On Multiple Caps in Finite Projective Spaces

Yves Edel yedel@cage.ugent.be
Department of Pure Mathematics and Computer Algebra,
Ghent University, Krijgslaan 281-S22, Ghent 9000, BELGIUM

Ivan Landjev i.landjev@nbu.bg
New Bulgarian University, 21 Montevideo str., 1618 Sofia, BULGARIA
Institute of Mathematics and Informatics, ivan@math.bas.bg
Bulgarian Academy of Sciences, 8 Acad. G. Bonchev, 1113 Sofia, BULGARIA

Abstract. In this paper, we consider new results on (k, n)-caps with $n > 2$. We provide a lower bound on the size of such caps. Furthermore, we generalize two product constructions for $(k, 2)$-caps to caps with larger n. We give explicit constructions for good caps with small n. In particular, we determine the largest size of a $(k, 3)$-cap in PG$(3, 5)$, which turns out to be 44. The results on caps in PG$(3, 5)$ provide a solution to four of the eight open instances of the main coding theory problem for $q = 5$ and $k = 4$.

Mathematics Subject Classification: 51E22, 94B05, 94B65

Keywords: caps, multiple caps, linear codes, Griesmer bound, Griesmer codes, finite projective geometries

Dedicated to the memory of András Gács (1969-2009)

1 Introduction

Let PG(t, q) be the t-dimensional projective geometry over the finite field with q elements. A (k, n)-cap in PG(t, q) is a set of k points, some n, but no $n+1$ of which are collinear. The $(k, 2)$-caps are simply known as k-caps, while caps with $n > 2$ are referred to as multiple caps. Apart from some papers by R. Hill [6], in which bounds and exact values on the maximal size of such multiple caps are obtained, (k, n)-caps with $n > 2$ have received little or no attention. In the same time, they are interesting in the context of the main problem of coding theory where many hypothetical codes meeting or lying close to the known bounds turn out to be multiple caps.

In this paper, we summarize the known results and prove new bounds on the maximal size of a (k, n)-cap in PG(t, q). In section 2, we prove a recursive upper bound on the size of a (k,n)-cap. As expected, a precise knowledge in the lower dimension gives good upper bounds in higher dimensions. In particular, the knowledge of the maximal size of a $(k,3)$-arcs in $\mathrm{PG}(2,q)$ gives bounds that are better than Hill's bound. In section 3, we present general product constructions for multiple caps. In section 4, some newly constructed multiple caps with $n=3$ and $n=4$ are presented. Finally, in section 5, we discuss the implication of some results from section 4 to the so-called main coding theory problem. In particular, we rule out the existence of Griesmer codes for $q=5$, $k=4$ and $d=31,32,36,37$.

2 An Upper Bound

In [6], Ray Hill proved the following result: a $(k,3)$-cap in $\mathrm{PG}(3,q)$, $q>3$, satisfies

$$k \leq 2q^2+1-\alpha(q),$$

where $\alpha(q)$ is the smallest integer a which satisfies

$$a^2\left(\frac{2q^2-a}{q+1-a}+q^2-q-1\right)+a\left(\frac{q(2q^2-a)}{q+1-a}+3q^3-6q\right)+6q^3-2q^4 \geq 0.$$

For sufficiently large q,

$$\alpha(q) \geq \frac{\sqrt{17}-3}{2}q+\frac{7}{2}-\frac{49}{2\sqrt{17}}.$$

Denote by $\mathrm{m}_n(s,q)$ the largest size of a (k,n)-cap in $\mathrm{PG}(s,q)$, $n<q$.

