The largest cap in $AG(4,4)$ and its uniqueness

Yves Edel
Mathematisches Institut der Universität
Im Neuenheimer Feld 288
69120 Heidelberg (GERMANY),

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

Abstract

We show that 40 is the maximum number of points of a cap in $AG(4,4)$. Up to semi-linear transformations there is only one such 40-cap. Its group of automorphisms is a semidirect product of an elementary abelian group of order 16 and the alternating group A_5.

1 Introduction

A cap is a set of points no 3 of which are collinear. The maximum number of points of a cap in $PG(n,q)$ or $AG(n,q)$ for $n>3, q>2$ is known only in a few cases. In $PG(4,3)$ and $AG(4,3)$ the maximum is 20 (see Pellegrino [7]) and all these caps are known. In $PG(5,3)$ the maximum is 56 (Hill [6]), in $AG(5,3)$ the maximum is 45 [3]. In both cases the maximal caps are uniquely determined . The 45-cap in $AG(5,3)$ is an affine section of the Hill cap in $PG(5,3)$. Only one further value of the problem mentioned above is known: the maximum size of a cap in $PG(4,4)$ is 41 [2]. The proof that there are exactly two 41-caps in $PG(4,4)$ under the action of $P\Gamma L(5,4)$ will appear in a forthcoming paper.

In the present paper we prove the following:

Theorem 1. *The maximum number of points of a cap in $AG(4,4)$ is 40. Call a cap in $PG(4,4)$ affine if it avoids a hyperplane. There is only one orbit of affine 40-caps in $PG(4,4)$ under the action of $P\Gamma L(5,4)$ and two orbits under the action of $PGL(5,4)$. This cap is complete in $PG(4,4)$. Its group of automorphisms has order 960 and is transitive on the points of the cap.*

In Section 2 we construct the 40-cap in $AG(4,4)$, starting from its automorphism group. The proof of maximality and uniqueness is described in the final section.

2 Description of the maximal cap in $AG(4,4)$

We start from a description of the group of automorphisms. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,4)$. The mapping

$$A \mapsto \iota(A) = \left(\begin{array}{cc|cc|c} a & b & 0 & 0 & (ab)^2 \\ c & d & 0 & 0 & (cd)^2 \\ \hline 0 & 0 & a^2 & b^2 & ab \\ 0 & 0 & c^2 & d^2 & cd \\ \hline 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

describes an embedding $\iota : SL(2,4) \to SL(5,4)$. Let $W(B) = \begin{pmatrix} I & B \\ 0 & I \end{pmatrix} \in SL(5,4)$, where B is a $(2,3)$-matrix. Then $W = \{W(B)\}$ is an elementary abelian group of order 4^6 and $W(B_1)W(B_2) = W(B_1 + B_2)$. We have

$$\iota(A)^{-1} W(\begin{pmatrix} u & v & x \\ w & x & u \end{pmatrix})\iota(A) = W(\begin{pmatrix} U & V & X \\ W & X & U \end{pmatrix}) \qquad (1)$$

where

$$X = ad^2x + b^2cu + cd^2v + ab^2w,\ U = bc^2x + a^2du + c^2dv + a^2bw,$$

$$V = bd^2x + b^2du + d^3v + b^3w,\ W = ac^2x + a^2cu + c^3v + a^3w$$

Lemma 1. *Consider the standard action of $SL(2,4)$ on a 2-dimensional $\mathbb{F}_4$-vector space S with basis v_1, v_2 :*

$$Av_1 = av_1 + cv_2,\ Av_2 = bv_1 + dv_2$$

and let $\phi(A)$ *be the image of* A *under the Frobenius automorphism (i.e. the mapping* $\phi : I\!F_4 \to I\!F_4 : x \mapsto x^2$*). The tensor product* $S \otimes S$ *is a* 4*-dimensional* $I\!F_4$*-vector space with basis* $v_1 \otimes v_1, v_2 \otimes v_2, v_1 \otimes v_2, v_2 \otimes v_1$*. Let* $SL(2,4)$ *act on* $S \otimes S$ *such that* A *acts on the first component and* $\phi(A)$ *acts on the second component (*$v \otimes w \mapsto (Av) \otimes (\phi(A)w)$*).*

This action of $SL(2,4)$ *is similar to the permutation action as described in (1) of* $\iota(SL(2,4))$ *on the* $W(\begin{pmatrix} u & v & x \\ w & x & u \end{pmatrix})$*. The* $SL(2,4)$*-equivariant isomorphism is given by*

$$w(v_1 \otimes v_1) + v(v_2 \otimes v_2) + x(v_1 \otimes v_2) + u(v_2 \otimes v_1) \mapsto W(\begin{pmatrix} u & v & x \\ w & x & u \end{pmatrix})$$

This follows directly by inspection. Because of Lemma 1 each additive subgroup of $S \otimes S$, which is invariant under the action of $SL(2,4)$, describes a semidirect product embedded in $SL(5,4)$.

