Mathematical Problems of Computer Science 57, 56–64, 2022.
doi: 10.51408/1963-0087

UDC 519.7

Complete Caps in Affine Geometry $AG(n,3)$

Karen I. Karapetyan

Institute for Informatics and Automation Problems of NAS RA
e-mail: karen-karapetyan@iiap.sci.am

Abstract

We consider the problem of constructing complete caps in affine geometry $AG(n,3)$ of dimension n over the field F_3 of order three. We will take the elements of F_3 to be 0, 1 and 2. A cap is a set of points, no three of which are collinear. Using the concept of P_n −set, we give two new methods for constructing complete caps in affine geometry $AG(n,3)$. These methods lead to some new upper and lower bounds on the possible minimal and maximal cardinality of complete caps in affine geometry $AG(n,3)$.

Keywords: Affine geometry, Projective geometry, Cap, Complete cap.

1. Introduction

A cap in an affine geometry $AG(n,q)$ or in a projective geometry $PG(n,q)$ over a finite field F_q is a set of points no three of which are collinear. A cap is called complete when it cannot be extended to a large cap. The central problem in the theory of caps is to find the maximal and minimal sizes of caps in the affine geometry $AG(n,q)$ or in the projective geometry $PG(n,q)$. In this paper, $s_{n,q}$ and $s'_{n,q}$ denote 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 from 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]. In the other cases, only lower and upper bounds on the sizes of caps in $AG(n,q)$ and $PG(n,q)$ are known. Finding the exact value for $s_{n,q}$ and $s'_{n,q}$ in the general case seems to be a very hard problem [8–10]. The only complete cap in $AG(n,2)$ is the whole $AG(n,2)$. The trivial lower bound for the size of the smallest complete cap in $AG(n,q)$ is $\sqrt{2}q^{\frac{n-1}{2}}$. For even q there exist complete caps in geometry $AG(n,q)$ with less than $q^{\frac{n}{2}}$ points. But for odd q complete caps in $AG(n,q)$ with less than $q^{\frac{n}{2}}$

points are known to exist [11, 12] only for $n = 0(mod\,4)$, $n = 2(mod\,4)$. For more information about complete caps, for small values n and q, we refer the reader to [10–13]. Note that the problem of determining the minimum size of a complete cap in a given geometry is of particular interest in Coding theory. Using the concept of a P_n-set, which was introduced by the author in 2015 [14], we give two new methods for constructing complete caps in the affine geometry $AG(n, 3)$. These methods yield some new upper and lower bounds on the possible minimal and maximal sizes of complete caps in the affine geometry $AG(n, 3)$.

2. Main Results

We will write the points of $AG(n, q)$ in the following way: $\boldsymbol{x} = (x_1, \cdots, x_n)$, and let us denote by $\boldsymbol{0} = (0, \cdots, 0)$ the origin point of the geometry $AG(n, 3)$. It is easy to check that if $\boldsymbol{S}$ is a cap in $AG(n, 3)$, then $\boldsymbol{\alpha} + \boldsymbol{\beta} + \boldsymbol{\gamma} \neq \boldsymbol{0}\ (mod\,3)$ for every triple of distinct points $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma} \in \boldsymbol{S}$. Let's denote by $B_n = \{\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n) | \alpha_i = 1, 2\}$ and by P_n the set of points of $AG(n, 3)$ satisfying the following two conditions:

i) for any two distinct points $\boldsymbol{\alpha}, \boldsymbol{\beta} \in P_n$, there exists i $(1 \leq i \leq n)$ such that $\alpha_i = \beta_i = 0$,

ii) for any triple of distinct points $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma} \in P_n$, $\boldsymbol{\alpha} + \boldsymbol{\beta} + \boldsymbol{\gamma} \neq \boldsymbol{0}(mod\,3)$.

We say P_n to be complete when it cannot be extended to a larger one. We will define the concatenation of the points of the sets 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 $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n, \alpha_{n+1}, \cdots, \alpha_{n+m})$, where $\boldsymbol{\alpha}^{(1)} = (\alpha_1, \cdots, \alpha_n) \in A$ and $\boldsymbol{\alpha}^{(2)} = (\alpha_{n+1}, \cdots, \alpha_{n+m}) \in B$. In a similar way, one can define the concatenation of the points for any number of sets.

Claim 1. Note that if $x, y, z \in F_3$, then $x + y + z = 0\ (mod\,3)$ if and only if $x = y = z$ or they are pairwise distinct numbers.
The following two theorems, which we need, are proven in [16, 17].

Theorem 1: *The following recurrence relation* $P_n = P_{n_1}P_{n_2}B_{n_3} \cup P_{n_1}B_{n_2}P_{n_3} \cup B_{n_1}P_{n_2}P_{n_3}$, *with initial sets* $P_1 = \{(0)\}$, $P_2 = \{(0,1), (0,2)\}$ *and* $n = \sum_{j=1}^{3} n_j$, *yields a complete* P_n *set.*

Having the sets $P_{n_1}, P_{n_2}, P_{n_3}, P_{n_4}, P_{n_5}, P_{n_6}$ and $B_{n_1}, B_{n_2}, B_{n_3}, B_{n_4}, B_{n_5}, B_{n_6}$, let us form the following ten sets, by concatenation of the points of the sets.

