Bounds on affine caps

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)
Yves Edel
Mathematisches Institut der Universität
Im Neuenheimer Feld 288
69120 Heidelberg (Germany)

September 7, 2000

1 Introduction

A **cap** in affine space $AG(k,q)$ is a set A of k-tuples in $\mathbb{F}_q^k$ such that whenever a_1, a_2, a_3 are different elements of A and $0 \neq \lambda_i \in \mathbb{F}_q, i = 1,2,3$ such that $\lambda_1 + \lambda_2 + \lambda_3 = 0$ we have $\sum_{i=1}^3 \lambda_i a_i \neq 0$. An equivalent condition is that any three of the $(k+1)$-tuples $(a_i, 1)$ are linearly independent.

Denote by $C_k(q)$ the maximum cardinality of a cap in $AG(k,q)$, and $c_k(q) = C_k(q)/q^k$. Clearly $c_k(2) = 1$. Henceforth we assume $q > 2$. The values $C_k(q)$ for $k \leq 3$ are well-known. We have $C_2(q) = q + 1$ in odd characteristic, $C_2(q) = q + 2$ for even $q > 2$, and $C_3(q) = q^2$ for all $q > 2$. Aside of these only a small number of values are known: $C_4(3) = 20$ (see [5]) and $C_5(3) = 45$ (see [2]).

Clearly $C_k(q) \leq qC_{k-1}(q)$, hence $c_k(q) \leq c_{k-1}(q)$. Our main results may be seen as lower bounds on $c_{k-1}(q) - c_k(q)$. In [4] Meshulam proves an upper bound on the size of subsets of abelian groups of odd order, which do not contain 3-term arithmetic progressions. The output for caps may be described as follows (see also [6]):

Theorem 1 (Meshulam). *Let $q = p^h$ be odd. Then*

$$c_k(q) \leq \frac{2}{kh}$$

As a cap in $AG(k, p^h)$ is also a cap in $AG(kh, p)$, Theorem 1 is implied by the special case $c_k(p) \leq 2/k$ for odd primes p. A more careful analysis of Meshulam's method in the case of caps shows that it can be generalized to cover also the characteristic 2 case. Moreover stronger bounds can be obtained. The central result is the following:

Theorem 2. *Let $q > 2$ be a prime-power. If $k \geq 3$, then*

$$c_k(q) \leq \frac{q^{-k} + c_{k-1}(q)}{1 + c_{k-1}(q)},$$

equivalently

$$(1 - c_k(q))(c_{k-1}(q) - c_k(q)) \geq c_k^2 - q^{-k}.$$

Theorem 1 follows immediately from Theorem 2. We will prove an improvement in Section 3.

In the next section we prove Theorem 2. It is possible to do this in the framework of Fourier analysis. We prefer to give a direct treatment.

2 Proof of Theorem 2

We have a prime-power $q > 2$, where $q = p^f$ (p a prime). Let $k > 3$ and $A \subset AG(k, q)$ a cap. As $q > 2$ we can find nonzero elements $\lambda_i \in \mathbb{F}_q$ such that $\lambda_1 + \lambda_2 + \lambda_3 = 0$. Let $x \cdot y$ be the ordinary dot product defined on $V = \mathbb{F}_q^k = AG(k, q)$ with values in $\mathbb{F}_q$, and $tr : \mathbb{F}_q \longrightarrow \mathbb{F}_p$ the trace. Put $Q = |V| = q^k$. Finally, ζ is a complex primitive p^{th} root of unity. We aim at an upper bound on $|A|$. Consider the complex number

$$S = \sum_{y \in V \setminus \{0\}} \sum_{a_1, a_2, a_3 \in A} \zeta^{tr((\sum_i \lambda_i a_i) \cdot y)}.$$

Lemma 1. $S = |A|(Q - |A|^2)$.

Proof. We have $S = \sum_{y \in V} \sum_{a_1, a_2, a_3 \in A} \zeta^{tr((\sum_i \lambda_i a_i) \cdot y)} - |A|^3$. Whenever $\sum_{i=1}^3 \lambda_i a_i \neq 0$, the corresponding sum over $y \in V$ vanishes. As A is a cap this will always be the case, unless $a_1 = a_2 = a_3$. The first sum is therefore $Q|A|$. ■

Definition 1. *Let $0 \neq \lambda \in I\!F_q$ and $0 \neq y \in V$. Consider the complex number $U(\lambda)_y = \sum_{a \in A} \zeta^{tr((\lambda a) \cdot y)}$. Let $u(\lambda)_y = |U(\lambda)_y|$. We define a real vector $u(\lambda)$ of length $Q-1$ whose coordinates are parametrized by the $0 \neq y \in V$, the corresponding entry being $u(\lambda)_y$.*

Lemma 2. *Let $0 \neq \lambda \in I\!F_q$ and $0 \neq y \in V$. Then*

$$u(\lambda)_y \leq qC_{k-1}(q) - |A| = c_{k-1}(q)Q - |A|.$$

Proof. As λA is a cap we can assume $\lambda = 1$. Denote by ν_c the number of elements $a \in A$ such that $a \cdot y = c$. As the $v \in V$ satisfying $v \cdot y = c$ form a subspace $AG(k-1, q)$, we have $\nu_c \leq C_{k-1}(q)$. It follows

$$u(\lambda)_y = |\sum_{c \in F_q} \nu_c \zeta^{tr(c)}| = |\sum_{c \in F_q} (C_{k-1}(q) - \nu_c) \zeta^{tr(c)}|$$

$$\leq \sum_c (C_{k-1}(q) - \nu_c) = qC_{k-1}(q) - |A|.$$

■

The same kind of calculation as in the proof of Lemma 1 shows the following.