Lemma 2. *The* $I\!F_2$*-submodule (additive subgroup)* V *generated by* $\overline{\omega}(v_1 \otimes v_1), \overline{\omega}(v_2 \otimes v_2)$ *and the* $\overline{\omega}\delta(v_1 \otimes v_2) + \overline{\omega}\delta^2(v_2 \otimes v_1)$ *is an* $SL(2,4)$*-module under the action of* $SL(2,4)$ *from Lemma 1.*

Corollary 1. *The group* $\iota(SL(2,4))$ *acts by conjugation on the elementary abelian subgroup* V *consisting of* $W(\begin{pmatrix} u & v & x \\ w & x & u \end{pmatrix})$ *where* $v, w \in \{0, \overline{\omega}\}$ *and* $(x,u) = \overline{\omega}(\delta, \delta^2)$ *for some* $\delta \in I\!F_4$*. Denote by* G *the semidirect product* $V : SL(2,4) \subset SL(5,4)$*.*

Definition 1. *Let* K *be the orbit of* $P = (0,0,0,0,1)^T$ *under* G*.*

Lemma 3. *We have* $|K| = 40$*, and* K *consists of the points* $Q = (\overline{\omega}a\delta + \overline{\omega}b\delta^2 + (ab)^2, \overline{\omega}c\delta + \overline{\omega}d\delta^2 + (cd)^2, ab, cd, 1)$*, where* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,4)$ *and* $\delta \in I\!F_4$*.*

Proof. Application of $W(B)$ to P yields $(\overline{\omega}\delta, \overline{\omega}\delta^2, 0, 0, 1)^T$. Its image under $\iota(A)$ is

$$Q = (\overline{\omega}a\delta + \overline{\omega}b\delta^2 + (ab)^2, \overline{\omega}c\delta + \overline{\omega}d\delta^2 + (cd)^2, ab, cd, 1).$$

Assume $Q = P$. Then $ab = cd = 0$, which means that A is in a subgroup $SL(2,2)$. The first coordinates show $\delta(a + b\delta) = \delta(c + d\delta) = 0$. If $\delta \neq 0$ we obtain the contradiction $det(A)=0$. It follows that the stabilizer of P in G consists of those elements $\iota(A)W(B)$, where $\delta=0$ and $ab=cd=0$. This group has order $4\cdot 6$. The length of the orbit of P under G is therefore 40. ∎

Lemma 4. *The intersection of K with the hyperplane $x_4=0$ consists of the affine ovoid $V(\omega X_2^2+X_3^2+X_1X_5+X_2X_3)\setminus\{(1,0,0,0,0)\}$. The intersection of K with the hyperplane $x_3=0$ consists of the affine ovoid $V(\omega X_1^2+X_4^2+X_2X_5+X_1X_4)\setminus\{(0,1,0,0,0)\}$. Here $V(f(X_1,\dots,X_n))$ denotes the algebraic variety determined by the homogeneous polynomial $f(X_1,\dots,X_n)$.*

Proof. Consider point Q in Lemma 3, the generic image of P under an element of G. We have $Q\in(x_4=0)$ if and only if $cd=0$. There are $16\cdot 24$ elements of G having this property. As the stabilizer of P has order 24 it follows $|C\cap(x_4=0)|=16$. The points $Q\in K\cap(x_4=0)$ have the form $Q=(\overline{\omega}a\delta+\overline{\omega}b\delta^2+(ab)^2,\overline{\omega}c\delta+\overline{\omega}d\delta^2,ab,0,1)$. Its coordinates satisfy

$$\omega x_2^2=\overline{\omega}c^2\delta^2+\overline{\omega}d^2\delta^4=\overline{\omega}c^2\delta^2+\overline{\omega}d^2\delta$$

(because $\delta^4=\delta$) and

$$x_3^2+x_1x_5=\overline{\omega}a\delta+\overline{\omega}b\delta^2,\ x_2x_3=\overline{\omega}abc\delta+\overline{\omega}abd\delta^2.$$

Collecting terms we obtain

$$\omega(\omega x_2^2+x_3^2+x_1x_5+x_2x_3)=\delta(a+abc+d^2)+\delta^2(b+abd+c^2).$$

Recall $cd=0$. Assume $c=0$. Then $ad=1$ and the coefficient of δ^2 vanishes. The coefficient of δ is $a+d^2=(1+d^3)/d=0$. In case $d=0$ a symmetric argument applies. This shows that the points $Q\in C\cap(x_4=0)$ are on the quadric as claimed. Case $x_3=0$ follows by symmetry. ∎