$$A_1 = P_{n_1}P_{n_2}B_{n_3}B_{n_4}B_{n_5}P_{n_6}, \qquad A_2 = B_{n_1}P_{n_2}P_{n_3}P_{n_4}B_{n_5}B_{n_6},$$
$$A_3 = P_{n_1}B_{n_2}P_{n_3}B_{n_4}P_{n_5}B_{n_6}, \qquad A_4 = B_{n_1}B_{n_2}P_{n_3}P_{n_4}B_{n_5}P_{n_6},$$
$$A_5 = B_{n_1}B_{n_2}P_{n_3}B_{n_4}P_{n_5}P_{n_6}, \qquad A_6 = B_{n_1}P_{n_2}B_{n_3}P_{n_4}P_{n_5}B_{n_6},$$
$$A_7 = B_{n_1}P_{n_2}B_{n_3}B_{n_4}P_{n_5}P_{n_6}, \qquad A_8 = P_{n_1}B_{n_2}B_{n_3}P_{n_4}P_{n_5}B_{n_6},$$
$$A_9 = P_{n_1}B_{n_2}B_{n_3}P_{n_4}B_{n_5}P_{n_6}, \qquad A_{10} = P_{n_1}P_{n_2}P_{n_3}B_{n_4}B_{n_5}B_{n_6}.$$

Theorem 2: *The following recurrence relation $P_n = \bigcup_{i=1}^{10} A_i$, with initial sets $P_1 = \{(0)\}$, $P_2 = \{(0,\ 1),(0,2)\}$ and $n = \sum_{i=1}^{6} n_i$ yields a complete P_n set.*

Claim 2. Note that from the construction of P_n in both theorems it follows that for every i $(1 \le i \le n)$, if the point $\boldsymbol{p} = (p_1, \dots, p_i, \dots, p_n) \in P_n$ and $p_i \neq 0$, then, also, the point $\boldsymbol{p}' = (p_1, \dots, p_i^{-1}, \dots, p_n) \in P_n$, where p_i^{-1} is the additive inverse of p_i in the field F_3.

The following two main theorems without proofs were first presented at CSIT 2015 in a weak form [14], that they yield caps. But at CSIT 2017 they were presented with a strong conclusion that they yield complete caps [15]. In this paper, we give their complete proofs.

Theorem 3: *If P_n and P_m are constructed either by Theorem 1 or by Theorem 2, then for the given natural numbers n and m, the set $S = P_nB_m \cup B_nP_m$ is a complete cap in the geometry $AG(n+m,3)$.*

Proof. First of all we will prove that the set $S = P_nB_m \cup B_nP_m$ is a cap. Suppose, to the contrary, that S is not a cap. Then there is a triple of distinct points $\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma} \in S$, such that $\boldsymbol{\alpha}+\boldsymbol{\beta}+\boldsymbol{\gamma} = \boldsymbol{0}(mod\ 3)$. Let's represent the points $\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma}$ as $\boldsymbol{\alpha} = \boldsymbol{\alpha}^{(1)}\boldsymbol{\alpha}^{(2)}$, $\boldsymbol{\beta} = \boldsymbol{\beta}^{(1)}\boldsymbol{\beta}^{(2)}$ and $\boldsymbol{\gamma} = \boldsymbol{\gamma}^{(1)}\boldsymbol{\gamma}^{(2)}$, respectively, where $\boldsymbol{\alpha}^{(1)} = (\alpha_1, \cdots, \alpha_n)$, $\boldsymbol{\alpha}^{(2)} = (\alpha_{n+1}, \cdots, \alpha_{n+m})$, $\boldsymbol{\beta}^{(1)} = (\beta_1, \cdots, \beta_n)$, $\boldsymbol{\beta}^{(2)} = (\beta_{n+1}, \cdots, \beta_{n+m})$, $\boldsymbol{\gamma}^{(1)} = (\gamma_1, \cdots, \gamma_n)$ and $\boldsymbol{\gamma}^{(2)} = (\gamma_{n+1}, \cdots, \gamma_{n+m})$. Thus, we obtain $\boldsymbol{\alpha}^{(1)} + \boldsymbol{\beta}^{(1)} + \boldsymbol{\gamma}^{(1)} = \boldsymbol{0}(mod\ 3)$ and $\boldsymbol{\alpha}^{(2)} + \boldsymbol{\beta}^{(2)} + \boldsymbol{\gamma}^{(2)} = \boldsymbol{0}(mod\ 3)$. If all three points $\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma} \in P_nB_m$, then it follows that $\boldsymbol{\alpha}^{(1)},\boldsymbol{\beta}^{(1)},\boldsymbol{\gamma}^{(1)} \in P_n$ and $\boldsymbol{\alpha}^{(2)},\boldsymbol{\beta}^{(2)},\boldsymbol{\gamma}^{(2)} \in B_m$. The definition of the set P_n implies that $\boldsymbol{\alpha}^{(1)} = \boldsymbol{\beta}^{(1)} = \boldsymbol{\gamma}^{(1)}$ and Claim 1 implies that $\boldsymbol{\alpha}^{(2)} = \boldsymbol{\beta}^{(2)} = \boldsymbol{\gamma}^{(2)}$. Therefore, $\boldsymbol{\alpha} = \boldsymbol{\beta} = \boldsymbol{\gamma}$, which contradicts that $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ and $\boldsymbol{\gamma}$ are pairwise distinct points. In the same manner, one can prove the case, when all three points $\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma} \in B_nP_m$, is impossible. Now let us assume that two of these points belong to one set (say $\boldsymbol{\alpha},\boldsymbol{\beta} \in P_nB_m$) and the third point $\boldsymbol{\gamma}$ belongs to the other set (say $\gamma \in B_nP_m$). By definition of P_n there is i, $1 \le i \le n$, so that $\alpha_i = \beta_i = 0$. But, by definition of B_n, $\gamma_i = 1$ or 2. Hence, $\alpha_i + \beta_i + \gamma_i \neq 0(mod\ 3)$, which contradicts that $\boldsymbol{\alpha}+\boldsymbol{\beta}+\boldsymbol{\gamma} = \boldsymbol{0}(mod\ 3)$. In a similar way, one can prove the case when two points belong to B_nP_m and the third one belongs to P_nB_m is impossible. Therefore, S is a cap.

