. π' and π'' are different from π since π does not belong to S. For if $\pi \in S$, then π would intersect ρ in a line.

The plane π' is not tangent to Q', and therefore intersects Q' in an irreducible conic C'. There are at most $(q^2+1)-(q^2-q+7) = q-6$ points in Q' which do not belong to K. Thus there are at least $(q+1)-(q-6) = 7$ points of K on C'. But these 7 points belong to Q, and therefore Q contains C'. Similarly Q contains C", the intersection of K and π''. Since π' and π'' are different from π, C' is different from C".

There is exactly one hyperquadric V in PG(4,q) which contains Q', Q", and P. Q cuts V in C', C", and P, and so Q belongs to V and is the intersection of V with S. Since Q, Q', and Q" are non-degenerate quadrics, V is either non-degenerate or else a cone having a single point as vertex. In the latter case, since Q is an elliptic quadric, V is a cone having a point as vertex and which projects an unruled quadric. We will show that V contains all points of K.

All the points of K belonging to S, S', S" lie in V. Let P* be any point of K not belonging to S, S', or S". We want to prove that P* belongs to V. Let ρ^* be a plane of the first kind passing through the secant PP* and which does not intersect π in a line. Clearly ρ^* does not belong to either S' or S". There are at least five hyperplanes of the first kind passing through ρ^*. Of these, two can be tangent to Q' and two others tangent to Q". There is at least one hyperplane S* which is tangent to neither of these quadrics. S* can-

not contain π since ρ^*, which is in S^*, does not cut π in a line.

Let Q^* be the elliptic quadric which contains the points of K in S^*, and let Γ' and Γ'' be the intersections of S^* with Q' and Q'', respectively. Then, as we saw before, Γ' and Γ'' must be different irreducible conics which belong to Q^*. But Q^* intersects V in Γ', Γ'', and P, and so Q^* belongs to V. But P^* belongs to Q^*, and thus P^* belongs to V. It follows that V contains K. This implies[1] $k \leq 2(q^2+1)$. We have

$$q^3 - q^2 + 8q - 13 \leq k \leq 2(q^2+1)$$

$$q^3 - 3q^2 + 8q - 15 \leq 0$$

The last inequality is impossible for $q \geq 3$. This contradiction completes the proof.

Theorem 4. If a k-cap exists in PG(r,q) with $r > 4$, $q \geq 7$ odd, then

$$k < q^{r-1} - q^{r-2} + 8q^{r-3} - 6\sum_{i=0}^{r-4} q^i - 8.$$

Alternatively

$$m_3(r+1,q) < q^{r-1} - q^{r-2} + 8q^{r-3} - 6\sum_{i=0}^{r-4} q^i - 8.$$

Proof: The proof is the same as that of Theorem 3 in [9], 24:

We have two cases.

Case 1: There is a 3-flat which contains at least q^2-q points of K. Then by counting the number of points of K which lie on 4-flats passing through this 3-flat and using Theorem 3 we have

(1). See [9], § 20.

(i) $$k \leq (q^2-q) + (q^{r-4} + \ldots + q + 1)\,[(q^3 + 8q - 14) - (q^2 - q)]$$

$$= q^{r-1} - q^{r-2} + 8q^{r-3} - 6\sum_{i=0}^{r-4} q^i - 8$$

Case 2: No 3-flat contains q^2-q points of K. The number of pairs of points of K and 3-flats passing through these points is

$$k \cdot \frac{(q^r-1)(q^{r-1}-1)(q^{r-2}-1)}{(q^3-1)(q^2-1)(q-1)} .$$

(See B. Segre [10] §167). On the other hand, since every 3-flat contains less than q^2-q points of K, the number of pairs is not greater than

$$(q^2-q) \cdot \frac{(q^{r+1}-1)(q^r-1)(q^{r-1}-1)(q^{r-2}-1)}{(q^4-1)(q^3-1)(q^2-1)(q-1)} .$$

Combining these results, we have

(ii) $$k < (q^2-q)\,\frac{q^{r+1}-1}{q^4-1} .$$

An upper bound for k in the general case is given by the larger of the expressions on the right-hand sides of (i) and (ii). It is easily shown that (i) is larger than (ii).

Theorem 5. If a k-cap exists in PG(r,q) with $r > 4$, $q = 7$, then

$$k \leq q^{r-1} - \sum_{i=1}^{r-3} q^i$$

Alternatively

$$m_3(r+1,7) \leq 7^{r-1} - \sum_{i=1}^{r-3} 7^i$$

for $r > 4$.

Proof: There are three cases to consider.

