Large Caps in Affine Space $AG(n,3)$

Karen Karapetyan

Institute for Informatics and Automation
Problems of NAS RA
Yerevan, Armenia
e-mail: karen-karapetyan@ipia.sci.am

ABSTRACT

A cap in a projective or affine geometry over a finite field F_q is a set of points no three of which are collinear. We give some new construction for caps in affine space $AG(n,3)$, which lead to some new lower bounds on the possible maximal cardinality of caps.

Keywords

Affine space, projective space, cap

1. INTRODUCTION

A cap in a projective $PG(n,q)$ or affine $AG(n,q)$ geometry over a finite field F_q is a set of points no three of which are collinear. The main problem in the theory of caps is to find the maximal size of a cap in $PG(n,q)$ or $AG(n,q)$. This is also known as the packing problem. In this paper $s_{n,q}$ and $s'_{n,q}$ denotes the size of the largest caps in $AG(n,q)$ and $PG(n,q)$, respectively. Presently, only the following exact values are known: $s_{n,2} = s'_{n,2} = 2^n$, $s_{2,q} = s'_{2,q} = q + 1$ if q is odd, $s_{2,q} = s'_{2,q} = q + 2$ if q is even, and $s'_{3,q} = q^2 + 1$, $s_{3,q} = q^2$ [1,2]. Aside of these general results the precise values are known only in the following cases: $s_{4,3} = s'_{4,3} = 20$[3], $s'_{5,3} = 56$ [4], $s_{5,3} = 45$ [5], $s'_{4,4} = 41$[6], $s_{6,3} = 112$ [7], $s_{7,3} = 236$ [8], $s'_{7,3} = 248$ [9]. In the other cases, only lower and upper bounds on the sizes of caps in $AG(n,q)$ and $PG(n,q)$ are known [12, 13, 14]. Finding the exact value for $s_{n,q}$ and $s'_{n,q}$ in general case seems to be a very hard problem [10,11]. There are many well-known constructions (doubling, product and recursive) which allow to create large high-dimensional caps based on large low-dimensional caps [12,13,14,15,16,17,18,19,20]. In this paper we give some new construction for caps in affine space $AG(n,3)$, which lead to some new lower bounds on the possible maximal cardinality of caps.

2. MAIN RESULTS

It is easy to see that if S is a cap in $AG(n,3)$ then for any triple of distinct points $\alpha, \beta, \gamma \in S$, $\alpha + \beta + \gamma \neq 0(mod3)$.
We will introduce two auxiliary sets, which will be important in our consideration. Let's denote by $B_n = \{(\alpha_1, \dots, \alpha_n) / \alpha_i = 0,1\}$ and by P_n the maximal sets of points of $AG(n,3)$ satisfying the following two conditions:

i) for any triple of distinct points $\alpha, \beta, \gamma \in P_n$, $\alpha + \beta + \gamma \neq 0(mod3)$

ii) for any two distinct points $\alpha, \beta \in P_n$, there exists i, $1 \leq i \leq n$, such that $\alpha_i = \beta_i = 2$.

It is convenient to assume that $P_1 = \{2\}$.
We will define the concatenation of the points in the following way. Let $A \subset AG(n,3)$ and $B \subset AG(m,3)$. We form a new set $AB \subset AG(n+m,3)$ consisting of all points $\alpha = (\alpha_1, \dots, \alpha_n, \alpha_{n+1}, \dots, \alpha_{n+m})$, where $\alpha' = (\alpha_1, \dots, \alpha_n) \in A$, and
$\beta' = (\alpha_{n+1}, \dots, \alpha_{n+m}) \in B$. In a similar way one can define the concatenation of the points of three, four, …etc. sets.
Note that, if $x, y, z \in F_3$, then $x + y + z = 0(mod3)$ if and only if $x = y = z$ or they are pairwise distinct.

Theorem 1. For any triple of natural numbers n, m, k, $|P_{n+m+k}| \geq |P_n||P_m||B_k| + |P_n||B_m||P_k| + |B_n||P_m||P_k|$.