We will prove the completeness of S again by contradiction. Suppose that there is a point $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n, \alpha_{n+1}, \dots, \alpha_{n+m})$, such that $\boldsymbol{\alpha} \notin$ S and S $\cup \{\boldsymbol{\alpha}\}$ is a cap. Let's represent the point $\boldsymbol{\alpha}$ as $\boldsymbol{\alpha} = \boldsymbol{\alpha}^{(1)}\boldsymbol{\alpha}^{(2)}$, where $\boldsymbol{\alpha}^{(1)} = (\alpha_1, \cdots, \alpha_n)$, $\boldsymbol{\alpha}^{(2)} = (\alpha_{n+1}, \cdots, \alpha_{n+m})$. The following two cases are possible.

Case 1. At least one of the sets $P_n \cup \{\boldsymbol{\alpha}^{(1)}\}$ or $P_m \cup \{\boldsymbol{\alpha}^{(2)}\}$ satisfies the condition i). Assume that the set $P_n \cup \{\boldsymbol{\alpha}^{(1)}\}$ satisfies the condition i). If $\boldsymbol{\alpha}^{(1)} \in P_n$, then we can choose two points $\boldsymbol{x}$, $\boldsymbol{y} \in B_m$ in the following way. If $\alpha_i = 0$, then we will assume that $x_i = 1$ and $y_i = 2$, otherwise $x_i = y_i = \alpha_i$, $n+1 \le i \le n+m$. Therefore, $\boldsymbol{\alpha}^{(2)} \notin B_m$, since $\boldsymbol{\alpha} \notin$ S and $\boldsymbol{\alpha}^{(1)} \in P_n$. Hence, $\boldsymbol{\alpha}^{(2)}$, $\boldsymbol{x}$ and $\boldsymbol{y}$ are pairwise distinct points. It is not difficult to see that $\boldsymbol{\alpha}^{(1)}\boldsymbol{x}$, $\boldsymbol{\alpha}^{(1)}\boldsymbol{y} \in P_nB_m$. Claim 1 implies that $\boldsymbol{\alpha}^{(1)}\boldsymbol{\alpha}^{(2)} + \boldsymbol{\alpha}^{(1)}\boldsymbol{x} + \boldsymbol{\alpha}^{(1)}\boldsymbol{y} = \boldsymbol{0}(mod\ 3)$, which contradicts the assumption that S $\cup$

$\{\boldsymbol{\alpha}\}$ is a cap. If $\boldsymbol{\alpha}^{(1)} \notin P_n$, then the completeness of the P_n implies that there are two distinct points $\boldsymbol{\beta}, \boldsymbol{\gamma} \in P_n$, such that $\boldsymbol{\alpha}^{(1)} + \boldsymbol{\beta} + \boldsymbol{\gamma} = \mathbf{0}(mod\ 3)$. Now, as described above, we will choose two points $\boldsymbol{x}, \boldsymbol{y} \in B_m$ in the following way. If $\alpha_i = 0$, then we will take $x_i = 1$ and $y_i = 2$, otherwise $x_i = y_i = \alpha_i$, $n+1 \le i \le n+m$. The choice of the points $\boldsymbol{x}, \boldsymbol{y}$ implies that $\boldsymbol{x}, \boldsymbol{y} \in B_m$ and $\boldsymbol{\alpha}^{(2)} + \boldsymbol{x} + \boldsymbol{y} = \mathbf{0}(mod\ 3)$. Therefore, $\boldsymbol{\alpha}^{(1)}\boldsymbol{\alpha}^{(2)} + \boldsymbol{\beta}\boldsymbol{x} + \boldsymbol{\gamma}\boldsymbol{y} = \mathbf{0}(mod 3)$, which contradicts the assumption that S ∪ $\{\boldsymbol{\alpha}\}$ is a cap. Similarly, one can prove the case, when the set $P_m \cup \{\boldsymbol{\alpha}^{(2)}\}$ satisfies the condition i), is impossible.

Case 2. Both sets $P_n \cup \{\boldsymbol{\alpha}^{(1)}\}$ and $P_m \cup \{\boldsymbol{\alpha}^{(2)}\}$ do not satisfy the condition i). Therefore, the condition i) for the set $P_n \cup \{\boldsymbol{\alpha}^{(1)}\}$ follows that there is a point $\boldsymbol{\beta} \in P_n$, such that if $\alpha_i = 0$, then $\beta_i \neq 0$ and if $\beta_i = 0$, then $\alpha_i \neq 0$, $1 \le i \le n$. We will choose the point $\boldsymbol{x} \in B_n$ in the following way. If $\alpha_i = 0$, then $x_i = \beta_i^{-1}$ and if $\beta_i = 0$, then $x_i = \alpha_i^{-1}$, otherwise, using Claim 2, we can assume that $x_i = \beta_i = \alpha_i$, $1 \le i \le n$. By the same reason, the condition i) for the set $P_m \cup \{\boldsymbol{\alpha}^{(2)}\}$ implies that there is a point $\boldsymbol{\gamma} \in P_m$, so that if $\alpha_i = 0$, then $\gamma_i \neq 0$ and if $\gamma_i = 0$, then $\alpha_i \neq 0, n+1 \le i \le n+m$. In the same manner, we will choose the point $\boldsymbol{y} \in B_m$. If $\alpha_i = 0$, then $y_i = \gamma_i^{-1}$ and if $\gamma_i = 0$, then $y_i = \alpha_i^{-1}$, otherwise, by Claim 2, we can assume that $y_i = \gamma_i = \alpha_i$, $n+1 \le i \le n+m$). It is obvious that $\boldsymbol{\beta}\boldsymbol{y} \in P_n B_m$ and $\boldsymbol{x}\boldsymbol{\gamma} \in B_n P_m$. The choice of the points $\boldsymbol{x}, \boldsymbol{y}$ implies that $\boldsymbol{\alpha}^{(1)} + \boldsymbol{\beta} + \boldsymbol{x} = \mathbf{0}(mod\ 3)$ and $\boldsymbol{\alpha}^{(2)} + \boldsymbol{\gamma} + \boldsymbol{y} = \mathbf{0}(mod\ 3)$. Therefore, $\boldsymbol{\alpha}^{(1)}\boldsymbol{\alpha}^{(2)} + \boldsymbol{\beta}\boldsymbol{y} + \boldsymbol{x}\boldsymbol{\gamma} = \mathbf{0}(mod\ 3)$, which again contradicts the assumption that S ∪ $\{\boldsymbol{\alpha}\}$ is a cap.