Theorem 1. *Let $2 \leq s < t$ be integers. For any $(s-1)$-dimensional subspace S of $\mathrm{PG}(t,q)$, the size of a (k,n)-cap $\mathfrak{K}$ in $\mathrm{PG}(t,q)$ satisfies*

$$k \leq \mathrm{m}_n(s,q)\frac{q^{t-s+1}-1}{q-1}-q\mathfrak{K}(S)\frac{q^{t-s}-1}{q-1}. \quad (1)$$

Proof. Let $\mathfrak{K}$ be a (k,n)-cap in $\mathrm{PG}(t,q)$. Let S be an $(s-1)$-dimensional subspace of $\mathrm{PG}(t,q)$ and let T be a $(t-s)$-dimensional subspace in $\mathrm{PG}(t,q)$ disjoint from S. Consider a projection π from S onto T, i.e.

$$\pi : \begin{cases} \mathcal{P}\setminus S & \rightarrow \quad T, \\ x & \rightarrow \quad \langle S,x\rangle \cap T, \end{cases}$$

where $\mathcal{P}$ is the pointset of $\mathrm{PG}(t,q)$. Every s-dimensional subspace through S maps to a point in T. The projection π induces a multiset $\mathfrak{K}^\pi$ on T by

$$\mathfrak{K}^\pi(x) = \sum_{y:y\in\mathcal{P}\setminus S,\pi(y)=x} \mathfrak{K}(y),$$

where $x \in T$. We have $k = \mathfrak{K}(S) + \mathfrak{K}^\pi(T)$. On the other hand $\mathfrak{K}^\pi(x) \leq \mathrm{m}_n(s,q) - \mathfrak{K}(S)$ for every $x \in T$. This implies

$$\begin{aligned} k &\leq \mathfrak{K}(S) + (\mathrm{m}_n(s,q) - \mathfrak{K}(S))\frac{q^{t-s+1}-1}{q-1} \\ &= \mathrm{m}_n(s,q)\frac{q^{t-s+1}-1}{q-1} - q\mathfrak{K}(S)\frac{q^{t-s}-1}{q-1}. \end{aligned}$$

□

In order to get a better bound, we have to take S to be of maximal multiplicity. A trivial lower bound is $\mathfrak{K}(S) \geq n + s - 2$, which gives

$$k \leq \mathrm{m}_n(s,q)\frac{q^{t-s+1}-1}{q-1} - q(n+s-2)\frac{q^{t-s}-1}{q-1}. \tag{2}$$

Using a more elaborate counting, we can get other estimates.

Fix an n-line L and count in two ways the multiplicities of all $(s-1)$-subspaces S through L. We have

$$\sum_{S: L \subset S} \mathfrak{K}^\pi(S) = (k-n)\frac{(q^{t-2}-1)\dots(q^{t-s+2}-1)}{(q^{s-3}-1)\dots(q-1)}.$$

Denote by M the maximal multiplicity of an $(s-1)$-dimensional subspace through L. Then

$$(M-n)\frac{(q^{t-1}-1)\dots(q^{t-s+2}-1)}{(q^{s-2}-1)\dots(q-1)} \geq (k-n)\frac{(q^{t-2}-1)\dots(q^{t-s+2}-1)}{(q^{s-3}-1)\dots(q-1)},$$

which implies

$$M \geq n + (k-n)\frac{q^{s-2}-1}{q^{t-1}-1}.$$

Substituting back in (1) and solving for k, we get the following corollary.

Corollary 2. *The size of a (k,n)-cap in $\mathrm{PG}(t,q)$ satisfies*

$$k \leq \frac{\mathrm{m}_n(s,q)(q^{t-s+1}-1)(q^{t-1}-1) - nq((q^{t-1}-1)(q-1)-(q^{t-s}-1)(q^{s-2}-1))}{(q^{t-1}-1)(q-1)+q(q^{s-2}-1)(q^{t-s}-1)}. \tag{3}$$

Let us note that (3) is better than (2) when s is close to t. For small values of s, (2) gives better estimates than (3). Note that (2) can be exact. For example, if we take $q = 5, t = 3, n = 4, s = 2$, we have $\mathrm{m}_4(2,5) = 16$ and (2) is $k \leq 76$.