Proof. Suppose we have the sets $P_n \subset AG(n,3)$, $P_m \subset AG(m,3)$, and $B_k \subset AG(k,3)$. Let's form a new set $A_1 = P_nP_mB_k$ by concatenation the points of the sets P_n, P_m, B_k. We can form the sets $A_2 = P_nB_mP_k$ and $A_3 = B_nP_mP_k \subset AG(n+m+k,3)$, as mentioned above. Clearly, the sets A_1, A_2 and A_3 are pairwise disjoint.
First, we have to prove that the sets $A_1 = P_nP_mB_k$, $A_2 = P_nB_mP_k$ and $A_3 = B_nP_mP_k$ will satisfy ii). If we have the points $\alpha = (\alpha_1, \dots, \alpha_{n+m+k})$ and $\beta = (\beta_1, \dots, \beta_{n+m+k}) \in A_1 = P_nP_mB_k$, then the points $\alpha' = (\alpha_1, \dots, \alpha_n)$ and $\beta' = (\beta_1, \dots, \beta_n)$ will belong to the set P_n and the definition of P_n implies $\alpha_i = \beta_i = 2$ for some i, $1 \leq i \leq n$.
Second, we have to prove by contradiction that the set A_1will satisfy the condition i). Assume that there are pairwise distinct points $\alpha = (\alpha_1, \dots, \alpha_{n+m+k})$, $\beta = (\beta_1, \dots, \beta_{n+m+k})$ and $\gamma = (\gamma_1, \dots, \gamma_{n+m+k}) \in A_1$ such that $\alpha + \beta + \gamma = 0(mod3)$. Then $\alpha' + \beta' + \gamma' = 0(mod3)$, $\alpha'' + \beta'' + \gamma'' = 0(mod3)$, $\alpha''' + \beta''' + \gamma''' = 0(mod3)$, where $\alpha' = (\alpha_1, \dots, \alpha_n)$, $\beta' = (\beta_1, \dots, \beta_n)$, $\gamma' = (\gamma_1, \dots, \gamma_n)$, $\alpha'' = (\alpha_{n+1}, \dots, \alpha_{n+m})$, $\beta'' = (\beta_{n+1}, \dots, \beta_{n+m})$,
$\gamma'' = (\gamma_{n+1}, \dots, \gamma_{n+m})$, $\alpha''' = (\alpha_{n+m+1}, \dots, \alpha_{n+m+k})$, $\beta''' = (\beta_{n+m+1}, \dots, \beta_{n+m+k})$, $\gamma''' = (\gamma_{n+m+1}, \dots, \gamma_{n+m+k})$.
Taking into account the definitions of P_n, P_m and B_k, the last three equalities hold $\alpha' = \beta' = \gamma'$, $\alpha'' = \beta'' = \gamma''$ and $\alpha''' = \beta''' = \gamma'''$. Hence $\alpha = \beta = \gamma$, which contradicts our assumption. By a similar argument one can prove that the sets A_2 and A_3 also satisfy the conditions i) and ii).
Now we want to prove that the set $A = A_1 \cup A_2 \cup A_3$ also satisfies the conditions i) and ii). Assume that there are three distinct points
$\alpha = (\alpha_1, \dots, \alpha_n, \alpha_{n+1}, \dots, \alpha_{n+m}, \alpha_{n+m+1}, \dots, \alpha_{n+m+k})$,
$\beta = (\beta_1, \dots, \beta_n, \beta_{n+1}, \dots, \beta_{n+m}, \beta_{n+m+1}, \dots, \beta_{n+m+k})$,
$\gamma = (\gamma_1, \dots, \gamma_n, \gamma_{n+1}, \dots, \gamma_{n+m}, \gamma_{n+m+1}, \dots, \gamma_{n+m+k}) \in A$
such that $\alpha + \beta + \gamma = 0(mod3)$. Since we have already proved that the points α, β, γ can not belong to the same A_i, $1 \leq i \leq 3$, thereby the following two cases are possible.