□

Corollary 1: *For the given natural numbers n and m,* $s_{n+m,3} \ge |P_n||B_m| + |B_n||P_m|$.

Corollary 2: *For every natural number n,* $s_{n+1,3} \ge 2|P_n| + |B_n|$.

Theorem 4: *If P_n and P_m are constructed by Theorem 1 or by Theorem 2, then for the given natural numbers n and m, $S = P_n P_m\{0\} \cup P_n B_m\{1\} \cup B_n P_m\{1\} \cup B_{n+m}\{2\}$ is a complete cap in the geometry $AG(n+m+1, 3)$.*

Proof. First we will prove that the set $S = P_n P_m\{0\} \cup P_n B_m\{1\} + B_n P_m\{1\} + B_{n+m}\{2\}$ is a cap by contradiction. Assume that there are three distinct points $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n, \alpha_{n+1}, \dots, \alpha_{n+m}, \alpha_{n+m+1})$, $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n, \beta_{n+1}, \dots, \beta_{n+m}, \beta_{n+m+1})$, $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_n, \gamma_{n+1}, \dots, \gamma_{n+m}, \gamma_{n+m+1}) \in S$, such that $\boldsymbol{\alpha} + \boldsymbol{\beta} + \boldsymbol{\gamma} = \mathbf{0}(mod\ 3)$. Therefore, $\boldsymbol{\alpha}^{(1)} + \boldsymbol{\beta}^{(1)} + \boldsymbol{\gamma}^{(1)} = \mathbf{0}(mod\ 3)$, $\boldsymbol{\alpha}^{(2)} + \boldsymbol{\beta}^{(2)} + \boldsymbol{\gamma}^{(2)} = \mathbf{0}(mod\ 3)$ and $\alpha_{n+m+1} + \beta_{n+m+1} + \gamma_{n+m+1} = \mathbf{0}(mod\ 3)$, where $\boldsymbol{\alpha}^{(1)} = (\alpha_1, \cdots, \alpha_n)$, $\boldsymbol{\alpha}^{(2)} = (\alpha_{n+1}, \cdots, \alpha_{n+m})$, $\boldsymbol{\beta}^{(1)} = (\beta_1, \cdots, \beta_n)$, $\boldsymbol{\beta}^{(2)} = (\beta_{n+1}, \cdots, \beta_{n+m})$, $\boldsymbol{\gamma}^{(1)} = (\gamma_1, \cdots, \gamma_n)$ and $\boldsymbol{\gamma}^{(2)} = (\gamma_{n+1}, \cdots, \gamma_{n+m})$. Claim 1 implies that $\alpha_{n+m+1} = \beta_{n+m+1} = \gamma_{n+m+1}$ or α_{n+m+1}, β_{n+m+1}, and γ_{n+m+1} are pairwise distinct numbers. Hence, the following four cases are possible.

Case 1. $\alpha_{n+m+1} = \beta_{n+m+1} = \gamma_{n+m+1} = 0$. Therefore, $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma} \in P_n P_m\{0\}$, $\boldsymbol{\alpha}^{(1)}, \boldsymbol{\beta}^{(1)}, \boldsymbol{\gamma}^{(1)} \in P_n$ and $\boldsymbol{\alpha}^{(2)}, \boldsymbol{\beta}^{(2)}, \boldsymbol{\gamma}^{(2)} \in P_m$. From the definition of P_n and P_m and the two relations $\boldsymbol{\alpha}^{(1)} + \boldsymbol{\beta}^{(1)} + \boldsymbol{\gamma}^{(1)} = 0(mod\ 3)$, $\boldsymbol{\alpha}^{(2)} + \boldsymbol{\beta}^{(2)} + \boldsymbol{\gamma}^{(2)} = \mathbf{0}(mod\ 3)\ it$ follows that $\boldsymbol{\alpha}^{(1)} = \boldsymbol{\beta}^{(1)} = \boldsymbol{\gamma}^{(1)}$ and

$\boldsymbol{\alpha}^{(2)}=\boldsymbol{\beta}^{(2)}=\boldsymbol{\gamma}^{(2)}$. Hence, $\boldsymbol{\alpha}=\boldsymbol{\beta}=\boldsymbol{\gamma}$, which contradicts the assumption that $\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma}$ are pairwise distinct points.

