Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Raymond Hill

On the largest size of cap in $S_{5,3}$

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **54** (1973), n.3, p. 378–384.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1973_8_54_3_378_0>

Geometria. — *On the largest size of cap in* $S_{5,3}$. Nota di RAYMOND HILL, presentata (*) dal Socio B. SEGRE.

RIASSUNTO. — Si dimostra che, in uno spazio di Galois di dimensione 5 ed ordine 3, l'ordine massimo delle calotte (ovoidi) è 56. Nella dimostrazione intervengono varie riposte considerazioni gruppali, nonchè la realizzazione di un disegno simmetrico recentemente considerato.

INTRODUCTION

Let $S_{r,q}$ denote a projective space of r dimensions over $GF(q)$, the Galois field of q elements. The points of $S_{r,q}$ are homogeneous $(r+1)$-tuples $(x_1, x_2, \cdots, x_{r+1})$, where $x_i \in GF(q)$ and not all the x_i's are zero; $(x_1, x_2, \cdots, x_{r+1}) = (y_1, y_2, \cdots, y_{r+1})$ if and only if $x_i = \lambda y_i$ for all i, for some $\lambda \in GF(q)$, $\lambda \neq 0$. A *k-cap* in $S_{r,q}$ is a set of k points, no three of which are collinear. The problem of finding the maximum size $m(r, q)$ of cap in $S_{r,q}$ has proved difficult, and only the following results are known to date:

Bose [1], 1947:	$m(r, 2) = 2^r$,	$r \geq 2$.
	$m(2, q) = q + 1$,	q odd.
	$m(2, q) = q + 2$,	q even.
	$m(3, q) = q^2 + 1$,	q odd.
Qvist [7], 1952:	$m(3, q) = q^2 + 1$,	q even.
Pellegrino [6], 1970:	$m(4, 3) = 20$.	

For $r \geq 4$, a comprehensive list of upper bounds on $m(r, q)$ is given by Segre [9], and lower bounds are found in [8]. Putting the best of these results together for the particular case of caps in $S_{5,3}$ gives

$$37 \leq m(5, 3) \leq 75.$$

In this work we show that

$$m(5, 3) = 56.$$

Section 1 is devoted to showing that $m(5, 3)$ is at most 56. In Section 2 we construct a 56-cap in $S_{5,3}$, which at the same time gives a new presentation of the recently-discovered symmetric block design with parameters (56, 56, 11, 11, 2). The result of Section 2 arises out of an investigation into a certain class of rank 3 permutation groups, as presented in [4].

(*) Nella seduta del 10 marzo 1973.

1. $m(5, 3) \leq 56$.

In this section we will show that no cap in $S_{5,3}$ can have size greater than 56. We first list the known $m(r, 3)$'s for $r \leq 4$, all of which are required later:

LEMMA 1. $m(2, 3) = 4$, $m(3, 3) = 10$, $m(4, 3) = 20$.

Let K be a k–cap in $S_{r,q}$. Denote the points of K by $A_1, A_2, \cdots, A_k$ and those of $S_{r,q}$ not in K by $B_1, B_2, \cdots$. No line in $S_{r,q}$ can intersect K in more than two points. A line is called a *secant* of K if it intersects K in two distinct points, A_i, A_j say, and is denoted $(A_i A_j)$. For each point B_i in $S_{r,q}$–K, let u_i be the number of secants of K through B_i; u_i is called the *weight* of B_i. For a secant $(A_i A_j)$ we define the weight of $(A_i A_j)$, denoted $w(A_i A_j)$, to be the sum of the weights of the $(q-1)$ B_l's lying on the secant.

LEMMA 2. *If every secant of a k–cap* K *in* $S_{5,3}$ *has weight at most* 20, *then* $k \leq 56$.

Proof. As above, let $K = \{A_1, A_2, \cdots, A_k\}$, and let u_i $(i = 1, 2, \cdots, m)$ denote the weights of the m $(m = 364-k)$ points of $S_{5,3}$–K. Simple counting arguments (see, e.g., Lemmas 1 and 2 of [2]) give

$$\sum_{i=1}^{m} u_i = k(k-1)$$

and

$$\sum_{i=1}^{m} u_i^2 = \sum_{i<j} w(A_i A_j), \qquad i, j = 1, 2, \cdots, k.$$

By hypothesis, $w(A_i A_j) \leq 20$ for all i, j. Hence

$$1/m \left(\sum_{i=1}^{m} u_i \right)^2 \leq \sum_{i=1}^{m} u_i^2 \leq 20k(k-1)/2.$$

Hence
$$k^2(k-1)^2 \leq (364-k)\, 10k(k-1),$$

which reduces to

$$(k-56)(k+65) \leq 0,$$

giving $k \leq 56$.