In fact, a $[76,4,60]_5$-code has been constructed in [2], which is equivalent to a $(76,4)$-cap in $\mathrm{PG}(3,5)$ meeting the upper bound.

Better estimates of the numbers $\mathrm{m}_n(s,q)$ will lead obviously to better bounds. On the other hand, it is better to work with the bound (1) rather than with (2) or (3) since for specific values of the parameters we might have additional knowledge on the multiplicity of the maximal $(s-1)$-dimensional subspaces.

The case of $(k,3)$-caps in $\mathrm{PG}(t,q)$ is of particular interest. A trivial counting in this case gives, which coincides with (2) for $s=2$:

$$k \leq \frac{q^{t-1}-1}{q-1}\mathrm{m}_3(2,q) - 3q\frac{q^{t-2}-1}{q-1}.$$

Since the best estimate we know about $\mathrm{m}_3(2,q)$ is $\mathrm{m}_3(2,q) \leq 2q+1$ for all $q>3$, we get

$$k \leq \frac{q^{t-1}-1}{q-1}(2q+1) - 3q\frac{q^{t-2}-1}{q-1}, \tag{4}$$

which for $t=3$ gives $k \leq 2q^2+1$. This has been improved already by Bramwell and Wilson [3] who proved that $k \leq 2q^2$, not to speak of Hill's result mentioned above which is much stronger: $k \leq 2q^2 - \alpha(q)$, where $\alpha(q) \sim Cq$ with $C > \frac{1}{2}$. But of course, better estimates for $\mathrm{m}_3(2,q)$, which is the case for $q = 8, 9, 11, 13$ (cf. [8]), will give better bounds. The nonexistence of $(2q+1,3)$-arcs for some q will already give $k \leq 2q^2 - q$.

3 Some general product constructions for multiple caps

In this section we present several product constructions for multiple caps. They generalize earlier constructions for classical caps from [4] to multiple caps.

Theorem 3. *Let there exist a (k,n) cap $\mathfrak{C}_1$ in $\mathrm{PG}(t,q)$ and a hyperplane H in $\mathrm{PG}(t,q)$ such that $|\mathfrak{C}_1 \setminus H| = w$. Assume furthermore there exists a (l,n)-cap $\mathfrak{C}_2$ in $\mathrm{PG}(s,q)$. Then there exists a $(wl+(k-w),n)$-cap in $\mathrm{PG}(s+t,q)$.*

Proof. Write the points of $\mathfrak{C}_1$ as $(\mathbf{x},1)$, $\mathbf{x} \in \mathbb{F}_q^t$, if they are not on H, and in the form $(\mathbf{x}',0)$, $\mathbf{x}' \in \mathbb{F}_q^t$, if they are incident with H. The points of $\mathfrak{C}_2$ are represented as $(s+1)$-tuples $\mathbf{y}$ over $\mathbb{F}_q$. It is claimed that the set

$$\mathfrak{C} = \{(\mathbf{x},\mathbf{y}) \mid (\mathbf{x},1) \in \mathfrak{C}_1 \setminus H, \mathbf{y} \in \mathfrak{C}_2\} \cup \{(\mathbf{x}',\mathbf{0}) \mid (\mathbf{x}',0) \in \mathfrak{C}_1 \cap H\}$$

is a $(wl+(k-w),n)$-cap in $\mathrm{PG}(s+t,q)$.

First, we prove that the set $\mathfrak{C}' = \{(\mathbf{x}, \mathbf{y}) \mid (\mathbf{x}, 1) \in \mathfrak{C}_1 \backslash H, \mathbf{y} \in \mathfrak{C}_2\}$ is a (wl, n)-cap. Assume there is a line containing at least $n+1$ points of the above set. The projections on the y-part of the coordinates of these points cannot be all different since this would give $n+1$ collinear points in $\mathrm{PG}(s, q)$, a contradiction to the fact that $\mathfrak{C}_2$ is a (l, n)-cap. Therefore there must be at least one $\mathbf{y}'$ in the projection that appears with multiplicity greater than 1. Hence the y-part of the points of $\mathfrak{C}'$ on the line before projection is a fixed non-zero vector $\mathbf{y}' \in \mathbb{F}_q^{s+1}$. But this contradicts the fact that $\mathfrak{C}_1$ is a (k, n)-cap.