Theorem 2. *The points of K form a cap.*

Proof. Recall that the 40 points of K form an orbit under the action of G and $P\in K$. Assume three points of K are collinear. Then there is a line through P containing two further points Q_1,Q_2 of K. The affine parts of these two points (the first four coordinates) must be scalar multiples of each other. Lemma 4 shows that this does not happen when these points satisfy $x_3=0$ or $x_4=0$. Consider a point $Q\in K$ such that $ab\neq 0, cd\neq 0$. We must have $ad\in\{\omega,\overline{\omega}\}$ and therefore $abcd=1$. It follows that such points satisfy $x_4=1/x_3$. For any two such points the pair (x_3,x_4) is one of $(1,1),(\omega,\overline{\omega}),(\overline{\omega},\omega)$. Any two such pairs which are scalar multiples of each other must be identical. ∎

Consider the hyperplanes

$$H_1 = (x_3 = 0),\ H_2 = (x_4 = 0),\ H_3 = (x_3 + x_4 + x_5 = 0),$$

$$H_4 = (\omega x_3 + \overline{\omega} x_4 + x_5 = 0),\ H_5 = (\overline{\omega} x_3 + \omega x_4 + x_5 = 0).$$

Then $\{H_1, H_2, H_3, H_4, H_5\}$ form an orbit under G. Clearly $\cap_{i=1}^5 H_i$ is the line $x_3 = x_4 = x_5 = 0$, and V acts on each H_i. The kernel of the permutation action of G on these hyperplanes is of course precisely V, and $\iota(SL(2,4))$ acts as A_5.

The intersection of K with hyperplane H_1 is an affine ovoid:

$$K \cap (x_3 = 0) = (x_3 = 0) \cap (x_5 = 1) \cap V(\omega X_1^2 + X_4^2 + X_2X_5 + X_1X_4).$$

The action of G shows that $K \cap H_i$ is an affine ovoid for all $i = 1, \ldots, 5$. In fact $K = \cup_{i=1}^5 (K \cap H_i)$, and each point of K is in precisely two of the hyperplanes H_i. Further $H_i \cap H_j \cap K$ has precisely 4 points whenever $i \neq j$, and K is the disjoint union of $H \cap H' \cap K$, where $\{H, H'\}$ varies over the pairs of our hyperplanes.

3 Maximality and uniqueness

We show that the affine 40-cap K described in Section 2 is up to the action of the group $P\Gamma L(5,4)$ of semi-linear transformations the only affine cap in $PG(4,4)$. Also, K is complete in $PG(4,4)$ and the group G from Section 2 is the full stabilizer of K in $P\Gamma L(5,4)$. This suffices to prove all claims of Theorem 1. As G does not have a subgroup of index 2 it follows that there are precisely two orbits of affine 40-caps under the action of $PGL(5,4)$.

Let $A \subset PG(4,4)$ be an affine 40-cap. Consider a $(5,40)$-matrix M whose columns are representatives of the points of A. Consider M as generator matrix of a code $\mathcal{C} = \mathcal{C}(A)$. Then $\mathcal{C}$ is a linear $[40,5]_4$-code, and w is the weight of a codeword from $\mathcal{C}$ if and only if there is a hyperplane of $PG(4,4)$ intersecting A in precisely $40 - w$ points.

Let d be the minimum distance of $\mathcal{C}$. By the Griesmer bound of coding theory [4] we have $d \leq 28$. This means that A meets some hyperplane in at least 12 points.

Assume $d = 28$, equivalently that all hyperplane sections of A are ≤ 12. Denote by n_i the number of hyperplanes intersecting A in i points and by H_0 a hyperplane avoiding A. We use a generalization of the construction of residual codes, which can be found in [5]:

Theorem 3. *If there is a linear $[n,k,d]_q$-code, which contains a codeword of weight w, where $w < dq/(q-1)$, then we can construct an $[n-w,k-1]_q$-code of minimum distance $\geq d - \lfloor w(q-1)/q \rfloor$.*

Note that in the situation of Theorem 3 the $n-w$ points in the hyperplane yield the columns of the generator matrix of a code $[n-w, k-1, d']$, where $d' \geq d - \lfloor w(q-1)/q \rfloor$.