Case 1. Each point belongs to only one set, say $\alpha \in A_1$,$\beta \in A_2$ and $\gamma \in A_3$. By construction of the sets A_1 and A_2, $\alpha' = (\alpha_1, \dots, \alpha_n)$ and $\beta' = (\beta_1, \dots, \beta_n)$ belong to P_n. Hence, there exists i, $1 \leq i \leq n$, such that $\alpha_i = \beta_i = 2$. But $\gamma' = (\gamma_1, \dots, \gamma_n) \in B_n$. Hence $\gamma_i = 0$ *or* 1. Therefore $\alpha_i + \beta_i + \gamma_i \neq 0(mod3)$, which contradicts our assumption.

Case2. Only two points from α, β, γ belong to the same set, say $\alpha, \beta \in A_1$ and $\gamma \in A_2$. Then again $\alpha'' + \beta'' + \gamma'' = 0(mod3)$, where $\alpha'' = (\alpha_{n+1}, \dots, \alpha_{n+m})$ and $\beta'' = (\beta_{n+1}, \dots, \beta_{n+m}) \in P_m, \gamma'' = (\gamma_{n+1}, \dots, \gamma_{n+m}) \in B_m$. Since $\alpha'', \beta'' \in P_m$ there is $i,\ n+1 \le i \le n+m$, such that $\alpha_i = \beta_i = 2$, but $\gamma_i = 0\ or\ 1$, because $\gamma'' \in B_m$.
Therefore $\alpha_i + \beta_i + \gamma_i \neq 0(mod3)$, which again contradicts $\alpha + \beta + \gamma = 0(mod3)$. So, A satisfies the condition i). To show that A satisfies the condition ii) assume that $\alpha, \beta \in A$.
Since we have already proved that A_1, A_2, A_3 satisfy the condition ii), it is enough to consider the case when α and β belong to distinct sets, say $\alpha \in A_1$ and $\beta \in A_2$.
Then it is easy to see that $\alpha', \beta' \in P_n$. Hence there is $i, 1 \le i \le n$, such that $\alpha_i = \beta_i = 2$. Note that other cases can be proved by similar arguments.
It is obvious that $|P_1| = |\{2\}| = 1$ and $|P_2| = |\{20,22\}| = |\{20,21\}| = |\{21,22\}| = \cdots = 2$. Applying Theorem 1 for small odd numbers and presenting them as the sum of three numbers, we can prove that
$|P_{1+1+1}| \ge 6, |P_4| \ge 12, |P_{3+1+1}| \ge 32, |P_6| \ge 64$, $|P_7| = |P_{1+3+3}| \ge 168$, $|P_8| \ge 336, |P_9| = |P_{3+3+3}| \ge 864$, $|P_{10}| \ge 1728$, $|P_{11}| = |P_{3+3+5}| \ge 4224$, etc.
Note that the value of the right side of the inequality in Theorem 1 essentially depends on the representation of n as the sum of three numbers.

Corollary 1. For every natural numbers $n_1, n_2, \dots, n_{2k+1}$,
$|P_{n_1+n_2+\cdots+n_{2k+1}}| \ge \Big[\dots\Big[[|P_{n_1}||P_{n_2}||B_{n_3}| + |P_{n_1}||B_{n_2}||P_{n_3}| + |B_{n_1}||P_{n_2}||P_{n_3}|](|P_{n_4}||B_{n_5}| + |B_{n_4}||P_{n_5}|) + |B_{n_1+n_2+n_3}||P_{n_4}||P_{n_5}|\Big] \dots\Big](|P_{n_{2k}}||B_{n_{2k+1}}| + |B_{n_{2k}}||P_{n_{2k+1}}|) + |B_{n_1+\cdots+n_{2k-1}}||P_{n_{2k}}||P_{n_{2k+1}}|$.