Note. In Section 2, we shall exhibit a 56–cap in which every secant has weight 20, showing that Lemma 2 is best possible.

LEMMA 3. *If a k–cap in* $S_{5,3}$ *intersects any* $S_{3,3}$ *in* 8 *or more points, then* $k \leq 56$.

Proof. Let W be a 3–space in $S = S_{5,3}$ which intersects the k–cap K in h points, where $h \geq 8$. Let U_1, U_2, U_3, U_4 be the 4–spaces of S containing W.

Since $m(4, 3) = 20$,

$$|U_i \cap K| \leq 20, \qquad i = 1, 2, 3, 4.$$

Hence

$$|(U_i - W) \cap K| \leq 20 - h, \qquad i = 1, 2, 3, 4.$$

Since S is the disjoint union of W and the sets $U_i - W$, we have

$$\begin{aligned} k = |K| &\leq h + 4(20 - h) \\ &= 80 - 3h \\ &\leq 56, \quad \text{if} \quad h \geq 8. \end{aligned}$$

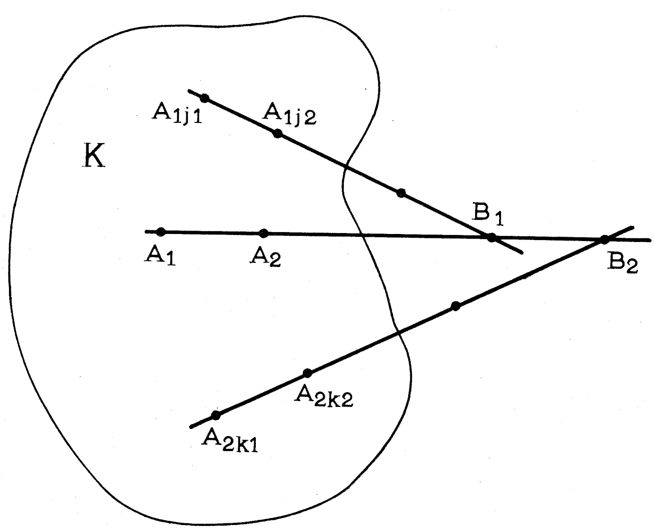
LEMMA 4. *Suppose* K *is a k-cap in* $S_{5,3}$ *containing points* $A_1 = (1,0,0,0,0,0)$ *and* $A_2 = (0,1,0,0,0,0)$, *so that* $(A_1A_2) = \{A_1, A_2, B_1, B_2\}$ *is a secant of* K, *where* $B_1 = (1, 1, 0, 0, 0, 0)$ *and* $B_2 = (1, 2, 0, 0, 0, 0)$. *Let the set of secants through* B_i $(i = 1, 2)$ *be*

$$\{(A_1A_2), (A_{ij1}A_{ij2}) \; ; \; j = 1, 2, \cdots, u_i - 1\},$$

where $A_{ij1} = (x_{ij}, y_{ij}, a_{ij}, b_{ij}, c_{ij}, d_{ij})$ *say, and* $A_{ij2} = A_{ij1} + B_i$.

Let $C_{ij} = (a_{ij}, b_{ij}, c_{ij}, d_{ij})$, $\quad i = 1, 2, \quad j = 1, 2, \cdots, u_i - 1$.

Then the C_{ij} *are distinct points of* $S_{3,3}$.



Proof. If $C_{ij} = C_{il}$, with $j \neq l$, then the set

$$\{A_1, A_2, A_{ij1}, A_{ij2}, A_{il1}, A_{il2}\}$$

is a 6-cap in an $S_{2,3}$, contradicting $m(2, 3) = 4$. If $C_{1j} = C_{2l}$, then at least five of the points $A_1, A_2, A_{1j1}, A_{1j2}, A_{2l1}, A_{2l2}$ are distinct, giving a 5-cap in $S_{2,3}$, again contradicting $m(2, 3) = 4$.

THEOREM 1. $m(5,3) \leq 56$.