Case 2. $\alpha_{n+m+1}=\beta_{n+m+1}=\gamma_{n+m+1}$=1. Assume that $\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma}\in P_nB_m\{1\}$. Then $\boldsymbol{\alpha}^{(1)},\boldsymbol{\beta}^{(1)},\boldsymbol{\gamma}^{(1)}\in P_n$ and $\boldsymbol{\alpha}^{(2)},\boldsymbol{\beta}^{(2)},\boldsymbol{\gamma}^{(2)}\in B_m$. The definition of P_n implies that $\boldsymbol{\alpha}^{(1)}=\boldsymbol{\beta}^{(1)}=\boldsymbol{\gamma}^{(1)}$, since $\boldsymbol{\alpha}^{(1)}+\boldsymbol{\beta}^{(1)}+\boldsymbol{\gamma}^{(1)}=\mathbf{0}(mod\ 3)$. Because $\boldsymbol{\alpha}^{(2)}+\boldsymbol{\beta}^{(2)}+\boldsymbol{\gamma}^{(2)}=\mathbf{0}(mod\ 3)$, Claim 1 implies that $\boldsymbol{\alpha}^{(2)}=\boldsymbol{\beta}^{(2)}=\boldsymbol{\gamma}^{(2)}$. Therefore, $\boldsymbol{\alpha}=\boldsymbol{\beta}=\boldsymbol{\gamma}$, which, again contradicts the assumption that $\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma}$ are pairwise distinct points. Similarly, one can prove that the case is impossible, when $\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma}\in B_nP_m\{1\}$. Therefore, two points, say $\boldsymbol{\alpha},\boldsymbol{\beta}\in P_nB_m\{1\}$ and $\boldsymbol{\gamma}\in B_nP_m\{1\}$. The definition of P_n implies that there is i, such that $\alpha_i=\beta_i=0,\ 1\le i\le n,$. But by the definition of $B_n,\ \gamma_i=1\ or\ 2$. Hence, $\alpha_i+\beta_i+\gamma_i\neq 0(mod\ 3)$, which contradicts that $\boldsymbol{\alpha}+\boldsymbol{\beta}+\boldsymbol{\gamma}=\mathbf{0}(mod\ 3)$. In a similar manner, one can prove that the case is impossible, when two points from $\boldsymbol{\alpha},\boldsymbol{\beta}$ and $\boldsymbol{\gamma}$ belong to B_nP_m and the third one belongs to P_nB_m. Therefore, S is a cap.

Case 3. $\alpha_{n+m+1}=\beta_{n+m+1}=\gamma_{n+m+1}=2$. Therefore $\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma}\in B_{n+m}\{2\}$. Hence, $\boldsymbol{\alpha}^{(1)}\boldsymbol{\alpha}^{(2)}$, $\boldsymbol{\beta}^{(1)}\boldsymbol{\beta}^{(2)},\boldsymbol{\gamma}^{(1)}\boldsymbol{\gamma}^{(2)}\in B_{n+m}$ and $\boldsymbol{\alpha}^{(1)}\boldsymbol{\alpha}^{(2)}+\ \boldsymbol{\beta}^{(1)}\boldsymbol{\beta}^{(2)}+\boldsymbol{\gamma}^{(1)}\boldsymbol{\gamma}^{(2)}=\mathbf{0}(mod\ 3)$. Claim 1 implies that $\boldsymbol{\alpha}^{(1)}\boldsymbol{\alpha}^{(2)}=\ \boldsymbol{\beta}^{(1)}\boldsymbol{\beta}^{(2)}=\boldsymbol{\gamma}^{(1)}\boldsymbol{\gamma}^{(2)}$. This yields $\boldsymbol{\alpha}=\boldsymbol{\beta}=\boldsymbol{\gamma}$, which, again contradicts the assumption that $\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\gamma}$ are pairwise distinct points.

Case α_{n+m+1}, β_{n+m+1} and γ_{n+m+1} are pairwise distinct numbers. Without loss of generality, let us assume that $\alpha_{n+m+1}=0$, $\beta_{n+m+1}=1$ and $\gamma_{n+m+1}=2$. Therefore, $\boldsymbol{\alpha}\in P_nP_m\{0\},\boldsymbol{\beta}\in P_nB_m\{1\}$ or $\boldsymbol{\beta}\in B_nP_m\{1\}$ and $\boldsymbol{\gamma}\in B_{n+m}\{2\}$. If $\boldsymbol{\beta}\in P_nB_m\{1\}$, then $\boldsymbol{\alpha}^{(1)},\boldsymbol{\beta}^{(1)}\in P_n$. Hence, the definition of P_n implies that there is i, such that $\alpha_i=\beta_i=0,1\le i\le n$. But, by the definition of $B_n,\gamma_i=1$ or 2. Therefore, $\alpha_i+\beta_i+\gamma_i\neq 0(mod\ 3)$, which contradicts that $\boldsymbol{\alpha}^{(1)}+\boldsymbol{\beta}^{(1)}+\boldsymbol{\gamma}^{(1)}=\mathbf{0}(mod\ 3)$. The last relation, in turn, implies that $\boldsymbol{\alpha}+\boldsymbol{\beta}+\boldsymbol{\gamma}\neq\mathbf{0}(mod\ 3)$. In a similar manner, one can prove the case when $\boldsymbol{\beta}\in B_nP_m\{1\}$ is impossible. Hence, S is a cap.
Now we will prove the completeness of S also by contradiction. Let us assume that there is a point $\boldsymbol{\alpha}=(\alpha_1,\dots,\alpha_n,\alpha_{n+1},\dots,\alpha_{n+m},\alpha_{n+m+1})$, such that $\boldsymbol{\alpha}\notin S$ and $S\cup\{\boldsymbol{\alpha}\}$ is a cap. The following three cases are possible.