Lemma 3. *Let $0 \neq \lambda \in I\!F_q$. Then*

$$\|u(\lambda)\|^2 = |A|(Q - |A|)$$

Comparison of Lemmas 2 and 3 yields a first lower bound on $c_{k-1}(q) - c_k(q)$, as follows. Choose $|A| = C_k(q)$. The entries of $u(\lambda)_y$ are positive numbers bounded by $Q(c_{k-1}(q) - c_k(q))$, the length of $u(\lambda)_y$ follows from Lemma 3. We obtain

Theorem 3. $(c_{k-1}(q) - c_k(q))^2 \geq c_k(q)(1 - c_k(q))/(q^k - 1)$.

In particular $c_k(q) < c_{k-1}(q)$. The following lemma is an obvious consequence of the definitions.

Lemma 4. *We have $S = \sum_{y \neq 0} U(\lambda_1)_y U(\lambda_2)_y U(\lambda_3)_y$, in particular*

$$|S| \leq \sum_{y \neq 0} u(\lambda_1)_y u(\lambda_2)_y u(\lambda_3)_y.$$

Use Lemma 2 to obtain an upper bound on $u(\lambda_1)_y$. The remaining expression has the form of a dot-product. Use the Cauchy-Schwartz inequality between the dot product and the lengths of the vectors $u(\lambda_2)$ and $u(\lambda_3)$. Because of Lemma 3 this yields

$$|S| \leq (c_{k-1}(q)Q - |A|)(|A|(Q - |A|)).$$

Choose $|A| = C_k(q)$. Standard constructions show $C_k(q) > \sqrt{Q}$ (see [1]). Lemma 1 implies that S is a negative integer. Comparison of Lemma 1 and the upper bound on $|S|$ yields after simplification the desired inequality.

3 Applications

Recall $c_3(q) = 1/q$ for $q > 2$. Theorem 2 yields $c_4(q) \leq \dfrac{q^3+1}{q^3(q+1)}$, or $C_4(q) \leq q^3 - q^2 + q$ (Theorem 3 is weaker). In particular $C_4(3) \leq 21$. It is easy to see that we have sharp inequality in this case. It was in fact proved by Pellegrino [5] that 20 is the maximal size of a cap not only in $AG(4,3)$ but also in $PG(4,3)$. Based on $C_4(3) = 20$ Theorem 2 yields $C_5(3) \leq 48$. The true value is $C_5(3) = 45$, and the only 45-cap in $AG(5,3)$ is the affine part of the Hill cap in $PG(5,3)$ (see [2, 3]). Based on this result Theorem 2 yields $C_6(3) \leq 114$. As the doubling process (see [1]) based on the Hill cap yields a 112-cap in $AG(6,3)$, we conclude that $112 \leq C_6(3) \leq 114$.

Theorem 4. *Let $q > 2$ and $k \geq 3$. Then*

$$c_k(q) \leq \frac{k+1}{k^2},$$

in particular $limsup_{k\to\infty}(kc_k(q)) \leq 1$.

Proof. We proceed by induction. For $k = 3$ the claim is true as $q > 9/4$. Let $k \geq 4$ and assume the claim is true for $k-1$. Put $c = c_{k-1}(q), d = c_k(q), Q = q^k$. Theorem 2 and the induction hypothesis yield

$$d \leq \frac{Q^{-1}+c}{1+c} \leq \frac{Q^{-1}+k/(k-1)^2}{1+k/(k-1)^2} = \frac{(k-1)^2/Q+k}{(k-1)^2+k}.$$

We have to prove that this expression is $\leq \dfrac{k+1}{k^2}$. An equivalent condition is $(k(k-1))^2 \leq q^k$. This is satisfied for all $k \geq 4$ when $q \geq 4$. The ternary case is special. Here the condition is satisfied only for $k \geq 7$. As the known values $C_k(3)$ for $k \leq 5$ and the bound $C_6(3) \leq 114$ satisfy the bound of our theorem, we are done in the ternary case as well. ■

As a cap in $AG(k, q^h)$ is a cap in $AG(hk, q)$ as well, Theorem 4 yields the following corollary:

Corollary 1. *Let $q > 2$ and $k \geq 3$. Then*

$$c_k(q^h) \leq \frac{hk+1}{(hk)^2}.$$

The following slight generalization of Theorem 2 may sometimes be useful.

Theorem 5. *Let $q > 2$ be a prime-power, $k \geq 3$ and $A \subset AG(k,q)$ be a cap such that $|A| \geq \sqrt{q^k}$ and A intersects each hyperplane $AG(k-1,q)$ in $\leq C$ points. Let $c = C/q^{k-1}$. Then*

$$\frac{|A|}{q^k} \leq \frac{q^{-k}+c}{1+c}.$$

The proof is the same as for Theorem 2. All we have used there is the fact that each hyperplane $AG(k-1,q)$ intersects A in $\leq C_{k-1}(q)$ points. We replace this number by our upper bound C now.

References

[1] Y.Edel and J.Bierbrauer: *Recursive constructions for large caps, Bulletin of the Belgian Mathematical Society - Simon Stevin* **6**(1999),249-258.

[2] Y.Edel, S.Ferret, I.Landgev, L.Storme, *The classification of the largest caps in $AG(5,3)$.*

[3] R.Hill: *On the largest size of cap in $S_{5,3}$, Atti Accad. Naz. Lincei Rendiconti* **54**(1973),378-384.

[4] R.Meshulam: *On subsets of finite abelian groups with no 3-term arithmetic progression, Journal of Combinatorial Theory A* **71**(1995),168-172.

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

[6] L.Storme, J.A.Thas and S.K.J.Vereecke: *New lower and upper bounds for the sizes of caps in finite projective spaces.*