Now assume that there is a line containing $n+1$ collinear points from $\mathfrak{C}$ of which at least one is of the form $(\mathbf{x}', \mathbf{0})$. But now we can repeat the above argument to get that the points on the line are of the form $(\mathbf{x}, \mathbf{y}')$ for a fixed non-zero $\mathbf{y}'$, $(\mathbf{x}', \mathbf{0})$. Now we can construct $n+1$ collinear points of the form $(\mathbf{x}, 1)$, $(\mathbf{x}', 0)$, which are obviously from $\mathfrak{C}_1$, a contradiction. The set $\mathfrak{C}$ has the required cardinality, which completes the proof. □

This theorem implies the following useful corollary.

Corollary 4. *Assume there exist a (k, n)-cap in $\mathrm{AG}(t, q)$ with i empty hyperplanes in general position and an (l, n)-cap in $\mathrm{PG}(s, q)$ that has j empty hyperplanes. Then there exists a (kl, n)-cap in $\mathrm{PG}(s+t, q)$, with $i+j-1$ empty hyperplanes in general position.*

Let us note that the construction from Corollary 4 can be reiterated to yield the following corollary.

Corollary 5. *Assume there exist caps with parameters (k_i, n) in $\mathrm{AG}(t_i, q)$, $i = 1, \dots, \sigma$. Assume furthermore there exists an (l, n)-cap in $\mathrm{PG}(s, q)$. Then there exists a $(k_1 \dots k_\sigma l, n)$-cap in $\mathrm{PG}(s + t_1 + \dots + t_n, q)$.*

Remark 3.1. The following simple geometric construction also yields multiple caps. Let $\Pi = \mathrm{PG}(s+t+1, q)$ and let Δ_1 and Δ_2 be two subspaces of Π with $\dim \Delta_1 = s$, $\dim \Delta_2 = t$ such that $\Delta_1 \cap \Delta_2 = \emptyset$.

Let $\mathfrak{C}_1$ be a (k_1, n)-cap in Δ_1 and $\mathfrak{C}_2$ be a (k_2, n)-cap in Δ_2, $n \le q-1$. For each pair of points x, y with $x \in \mathfrak{C}_1$, $y \in \mathfrak{C}_2$, select n points $z_1, \dots, z_n$, $z_i \ne x, y$, that are incident with the line through x and y. Define $\mathfrak{C}$ as the set of all points z_i obtained in this way. It is straightforward to check that each point from $\mathfrak{C}$ is obtained from only one pair of points $(x, y) \in \mathfrak{C}_1 \times \mathfrak{C}_2$. The set $\mathfrak{C}$ turns out to be a $(k_1 k_2 n, n)$-cap.

This construction can be obtained as a special case of Theorem 3. Any n points in $\mathrm{PG}(1, q)$ are trivially a (n, n)-cap. For $n \le q$, this cap is affine. If there exists a (k, n)-cap in $\mathrm{PG}(t, q)$, then there is a (kn, n)-cap in $\mathrm{PG}(t+1, q)$, which is also in $\mathrm{AG}(t+1,q)$ if $n < q$. This observation and Theorem 3 now imply the geometric construction.

What is a bit unsatisfactory about Theorem 3 is the fact that it uses its ingredients in a unsymmetrical fashion. Now we present another construction, which is a generalization of Theorem 10 from [4] for multiple caps.

Let the following be given:

- a $(t+1)\times k$ matrix A, whose columns represent the points of a (k,n)-cap in $\mathrm{PG}(t,q)$; we assume that the first row of A has w entries (in the first positions from the left) equal to 1, the remaining entries being 0;
- a $(s+1)\times l$ matrix B, whose columns represent the points of an (l,n)-cap in $\mathrm{PG}(s,q)$; we assume that the first row of B has v entries equal to 1 (in the first v positions from the left) while the remaining entries are 0.