Case 1: There is a secant to K such that no plane through this secant cuts K in a $(q+1)$-arc. By counting the points of K on the planes through this secant we have

(i) $$k \leq q^{r-1} - \sum_{i=1}^{r-2} q^i$$

Case 2: There is a plane α which cuts K in a $(q+1)$-arc but such that no 3-flat through α cuts K in a (q^2+1)-cap. By counting points of K on these 3-flats through α, we have

(ii) $$k \leq q^{r-1} - \sum_{i=1}^{r-3} q^i$$

Case 3: There is at least one 3-flat S which cuts K in a (q^2+1)-cap. By counting points of K on the 4-flats through S we obtain, using Theorem 3,

(iii) $$k \leq q^2 + 1 + [q^3 - q^2 + 8q - 14 - (q^2+1)] \sum_{i=0}^{r-4} q^i$$

$$= q^{r-1} - q^{r-2} + 7q^{r-3} - 8 \sum_{i=1}^{r-4} q^i + q - 14.$$

Comparing (i), (ii), and (iii), we see that the upper bound given by (ii) is largest. Hence in the general case this is an upper bound for k.

Theorem 6. If a k-cap exists in PG(4, q), $q = 5$, then

$$k \leq q^3 - 1$$

Alternatively

$$m_3(5,5) \leq 124.$$

(The proof is given in [2]).

Theorem 7. If a k-cap exists in PG(r,q), $r > 4$, $q = 5$, then

$$k \leq q^{r-1} - 2q \sum_{i=0}^{r-5} q^i - 1$$

Alternatively

$$m_3(r+1,5) < 5^{r-1} - 10 \sum_{i=0}^{r-5} 5^i - 1 \quad \text{for } r > 4.$$

(The proof is given in [2]).

Theorem 8. If $q > 2$, $r \geq 3$, then the maximum possible number of points in any k-cap in PG(r,q) cannot exceed the positive root of the quadratic equation

$$f(x) = (q^2-q-1)\, x^2 - [q^2-2q-1+(q-2) \sum_{i=0}^{r} q^i]\, x - 2 \sum_{i=0}^{r} q^i = 0.$$

The proof is given in [6]. Using this theorem we obtain improvements over previous results in the following special cases ([6] § 6):

$$m_3(r+1,3) \leq \frac{3^{r+1} + 23}{10} \quad r \geq 4,$$

$$m_3(5,q) \leq q^3 - 1 \qquad q > 2 \text{ even},$$

$$m_3(r+1,q) < \frac{q^2-2q-1+(q-2)\sum_{i=0}^{r} q^i}{q^2 - q - 1} + 1, \quad q > 2, \text{ even}.$$

This last bound is improved by the following theorem:

Theorem 9. In PG(r,q), $r > 4$, $q > 2$ even,

$$m_3(r+1,q) \leq q^{r-1} - 2 \sum_{i=1}^{r-4} q^i \qquad -1.$$

The proof is similar to that of Theorem 5, using the bound $m_3(5,q) \leq q^3-1$ given by the previous theorem. We must consider the additional case in which a plane cuts the k-cap in a $(q+2)$-arc, however.

REFERENCES

[1]. A. Barlotti, Un'osservazione sulle k-calotte degli spazi lineari finiti di dimensione tre. Boll. Un. Mat. Ital. (3) 11 (1956), 248-252.

[2]. A. Barlotti. Una limitazione superiore per il numero di punti appartenenti a una k-calotta C(k,0) di uno spazio lineare finito. Boll. Un. Mat. Ital. (3) 12 (1957), 67-70.

[3]. R.C. Bose, Mathematical theory of the symmetrical factorial design Sankhya, 8 (1947), 107-166.

[4]. R.C. Bose, On some connections between the design of experiments and information theory. Bull. of the International Statistical Institute, 38 part IV (1961).

[5]. R.C. Bose, Error correcting, error detecting and error locating codes. Mimeo Series No. 426, University of North Carolina (1965).

[6]. R.C. Bose and J.N. Srivastava, On a bound useful in the theory of factorial designs and error correcting codes. Ann. Math. Statist. 35 (1964),408-414.

[7]. I.M. Chakravarti, Bounds on error correcting codes (non-random). Mimeo Series No. 451, University of North Carolina, (1965).

[8]. B. Qvist., Some remarks concerning curves of the second degree in a finite plane. Ann. Acad. Sci. Fenn. Ser. A. I. 134 (1952), pp. 1-27.

[9]. B. Segre, Le geometrie di Galois. Ann. Mat. Pura. Appl. (4) 48(1959),1-97.

[10]. B. Segre, Lectures on Modern Geometry, with an appendix by Lucio Lombardo-Radice. Cremonese, Rome, 1961.

[11]. G. Tallini, Sulle k-calotte di uno spazio lineare finito. Ann. Mat. Pura Appl. (4) 42 (1956), 119-164.