Assume A intersects a hyperplane in 11 points. Then Theorem 3 produces an $[11,4,7]_4$-code. As such a code does not exist [1] we obtain a contradiction. By the same argument the non-existence of $[7,4,4]_4$- and $[6,4,3]_4$-codes [1] shows that A has no hyperplane section of 7 or 6 points. Let H_0 be the hyperplane at infinity avoiding A. In homogeneous coordinates we write $H_0 = (x_0 = 0)$ and represent points not in H_0 as $(1 : x_1 : x_2 : x_3 : x_4)$. Call two hyperplanes different from H_0 parallel if they intersect H_0 in the same plane. The 340 hyperplanes different from H_0 come in 85 parallel classes of four each. Such a parallel class has type (s_1, s_2, s_3, s_4), where $s_1 \geq s_2 \geq s_3 \geq s_4$, if A intersects the hyperplanes of this parallel class in s_1, s_2, s_3 and s_4 points. As none of the s_i exceeds 12 and none equals 11, 7 or 6 the only possible types of parallel classes of hyperplanes are

$$(12,12,12,4),\ (12,12,8,8),\ (12,10,10,8),\ (12,10,9,9),\ (10,10,10,10).$$

Let $a_1, \ldots, a_5$ be the number of parallel classes of the respective type. Assume $a_3 = a_5 = 0$. The standard equations on the hyperplane intersection numbers

$$\sum_{i \geq 0} \binom{i}{s} n_i = \binom{40}{s} \frac{4^{5-s}-1}{3}, \quad s = 0 \ldots 3,$$

(equivalent to $\mathcal{C}$ having dual distance > 3) yield equations on the a_i :

$$\begin{aligned} a_1 + a_2 + a_4 &= 85 \\ 204a_1 + 188a_2 + 183a_4 &= 16380 \\ 664a_1 + 552a_2 + 508a_4 &= 49400 \end{aligned}$$

The unique solution has $a_2 < 0$, contradiction.

Consequently parallel classes of type $(12,10,10,8)$ or $(10,10,10,10)$ must occur. We can assume that $H_1 = (x_1 = 0)$ is one of the hyperplanes intersecting A in 10 points. Theorem 3 shows in fact that the $(4,10)$-matrix with columns $(1, x_2, x_3, x_4)^T$, where $(1 : 0 : x_2 : x_3 : x_4)$ varies over $A \cap H_1$, generates a code $[10, 4, 6]_4$. Such codes (containing the 1-word, of dual distance 4) do exist. Fortunately they can be classified. An exhaustive computer search was performed. Under the action of the stabilizer of H_0 and of H_1 in $P\Gamma L(5, 4)$ there are 3 orbits of such codes (equivalently, from the dual perspective, orbits of 10-caps in $H_1 \setminus H_0$, which generate a code of dual distance 6). Using a similar computer search as in [2] we see that none of these 10-caps in H_1 can be completed to an affine 40-cap intersecting the parallels of H_1 in $\{12, 10, 8\}$ or $\{10, 10, 10\}$ points.

This shows that $d < 28$, equivalently A must intersect some hyperplane in more than 12 points. Assume the largest hyperplane intersection is $13, 14$ or 15. It is possible to classify the caps of these sizes in $H_1 \setminus H_0$. The group induced by $P\Gamma L(5, 5)$ on H_1, mapping H_0 to itself, is a semidirect product of an elementary abelian group of order 4^3 and $\Gamma L(3, 4)$. There are 4 orbits of 13-caps, 2 orbits of 14-caps and one orbit of 15-caps (of course). None of these can be completed to an affine 40-cap.

This shows that the maximal hyperplane intersection size must be 16. The 16-cap in H_1 is uniquely determined. Another exhaustive search produced all the affine 40-caps containing this starting cap. It turns out that they all are in one orbit under $P\Gamma L(5, 4)$. Moreover K is complete as a cap in $PG(4, 4)$. Another computer search shows that the stabilizer of K in $P\Gamma L(5, 4)$ has order 960. This completes the proof of Theorem 1. The hyperplane intersection numbers are

$$n_{16} = 5,\ n_{12} = 120,\ n_{10} = 160,\ n_8 = 15,\ n_4 = 40,\ n_0 = 1.$$

References

[1] A.E. Brouwer: Data base of bounds for the minimum distance for linear codes, URL http://www.win.tue.nl/∼aeb/voorlincod.html

[2] Y.Edel and J.Bierbrauer, *41 is the largest size of a cap in* $PG(4, 4)$, *Designs, Codes and Cryptography* **16** (1999),151-160.

[3] Y.Edel, S.Ferret, I.Landjev and L.Storme: *The classification of the largest caps in* $AG(5, 3)$, *Journal of Combinatorial Theory A* **99** (2002), 95-110.

[4] J.H. Griesmer: *A bound for error correcting codes,*
IBM Journal Research Development **4** (1960), 532-542.

[5] B. Groneick and S. Grosse: *New binary codes,*
IEEE Transactions on Information Theory **40** (1994), 510-512.

[6] R.Hill: *The largest size of cap in* $S_{5,3}$,
Rend. Acc. Naz. Lincei (8) **54** (1973), 378-384.

[7] G.Pellegrino: *Sul massimo ordine delle calotte in* $S_{4,3}$,
Matematiche (Catania) **25** (1970), 1-9.