Denote by $\mathbf{a}$ a typical column of A with first component equal to 1; by α a column of A with first component equal to 0. Analogously, let $\mathbf{b}$ (resp. β) be a vector of B having first component equal to 1 (resp. equal to 0). Let $\mathbf{a}'$, α', $\mathbf{b}'$, β' be obtained from $\mathbf{a}$, α, $\mathbf{b}$, β, respectively by omitting the first component (which is 0 or 1). Form all possible vectors of the following types:

type I $(1,\mathbf{b}',\mathbf{a}')^t$,
type II $(0,\beta',\mathbf{a}')^t$,
type III $(0,\mathbf{b},\alpha')^t$.

By Theorem 3, the columns of types I and II yield a (κ,n) cap for some κ. By symmetry this is true for all columns of type I and III. Denote by M the matrix containing the columns of all three types.

In what follows, we assume that the caps given by the matrices A and B have tangent hyperplanes and these are the hyperplanes with equation $X_0=0$, i.e. $k-w=l-v=1$. Let us denote by $\mathcal{Q}$ a set of points in $\mathrm{PG}(r,q)$ and let $\mathbf{x},\mathbf{y}\in\mathbb{F}_q^{r+1}$ be the (homogeneous) coordinates of two different points from $\mathcal{Q}$. We define

$$\mathrm{coef}_{\mathcal{Q}}(\mathbf{x},\mathbf{y}) := \left\{\lambda \mid \mathbf{x}+\lambda\mathbf{y}\in\mathcal{Q}, \lambda\in\mathbb{F}_q^*\right\}. \tag{5}$$

Theorem 6. *Assume the following exist:*

(1) a (k,n)-cap $\mathfrak{C}_A\subset\mathrm{PG}(t,q)$ having a tangent hyperplane H_A;

(2) an (l,n)-cap $\mathfrak{C}_B\subset\mathrm{PG}(s,q)$ having a tangent hyperplane H_B;

(3) representatives $\mathbf{x}$, $\alpha\in\mathbb{F}_q^{t+1}$ with $\mathbf{x}\in\mathfrak{C}_A\setminus H_A$ and $\alpha=\mathfrak{C}_A\cap H_A$, and representatives $\mathbf{y}$, $\beta\in\mathbb{F}_q^{s+1}$ with $\mathbf{y}\in\mathfrak{C}_B\setminus H_B$ and $\beta=\mathfrak{C}_B\cap H_B$ such that

$$\mathrm{coef}_{\mathfrak{C}_A}(\mathbf{x},\alpha)\cap\mathrm{coef}_{\mathfrak{C}_B}(\mathbf{y},\beta)=\emptyset.$$

then there is a $(kl-1,n)$*-cap in* $\mathrm{PG}(s+t,q)$.

Proof. The vector space coordinates are chosen in such a way that H_A is the hyperplane $X_0 = 0$, and $\mathbf{x} = (1,0,\ldots,0)$. For the points of $\mathfrak{C}_A \setminus \{\mathbf{x},\alpha\}$, we choose a representative with first coordinate 1. We choose $\mathbf{y}$, β and H_B analogously.

Now we are going to prove that the point set defined above is a $(kl-1,n)$-cap.

Assume that there exists a line L containing $n+1$ points. By Theorem 3, this line contains a point represented by type II columns, as well as points represented by type III columns. So assume that the points $(0,\beta',\mathbf{a}')$ and $(0,\mathbf{b}',\alpha')$ are on L. First, let us check that these points are different. Assume this not the case. Then $\mathbf{b}' \neq \mathbf{0}$ and $\mathbf{a}' \neq 0$ and there is $\lambda \neq 0$ such that $(0,\beta',\mathbf{a}') = \lambda(0,\mathbf{b}',\alpha')$. This implies that $\lambda \in \mathrm{coef}_{\mathfrak{C}_A}(\mathbf{x},\alpha) \cap \mathrm{coef}_{\mathfrak{C}_B}(\mathbf{y},\beta)$, contradicting (3).