Case $\alpha_{n+m+1}=2$. Since $\boldsymbol{\alpha}\notin S$, we have $(\alpha_1,\dots,\alpha_n,\alpha_{n+1},\dots,\alpha_{n+m})\notin B_{n+m}$. We can choose two points $\boldsymbol{x},\boldsymbol{y}\in B_{n+m}\{2\}$, such that, if $\alpha_i=0$ then $x_i=2$ and $y_i=1$, otherwise $x_i=y_i=\alpha_i,\ 1\le i\le n+m$. It is obvious that $\boldsymbol{x}\{2\},\ \boldsymbol{y}\{2\}\in B_{n+m}\{2\}$ and $\boldsymbol{\alpha},\boldsymbol{x}\{2\},\ \boldsymbol{y}\{2\}$ are pairwise distinct points. Claim 1 implies that $\boldsymbol{x}\{2\}+\ \boldsymbol{y}\{2\}+\boldsymbol{\alpha}=\mathbf{0}(mod\ 3)$, which contradicts the assumption that $S\cup\{\boldsymbol{\alpha}\}$ is a cap.

Case $\alpha_{n+m+1}=1$. Let's represent the point $\boldsymbol{\alpha}$ as $\boldsymbol{\alpha}=\boldsymbol{\alpha}^{(1)}\boldsymbol{\alpha}^{(2)}\{1\}$, where $\boldsymbol{\alpha}^{(1)}=(\alpha_1,\cdots,\alpha_n)$ and $\boldsymbol{\alpha}^{(2)}=(\alpha_{n+1},\cdots,\alpha_{n+m})$. Assume that at least one of the sets $P_n\cup\{\boldsymbol{\alpha}^{(1)}\}$ or $P_m\cup\{\boldsymbol{\alpha}^{(2)}\}$ satisfies the condition i), say $P_n\cup\{\boldsymbol{\alpha}^{(1)}\}$. First, suppose that $\boldsymbol{\alpha}^{(1)}\notin P_n$. Then the completeness of the set P_n follows that there are two points $\boldsymbol{\beta},\boldsymbol{\gamma}\in P_n$, such that $\boldsymbol{\beta}+\boldsymbol{\gamma}+\boldsymbol{\alpha}^{(1)}=\mathbf{0}(mod\ 3)$. We will choose two points $\boldsymbol{x},\boldsymbol{y}\in B_m$ in the following way. If $\alpha_i=0$, then $x_i=1$ and $y_i=2$, otherwise $x_i=y_i=\alpha_i,\ n+1\le i\le n+m$. From the choice of the points $\boldsymbol{x},\boldsymbol{y}$ it follows that

$\boldsymbol{x}, \boldsymbol{y} \in B_m$ and $\boldsymbol{\alpha}^{(2)} + \boldsymbol{x} + \boldsymbol{y} = \boldsymbol{0}(mod\ 3)$. Therefore, $\boldsymbol{\alpha}^{(1)}\boldsymbol{\alpha}^{(2)}\{1\} + \boldsymbol{\beta x}\{1\} + \boldsymbol{\gamma y}\{1\} = \boldsymbol{0}(mod\ 3)$, which contradicts the assumption that $S \cup \{\boldsymbol{\alpha}\}$ is a cap. Otherwise, if $\boldsymbol{\alpha}^{(1)} \in P_n$, then $\boldsymbol{\alpha}^{(2)} \notin B_m$, because $\boldsymbol{\alpha} \notin S$. Then it is easy to see that $\boldsymbol{\alpha}^{(1)}\boldsymbol{\alpha}^{(2)}\{1\} + \boldsymbol{\alpha}^{(1)}\boldsymbol{x}\{1\} + \boldsymbol{\alpha}^{(1)}\boldsymbol{y}\{1\} = \boldsymbol{0}(mod\ 3)$, which, again contradicts the assumption that $S \cup \{\boldsymbol{\alpha}\}$ is a cap. Similarly, one can prove the case, when the set $P_m \cup \{\boldsymbol{\alpha}^{(2)}\}$ satisfies the condition i) is impossible. Therefore, both sets $P_n \cup \{\boldsymbol{\alpha}^{(1)}\}$ and $P_m \cup \{\boldsymbol{\alpha}^{(2)}\}$ do not satisfy the condition i). Hence, there is a point $\boldsymbol{\beta} \in P_n$, (respectively, $\boldsymbol{\gamma} \in P_m$), such that if $\alpha_i = 0$, then $\beta_i \neq 0$ and if $\beta_i = 0$, then $\alpha_i \neq 0, 1 \leq i \leq n$ (respectively, if $\alpha_i = 0$, then $\gamma_i \neq 0$ and if $\gamma_i = 0$, then $\alpha_i \neq 0, n+1 \leq i \leq n+m$). First, let's choose the point $\boldsymbol{x} \in B_n$ in the following way. If $\alpha_i = 0$, then $x_i = \beta_i^{-1}$ and if $\beta_i = 0$, then $x_i = \alpha_i^{-1}$, otherwise, by Claim 2, we can assume that $x_i = \beta_i = \alpha_i$, $1 \leq i \leq n$. In the same manner, we will choose the point $\boldsymbol{y} \in B_m$. If $\alpha_i = 0$, then $y_i = \gamma_i^{-1}$ and if $\gamma_i = 0$, then $y_i = \alpha_i^{-1}$, otherwise, using Claim 2, we can assume that $y_i = \gamma_i = \alpha_i$, $n+1 \leq i \leq n+m$). The choice of the points $\boldsymbol{x}$ and $\boldsymbol{y}$ implies that $\boldsymbol{\alpha}^{(1)}\boldsymbol{\alpha}^{(2)}\{1\} + \boldsymbol{\beta y}\{1\} + \boldsymbol{x\gamma}\{1\} = \boldsymbol{0}(mod\ 3)$, which again contradicts the assumption that $S \cup \{\boldsymbol{\alpha}\}$ is a cap.