Proof. Suppose K is a k–cap in $S_{5,3}$ with $k \geq 57$. By Lemma 2, there is a secant of K of weight at least 21. We may assume (by a suitable change of basis, if necessary) that this secant is (A_1A_2) with the notation of Lemma 4. Let L be the subset

$$\{C_{ij} : i = 1, 2 ; j = 1, 2, \cdots, u_i - 1\}$$

of $S_{3,3}$. If three points $C_{i_1j_1}, C_{i_2j_2}, C_{i_3j_3}$ of L are collinear, then the set

$$\{A_1, A_2, A_{i_lj_lm} : l = 1, 2, 3 ; m = 1, 2\}$$

is a set of 8 points of K lying in an $S_{3,3}$, which implies that $k \leq 56$ by Lemma 3. Thus, if $k \geq 57$, L is a cap in $S_{3,3}$ of size

$$u_1 + u_2 - 2 = w(A_1A_2) - 2 \geq 19,$$

contradicting $m(3,3) = 10$. This contradiction shows that

$$m(5,3) \leq 56.$$

2. $m(5,3) \geq 56$.

To complete the proof that $m(5,3)$ is 56, it is sufficient to exhibit a 56–cap in $S_{5,3}$.

If K is a k–cap in $S_{r,q}$, let Aut K be the group

$$\{t \in \mathrm{PGL}(r+1, q) : (P)t \in K, \quad \text{for all } P \in K\}.$$

For each of the known values of $m(r,q)$, there is a cap K of that size on which Aut K acts as a transitive permutation group. For example (see Theorem 10 of [9]), the only caps of size q^2+1 in $S_{3,q}$ are the elliptic quadrics, for which Aut K is $[\mathrm{PO}^-(4,q)]\,C_2$, an extension of the projective orthogonal group $\mathrm{PO}^-(4,q)$ by a cyclic group of order 2. In this case Aut K is even doubly-transitive on K.

On the other hand, it was shown in [4] that if G is a subgroup of $\mathrm{PGL}(r+1, q)$ acting on $S_{r,q}$ with two orbits, K and L say, then certain conditions of high transitivity of G on K imply that K is a cap in which every secant has the same weight, m say. For such a subgroup to exist, certain numerical relations must be satisfied. It was found that

$$q = 3 \quad , \quad r = 5 \quad , \quad |K| = 56 \quad , \quad m = 20$$

satisfy these relations, and this was our justification for proceeding in the following way, guessing that there is a 56–cap K in $S_{5,3}$ on which Aut K is transitive.

There are 112 points in an elliptic quadric in $S_{5,3}$. Perhaps there is some subgroup G of $\mathrm{PO}^-(6,3)$ under whose action these 112 points split into two orbits, each of size 56, with one (or each) of them a 56–cap. This turns out to be the case. Moreover the group G and an associated block design are of independent interest. We outline the construction:

(1). If K is a subset of order 56 of an elliptic quadric and if a subgroup G of $PO^{-}(6, 3)$ acts transitively on K, then G contains a Sylow 7–subgroup of $PO^{-}(6, 3)$ of order 7.

Let f be the quadratic form given by

$$(P, Q)f = \sum_{i=1}^{6} x_i y_i + \sum_{i=1}^{5} (x_i y_{i+1} + x_{i+1} y_i),$$

for $P = (x_1, x_2, \cdots, x_6)$ and $Q = (y_1, y_2, \cdots, y_6)$ in $S_{5,3}$. Then

$$t = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 \end{bmatrix}$$

has order 7, and since

$$(Pt, Qt)f = (P, Q)f,$$

for all P and Q in $S_{5,3}$, t is in the orthogonal group $PO^{-}(6, 3)$ consisting of isometries of f.

(2). Let X be the set of points in the elliptic quadric associated with f; i.e.

$$X = \{P \in S_{5,3} : (P, P)f = 0\}.$$

Under the natural action of t, X splits into 16 orbits, each containing 7 points:

$$X = \bigcup_{i=1}^{16} X_i .$$

Having listed the X_i it is a simple task to choose eight of them ($X_1, X_2, \cdots, X_8$, say) whose union K is a 56–cap. With f and t as above $K = \bigcup_{i=1}^{8} X_i$ is a 56–cap, where

$X_1 = \{(210000), (021000), (002100), (000210), (000021), (222221), (211111)\}$,

$X_2 = \{(201010), (020101), (221202), (100201), (202212), (101002), (121211)\}$,

$X_3 = \{(112000), (011200), (001120), (000112), (111122), (122220), (012222)\}$,

$X_4 = \{(110201), (200212), (101102), (121221), (201011), (212020), (021202)\}$,

$X_5 = \{(110202), (122101), (201102), (101221), (202011), (212120), (021212)\}$,

$X_6 = \{(111200), (011120), (001112), (111222), (122200), (012220), (001222)\}$,

$X_7 = \{(112200), (011220), (001122), (111220), (011122), (112220), (011222)\}$,

$X_8 = \{(211012), (102212), (121002), (120211), (201210), (020121), (221201)\}$.