Now we can conclude that all points on the line L are represented by type II or type III columns. We claim that there are at most $n-2$ different columns $\mathbf{a}'$ that are a nonzero multiple of column α'. This is true as these correspond to the points on the line $(1,\mathbf{0})$ and $(0,\alpha')$ and we have at most n points of $\mathfrak{C}_A$ on a line. Analogous conclusion can be made for $\mathfrak{C}_B$.

All the points on the line L that are different from the two already considered are given by $(0,\mathbf{b}',\alpha') + \lambda(0,\beta',\mathbf{a}')$, where $\lambda \neq 0$. As there are at most $n-2$ different columns $\mathbf{a}'$ that are a nonzero multiple of the column α', there must be two points that have the same entry in the last segment. Hence $\mathbf{a}' = \mathbf{0}$ (as $\alpha \neq 0$). Analogously we get $\mathbf{b}' = \mathbf{0}$. So the line L contains just only two points $(0,\mathbf{0},\alpha)$ and $(0,\beta,\mathbf{0})$, a contradiction to $n \geq 2$. □

4 Results on caps in $\mathrm{PG}(k,q)$ for small q and small n

4.1 Caps with $n = 3$

The problem of finding the largest size of a $(k,3)$-cap in $\mathrm{PG}(t,q)$ is nontrivial for $q \geq 4$. It is known that 31 is the largest size of such a cap in $\mathrm{PG}(3,4)$ [6]. In the same paper, Hill proved that the $(31,3)$-cap is projectively unique. Let us note that this value implies an upper bound of $119 = 5 \cdot 31 - 4 \cdot 9$ for the maximal size of a $(k,3)$-cap in $\mathrm{PG}(4,4)$. This value is rather inaccurate since the nonexistence of Griesmer $[116,5,85]$ codes (cf. [10]) implies that a $(k,3)$-cap in $\mathrm{PG}(4,4)$ has not more than 115 points. Using the trivial construction (Remark 3.1.) trippling the number of points in the higher dimension one gets a $(93,3)$-cap in $\mathrm{PG}(4,4)$. We can get a $(95,3)$-cap by acting on the coordinate positions of the points

$$
\begin{matrix}
1222333121321233323\\
0101133112123111222\\
0011110111222331233\\
0000001111111111111\\
0000000000000001111
\end{matrix}
$$

with the cyclic group $\langle g \rangle$ of order 5. It is assumed here that $(x_0, x_1, x_2, x_3, x_4)^g = (x_1, x_2, x_3, x_4, x_0)$. For the sake of brevity, the field elements $0, 1, \alpha, \alpha^2$ are denoted by $0, 1, 2, 3$, respectively.

In PG$(3, 5)$, it was known that a $(k, 3)$-cap contains at most 48 points [9]. The parameters in this case are small enough to make a brute-force attack feasible. Assuming the existence of an 11-plane in a maximal $(k, 3)$-arc and using the classification of the plane $(11, 3)$-arcs (cf. e.g. [7]), we can fix (up to equivalence) a part of the arc. It is then possible to perform an exhaustive search for all possible extensions of the fixed set to a $(k, 3)$-arc. The largest size of a cap thus obtained is 44. Clearly, a cap with more than 43 points has to have an 11-plane [9]. This implies that 44 is the largest size of a cap in PG$(3, 5)$.