Case $\alpha_{n+m+1} = 0$. Assume that at least one of the sets $P_n \cup \{\boldsymbol{\alpha}^{(1)}\}$ or $P_m \cup \{\boldsymbol{\alpha}^{(2)}\}$ does not satisfy the condition i), say the set $P_n \cup \{\boldsymbol{\alpha}^{(1)}\}$**.** Therefore, the condition i) implies that there is a point $\boldsymbol{\beta} \in P_n$, such that, if $\alpha_i = 0$, then $\beta_i \neq 0$ and if $\beta_i = 0$, then $\alpha_i \neq 0, 1 \leq i \leq n$. We will choose the points $\boldsymbol{z}^{(1)} \in B_n$ and $\boldsymbol{z}^{(2)}$, $\boldsymbol{y} \in B_m$ in the following way. First let's choose $\boldsymbol{z}^{(1)}$**.** If $\alpha_i = 0$, then $z_i = \beta_i^{-1}$ and if $\beta_i = 0$, then $z_i = \alpha_i^{-1}$, otherwise, using Claim 2, we will assume that $z_i = \beta_i = \alpha_i$, $1 \leq i \leq n$. Now we will choose the points $\boldsymbol{z}^{(2)}$, $\boldsymbol{y} \in B_m$ in the following way. If $\alpha_i = 0$, then we will assume that $z_i = 1$ and $y_i = 2$, otherwise $z_i = y_i = \alpha_i$, $n+1 \leq i \leq n+m$. It is easy to see that $\boldsymbol{\beta y}\{1\} \in P_n B_m\{1\}, \boldsymbol{z}^{(1)}\boldsymbol{z}^{(2)}\{2\} \in B_{n+m}\{2\}$. The choice of the points $\boldsymbol{z}^{(1)}, \boldsymbol{z}^{(2)}$ and $\boldsymbol{y}$ imply that $\boldsymbol{\alpha}^{(1)}\boldsymbol{\alpha}^{(2)}\{0\} + \boldsymbol{\beta y}\{1\} + \boldsymbol{z}^{(1)}\boldsymbol{z}^{(2)}\{2\} = \boldsymbol{0}(mod\ 3)$, which contradicts the assumption that $S \cup \{\boldsymbol{\alpha}\}$ is a cap. Similarly, one can prove the case is impossible, when the set $P_m \cup \{\boldsymbol{\alpha}^{(2)}\}$ does not satisfy the condition i). Therefore, both sets $P_n \cup \{\boldsymbol{\alpha}^{(1)}\}$ and $P_m \cup \{\boldsymbol{\alpha}^{(2)}\}$ are satisfying the condition i). Since $\boldsymbol{\alpha} \notin S$, therefore either $\boldsymbol{\alpha}^{(1)} \notin P_n$ or $\boldsymbol{\alpha}^{(2)} \notin P_m$. If $\boldsymbol{\alpha}^{(1)} \notin P_n$ and $\boldsymbol{\alpha}^{(2)} \in P_m$, then the completeness of P_n follows that there are two points $\boldsymbol{x}, \boldsymbol{y} \in P_n$, so that $\boldsymbol{x} + \boldsymbol{y} + \boldsymbol{\alpha}^{(1)} = \boldsymbol{0}(mod\ 3)$. Since $\boldsymbol{x}, \boldsymbol{y} \in P_n$ and $\boldsymbol{\alpha}^{(2)} \in P_m$, we have $\boldsymbol{x\alpha}^{(2)}, \boldsymbol{y\alpha}^{(2)} \in P_n P_m$ and $\boldsymbol{x\alpha}^{(2)}\{0\} + \boldsymbol{y\alpha}^{(2)}\{0\} + \boldsymbol{\alpha}^{(1)}\boldsymbol{\alpha}^{(2)}\{0\} = \boldsymbol{0}(mod\ 3)$, which contradicts the assumption that $S \cup \{\boldsymbol{\alpha}\}$ is a cap. The case, when $\boldsymbol{\alpha}^{(2)} \notin P_m$ and $\boldsymbol{\alpha}^{(1)} \in P_n$ is analogous to the above described one and therefore is impossible. Hence, $\boldsymbol{\alpha}^{(1)} \notin P_n$ and $\boldsymbol{\alpha}^{(2)} \notin P_m$. Therefore, from the completeness of P_n and P_m it follows that there are points $\boldsymbol{\beta}, \boldsymbol{\gamma} \in P_n$ and $\boldsymbol{\delta}, \boldsymbol{\theta} \in P_m$, so that $\boldsymbol{\beta} + \boldsymbol{\gamma} + \boldsymbol{\alpha}^{(1)} = \boldsymbol{0}(mod\ 3)$ and $\boldsymbol{\delta} + \boldsymbol{\theta} + \boldsymbol{\alpha}^{(2)} = \boldsymbol{0}(mod\ 3)$. The last two relations imply that $\boldsymbol{\alpha}^{(1)}\boldsymbol{\alpha}^{(2)}\{0\} + \boldsymbol{\beta\delta}\{0\} + \boldsymbol{\gamma\theta}\{0\} = \boldsymbol{0}(mod\ 3)$, which contradicts the assumption that $S \cup \{\boldsymbol{\alpha}\}$ is a cap.

□

Corollary 3: *For the given natural numbers n and m,* $s_{n+m+1,3} \geq |P_n||P_m| + |P_n||B_m| + |B_n||P_m| + |B_{n+m}|$.

Corollary 4: $s_{5,3} \geq 42$.