Proof. We use induction on k. If k=1, then $|P_{n_1+n_2+n_3}| \ge |P_{n_1}||P_{n_2}||B_{n_3}| + |P_{n_1}||B_{n_2}||P_{n_3}| + |B_{n_1}||P_{n_2}||P_{n_3}|$, hence we are done. Assume that the inequality holds for the numbers $n_1, n_2, \dots, n_{2k-1}$ and we will prove it for numbers $n_1, n_2, \dots, n_{2k+1}$. By Theorem 1,
$|P_{(n_1+\cdots+n_{2k-1})+n_{2k}+n_{2k+1}}| \ge |P_{n_1+\cdots+n_{2k-1}}||P_{n_{2k}}||B_{n_{2k+1}}| + |P_{n_1+\cdots+n_{2k-1}}||B_{n_{2k}}||P_{n_{2k+1}}| + |B_{n_1+\cdots+n_{2k-1}}||P_{n_{2k}}||P_{n_{2k+1}}| = |P_{n_1+\cdots+n_{2k-1}}| \cdot (|P_{n_{2k}}||B_{n_{2k+1}}| + |B_{n_{2k}}||P_{n_{2k+1}}|) + |B_{n_1+\cdots+n_{2k-1}}||P_{n_{2k}}||P_{n_{2k+1}}|$.
Recalling the induction hypothesis and replacing $|P_{n_1+\cdots+n_{2k-1}}|$ by the corresponding inequality we obtain the desired result.

Corollary 2. For every natural number n,
$$|P_{3n}| \ge 3|P_n|^2|B_n|.$$

Corollary 3. For every natural number n,
$$|P_{n+2}| \ge 4 \cdot |P_n| + 2^n.$$

Corollary 4. For every natural number n,
$$|P_{3^n}| \ge 3^{2^n-1}2^{3^n-2^n}.$$

Proof. We use induction on n. If $n = 1$, then $|P_3| \ge |\{220,221,202,212,022,122\}| = 6 = 3^{2^1-1}2^{3^1-2^1}$ and we are done when n=1. Supposing, that it is true for $n = k-1$, let's prove it for $n = k$. We have by Theorem 1,
$|P_{3^k}| = |P_{3^{k-1}+3^{k-1}+3^{k-1}}| \ge |P_{3^{k-1}}||P_{3^{k-1}}||B_{3^{k-1}}| + |P_{3^{k-1}}||B_{3^{k-1}}||P_{3^{k-1}}| + |B_{3^{k-1}}||P_{3^{k-1}}||P_{3^{k-1}}| = 3|P_{3^{k-1}}|^2|B_{3^{k-1}}|$.
By the induction hypothesis,
$$3|P_{3^{k-1}}|^2|B_{3^{k-1}}| \ge 3\left(3^{2^{k-1}-1}2^{3^{k-1}-2^{k-1}}\right)^2 2^{3^{k-1}} = 3^1 3^{2(2^{k-1}-1)}\ 2^{2(3^{k-1}-2^{k-1})}2^{3^{k-1}} = 3^{2^k-1}2^{3^k-2^k}.$$
In a similar way one can prove the following.

Corollary 5. For every natural numbers n, k, m,
$$|P_{3^n+3^m+3^k}| \ge \frac{2^{3^n+3^m+3^k}}{3^2}\left[\left(\frac{3}{2}\right)^{2^n+2^m} + \left(\frac{3}{2}\right)^{2^m+2^k} + \left(\frac{3}{2}\right)^{2^k+2^n}\right].$$

Theorem 2. For every natural number n and m,
$$s_{m+n,3} \ge |P_n||B_m| + |B_n||P_m|.$$

Proof. Suppose we have the sets $A_1 = P_nB_m$ and $A_2 = B_nP_m$. It is obvious that $A_1, A_2 \subset P_{n+m}$ and $A_1 \cap A_2 = \emptyset$.
We will prove the inequality by contradiction. Assume that there exist three distinct points $\alpha, \beta, \gamma \in A_1 \cup A_2$ such that $\alpha + \beta + \gamma = 0(mod3)$. We suppose that two of them belong to one set (say $\alpha, \beta \in A_1$) and the third point to other (say $\gamma \in A_2$). By definition of P_n there is i , $1 \le i \le n$, such that $\alpha_i = \beta_i = 2$. But by definition of $B_n, \gamma_i = 0\ or\ 1$, hence $\alpha_i + \beta_i + \gamma_i \neq 0(mod3)$, which contradicts that $\alpha + \beta + \gamma = 0(mod3)$. In a similar way one can prove that the case when two points belong to A_2 and the last one belongs to A_1 is impossible, hence the inequality is true.