Since we will now show that Aut K is transitive, the fact that K is indeed a cap follows if we show that just one point of K is not collinear with any other two, and this is readily checked. We have thus completed the proof of our main result, that $m(5, 3)$ is 56.

(**3**). A generating set for G = Aut K is $\{t, x, y, z, w\}$, where

$$x = \begin{bmatrix} 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 2&1&1&1&0&2\\ 0&0&0&2&0&0\\ 1&2&0&1&1&1\\ 1&2&0&0&0&1 \end{bmatrix} \quad y = \begin{bmatrix} 0&1&0&0&0&0\\ 1&0&0&0&0&0\\ 2&2&2&2&0&0\\ 0&0&0&1&0&0\\ 0&0&0&2&2&0\\ 0&0&0&0&0&2 \end{bmatrix} \quad z = \begin{bmatrix} 0&2&0&1&2&0\\ 2&0&0&1&2&0\\ 2&1&1&0&2&0\\ 1&2&0&1&1&0\\ 1&2&0&0&1&0\\ 2&0&0&2&2&1 \end{bmatrix} \quad w = \begin{bmatrix} 1&1&0&0&2&0\\ 2&0&0&0&2&0\\ 0&1&1&2&1&0\\ 0&2&0&1&0&0\\ 0&2&0&2&2&0\\ 0&1&0&0&1&1 \end{bmatrix}$$

(**4**). We now identify the group G. Let P be the point $(2, 1, 0, 0, 0, 0)$ of K. Then G_P, the stabilizer of P in G, is generated by $\{x, y, z, w\}$. G is transitive on K and has rank 3 with subdegrees 1, 10 and 45, for the orbits of G_P on K are $\{P\}$, $K_1(P)$ and $K_2(P)$, where

$$K_1(P) = \{(000210), (100201), (000221), (200212), (210122), (010202), (000012), (110202), (220102), (020121)\}.$$

We note that

$$K_1(P) = \{Q \in K : (P, Q)f = 0, \ Q \neq P\}$$

and

$$K_2(P) = \{Q \in K : (P, Q)f \neq 0\}.$$

We see also that $K_1(P)$ is a 10–cap in an $S_{3,3}$, and so by Theorem 10 of [9] is an elliptic quadric. It follows that G_P is isomorphic to $PO^-(4, 3)$. But $PO^-(4, 3)$ is isomorphic to the group $PGL(2, 9)$ (see, for example, page 25 of [10]), and it has been shown by Montague [5] that a rank 3 extension of this group with subdegrees 1, 10 and 45 is unique and is isomorphic to $[PSL(3, 4)]C_2$. This rank 3 representation of $PSL(3, 4)$ was found independently by Wales [11] and Montague [5], though not as a subgroup of $PGL(6, 3)$.

(**5**). The symmetric block design with parameters (56, 56, 11, 11, 2) (with the notation of [3]) is now presented in $S_{5,3}$, with points the points of K, and blocks the sets $\{Q \in K : (P, Q)f = 0\}$, one for each point P of K.

References

[1] R. C. BOSE, *Mathematical Theory of the Symmetrical Factorial Design*, « Sankhyā », *8*, 107–166 (1947).

[2] 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*, 408–414 (1964).

[3] M. HALL, *Combinatorial Theory*, Blaisdell, Waltham, Mass. (1967).

[4] R. HILL, *Rank 3 permutation groups with a regular normal subgroup*, Ph. D. Thesis, University of Warwick, September 1971.

[5] S. MONTAGUE, *On rank* 3 *groups with a multiply transitive constituent*, « J. Alg. », *14*, 506–522 (1970).

[6] G. PELLEGRINO, *Sul massimo ordine delle calotte in* $S_{4,3}$, « Matematiche », *25* (1970), 149–157 (1971).

[7] B. QVIST, *Some remarks concerning curves of the second degree in a finite plane*, « Ann. Acad. Sci. Fenn. Ser. AI », *134* (1952).

[8] B. SEGRE, *Le geometrie di Galois*, « Ann. Mat. Pura Appl. », *48*, 1–97 (1959).

[9] B. SEGRE, *Introduction to Galois geometries*, « Atti. Accad. Naz. Lincei », Mem., ser. VIII, 7 (1967).

[10] B. VAN DER WAERDEN, *Gruppen von Linearen Transformationen*, Chelsea, New York 1948.

[11] D. WALES, *Uniqueness of the graph of a rank 3 group*, « Pac. J. Math. », *30* (1), 271–277 (1969).