Proof. By definition P_1={(0)}. From Theorem 1 it follows that $P_3 = P_{1+1+1} = P_1P_1B_1 \cup P_1B_1P_1 \cup B_1P_1P_1$ ={(0, 0, 1), (0, 0, 2), (0, 1, 0), (0, 2, 0), (1, 0, 0), (2, 0, 0)}. It is easy to see that $|B_n| = 2^n$. Therefore, $s_{5,3} \geq |P_3||P_1| + |P_3||B_1| + |B_3||P_1| + |B_4|$ $=6 \times 1 + 6 \times 2 + 8 \times 1 + 16 = 42$.

□

3. Conclusion

Notice that the cardinality of P_n obtained by Theorem 1 (Theorem 2) [16, 17], essentially depends on the representation of n as the sum of three (six) natural numbers. Presenting the natural numbers as the sum of six natural numbers and applying Theorem 2, for some $n \geq 6$ in some cases, one can obtain larger complete P_n sets than those, which are constructed by Theorem 1. It is easy to check that $|P_1| = 1$, $|P_2| = 2$, and $|P_{1+1+1}| = 6$. $|P_{2+1+1}| = 12$, $|P_{3+1+1}| = 32$, $|P_{1+1+1+1+1+1}| = 80$, $|P_7| = |P_{3+3+1}| = 168$, $|P_8| = |P_{1+1+1+1+1+3}| = 400$, $|P_9| = |P_{3+3+3}| = 864$… It is not difficult to see that the maximal size $|P_n| > 2^n$, if $n > 5$. Therefore, to construct large complete caps it is convenient to use Corollary 2, but for small complete caps one can use Theorem 4.

References

[1] R. C. Bose, "Mathematical theory of the symmetrical factorial design", *Sankhya*, vol. 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, vol. 134, p. 27. 1952.

[3] G. Pellegrino, "Sul Massimo ordine delle calotte in $S_{4,3}$", *Matematiche* (Catania), vol. 25, pp. 1-9, 1970.

[4] R. Hill, "On the largest size of cap in $S_{5,3}$", *Atti Accad Naz.Lincei Rendicondi*, vol. 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*, ser. A, vol. 99, pp. 95-110, 2002.

[6] Y. Edel and J. Bierbrauer, "41 is the largest size of a cap in $PG(n,3)$", *Designs, Codes and Cryptography*, vol. 16, pp. 151-160, 1999.

[7] A. Potechin, "Maximal caps in $AG(6,3)$", *Designs, Codes and Cryptography*, vol. 46, pp. 243-259, 2008.

[8] 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.

[9] 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.

[10] J. Bierbrauer and Y. Edel, "Large caps in projective Galois spaces", In: Current topics in Galois geometry, Editors J. De Beule and L.Storm, pp. 87-104, 2012.

[11] A. A. Davidov, G. Faina, S. Marcugini and F. Pambianco, “Computer search in projective planes for the sizes of complete arcs”, *J. Geometry*, vol. 82, pp. 50-62, 2005.

[12] A. A. Davidov and P. R. J. Ostergard, “Recursive constructions of complete caps”, *J. Statist. Planning Infer*, vol. 95, pp. 167-173, 2001.

[13] M. Geuletti, “Small complete caps in Galois affine spaces”, *J. Algebr. Comb.* Vol. 25, pp.149-168, 2007.

[14] K. Karapetyan, “Large Caps in Affine Space”, *Proceedings of International Conference Computer Science and Information Technologies*, Yerevan, Armenia, pp. 82-83, 2015.

[15] K. Karapetyan, “On the complete caps in Galois affine space $AG(n,3)$”, *Proceedings of International Conference Computer Science and Information Technologies*, Yerevan, Armenia, p. 205, 2017.

[16] I.A. Karapetyan and K.I. Karapetyan. “The Complete Caps in Projective Geometry $PG(n,3)$”, *«Լրաբեր» գիտական հոդվածների ժողովածու (ՀԱՊՀ)*, հատոր 1, էջեր 35-44, 2021.

[17] I. Karapetyan and K. Karapetyan, “Complete Caps in Projective Geometry $PG(n,3)$”, *Proceedings of International Conference Computer Science and Information Technologies*, Yerevan, Armenia, pp. 57-60, 2021.

Submitted 28.03.22, accepted 27.05.2022.

Լրիվ գլխարկներ $AG(n,3)$ աֆինական երկրաչափությունում

Կարեն Ի. Կարապետյան

ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտ
e-mail: karen-karapetyan@iiap.sci.am

Ամփոփում

Դիտարկվում է n չափանի $AG(n,3)$ աֆինական երկրաչափությունում լրիվ գլխարկների կառուցման խնդիրը $F_3=\{0,1,2\}$ դաշտի վրա: Գլխարկը այն կետերի բազմությունն է, որոնցից ոչ մի երեքը համագիծ չեն: Օգտագործելով P_n բազմության հասկացությունը, մշակվել են լրիվ գլխարկների կառուցման երկու նոր մեթոդներ:

Բանալի բառեր՝ աֆինական երկրաչափություն, պրոյեկտիվ երկրաչափություն, կետեր, գլխարկներ, լրիվ գլխարկներ:

Полные шапки в аффинной геометрии $AG(n,3)$

Карен И. Карапетян

Институт проблем информатики и автоматизации НАН РА
e-mail: karen-karapetyan@iiap.sci.am

Аннотация

Рассматривается задача построения полных шапок в аффинной геометрии $AG(n,3)$ размерности n над полем $F_3 = \{0,1,2\}$. Шапка — это набор точек, никакие три из которых не коллинеарны. С помощью понятия множества P_n, разработаны две новые конструкции построения полных шапок.

Ключевые слова: аффинная геометрия, проективная геометрия, точки, шапки, полные шапки.