Corollary 6. For every natural number n $(n \ge 2)$,
$$s_{n,3} \ge 2|P_{n-1}| + |B_{n-1}|.$$
For example,
$$s_{10,3} \ge 2|P_9| + |B_9| = 2 \cdot 864 + 512 = 2240.$$

Theorem 3. For every natural n $(n \ge 2)$ and $i, 1 \le i \le n-1$,
$$s_{n+1,3} \ge |P_i||P_{n-i}| + |P_i||B_{n-i}| + |B_i||P_{n-i}| + |B_n|.$$

3. ACKNOWLEDGEMENT

We would like to express our gratitude to Professor Ara Aleksanyan for informing me and interesting conversations on this topic.

REFERENCES

[1] R.C. Bose,‘‘Mathematical theory of the symmetrical factorial design’’, *Sankhya̅ 8*, pp.107-166, 1947.
[2] B. Qvist, ‘‘Some remarks concerning curves of the second degree in a finite plane’’, *Ann. Acad. Sci. Fenn. Ser. A* **134**, p. 27, 1952.
[3] G. Pellegrino, ‘‘Sul massimo ordine delle calotte in $S_{4,3}$’’, *Matematiche (Catania)* **25**, pp. 1-9, 1970.
[4] R. Hill, ‘‘On the largest size of cap in $S_{5,3}$’’, *Atti Accad. Naz. Lincei Rendiconti* **54**, pp. 378-384, 1973.
[5] 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**, pp. 95-110, 2002.
[6] Y. Edel and J. Bierbrauer, ‘’41 is the largest size of a cap in PG(4,4)’’, *Designs, Codes and Cryptography* **16**, pp.151-160, 1999.
[7] A. Potechin, ‘‘Maximal caps in AG(6,3)’’, *Designs, Codes and Cryptography* **46**, pp.243-259, 2008.
[8] A.R. Calderbank and P.C.Fishburn, ‘‘Maximal three-independent subsets of $\{0,1,2\}^n$ ’’, *Designs, Codes and Cryptography* **4**, pp. 203-211, 1994.

[9] Y. Edel, ‘‘Large caps in small spaces’’, *Designs, Codes and Cryptography* **23**, pp. 197-212, 2001.

[10] J.W. Hirschfeld and L. Storme, ‘‘ The packing problem in statistics, coding theory and finite projective spaces’’, *Journal of Statistical Planning and Inference* **72**, pp. 355-380, 1998.

[11] J.W. Hirschfeld and L. Storme, ‘‘The packing problem in statistics, coding theory and finite projective spaces’’, *Proceeding of the Fourth Isle of Thorns conference* , pp. 201-246, July 16-21 2000.

[12] R. Meshulam, ‘‘On subsets of finite abelian groups with no 3-term arithmetic progressions’’ *Journal of Combinatorial Theory A* **71**, pp. 168-172, 1995.

[13] J. Bierbrauer and Y. Edel, ‘‘Bounds on affine caps’’, *J. Combin. Des.***10**, pp. 111-115, 2002.

[14] B. Segre, ‘‘On complete caps and ovaloids in three dimensional Galois spaces of charaterisetic two’’, *Acta Arithmetica* **5**, pp. 315-332,1959.

[15] B. Segre, ‘‘Le geometrie di Galois’’, *Ann. Mat. Pura Appl.* **48**, pp. 1-97, 1959.

[16] J. Tits, ‘‘Ovoides et groups de Suzuki’’, *Archiv der Mathematik* **13**, pp. 187-198, 1962.

[17] A.C. Mukhopadhyay, ‘‘Lower bounds on $m_t(r,s)$’’, *Journal of Combinatorial Theeory A* **25** ,pp. 1-13, 1978.

[18] Y. Edel, J. Bierbrauer. ‘‘Recursive constructions for large caps’’, *Bull. Belg. Math Soc.* **6**, pp. 249-258, 1999.

[19] Y. Edel, ‘‘Extensions of Generalized Product Caps’’, *Designs, Codes and Cryptography* **31**, pp. 5- 14, 2004.

[20]A. Aleksanyan, M. Papikian, “On bloking sets of affine spaces”*arXiv:math.Co* ,9910084v1, 1999.