Theorem 7. *The largest size of a* $(k, 3)$*-cap in* PG$(3, 5)$ *is 44.*

We give examples of two non-isomorphic $(44, 3)$-caps in PG$(3, 5)$. The homogeneous coordinates of the points are given as columns of the matrices below.

$$
\begin{matrix}
10101024214010324122314004133122403041412243\\
01100112344001122330011344112334400112240234\\
00011111111000000000111111222222233333334444\\
00000000000111111111111111111111111111111111
\end{matrix}
$$

with spectrum

$$a_2 = 8, a_4 = 8, a_7 = 14, a_8 = 12, a_9 = 40, a_{10} = 52, a_{11} = 22,$$

and $a_i = 0$ for $i \neq 2, 4, 7 \ldots, 11$, and

$$
\begin{matrix}
10101024210101322014340142323142041234231203\\
01100112340011234122334401122440223344001133\\
00011111110000000111111222222233333333444444\\
00000000001111111111111111111111111111111111
\end{matrix}
$$

with spectrum

$$a_2 = 6, a_3 = 5, a_4 = 2, a_5 = 4, a_6 = 5, a_7 6, a_8 = 12, a_9 = 36, a_{10} = 63, a_{11} = 17,$$

$a_i = 0$ for $i \neq 2, 3, \ldots, 11$. Let us note that this is not a classification result.

Modifying the search, we can obtain a result, which is not so interesting in the context of the maximal cap problem, but has important implications for the main coding theory problem for four-dimensional codes over $\mathbb{F}_5$. Here we state it separately. If we assume that the maximal multiplicity of a plane in $\mathrm{PG}(3,5)$ is 10, we can use the classification of all $(10,3)$-arcs to fix a part of the arc and try all possible completions. It turns out that the maximal size of a $(k,3)$-cap in $\mathrm{PG}(3,5)$ without 11-planes is 40.

Theorem 8. *Every $(k,3)$-cap in $\mathrm{PG}(3,5)$ with $k \geq 41$ has an 11-plane.*

Theorem 7 implies a better bound on the size of a $(k,3)$ cap in larger dimensions. So, the maximal size of a cap in $\mathrm{PG}(4,5)$ is bounded by $k \leq 209$ ($k \leq 6 \cdot 44 - 5 \cdot 11$), while the general bound (4) gives only $k \leq 251$.

There exists a (145,3)-cap in $\mathrm{PG}(4,5)$ having a cyclic automorphism of order 5. The generators of the 29 orbits of length 5 are given as columns of the following matrix.

11113421342312221212232324343
01012231223144122423221144234
00111110000111223344112222443
00000001111111111111111111112
00000000000000000000111111111

There is a (467,3)-cap in $\mathrm{PG}(5,5)$. It is invariant under the symmetric group S_6 acting on the points. The orbit lengths are $90, 60, 60, 60, 60, 45, 30, 30, 20, 6, 6$. Below, we give as columns representatives of the point orbits:

34224432132
34121421111
21111110111
21110110011
11010010011
10000010011

There is a better construction though. If we start with an $(11,3)$-arc in $\mathrm{AG}(2,5)$ (which exists since each one of the two such arcs has an empty line) and the $(44,3)$-cap in $\mathrm{PG}(3,5)$, we get by Corollary 4 a $(484,3)$-cap in $\mathrm{PG}(5,5)$.

We now turn to caps with $n = 3$ in $\mathrm{PG}(t,7)$. In R. Hill's bound $\alpha(7) = 3$ and $k \leq 96$ for $t = 3$.

The largest $(k,3)$-cap, we can construct in $\mathrm{PG}(3,7)$ so far is a (70,3)-cap. The following is a nice description regarding the points as elements in $\mathrm{GF}(7^4)$.

Take $GF(7^4)$ and the group of 5th unit roots. The 70 points are the cosets of a^x with a a primitive root and $x \in \{0, 4, 7, 8, 12, 31, 32, 36, 53, 56, 57, 59, 64, 72\}$.

There is a (300,3)-cap in PG(4,7) invariant under the symmetric group S_5. The orbit lengths are $60, 60, 60, 30, 20, 20, 20, 15, 5, 5, 5$. Representatives of the points are:

66653566156
25252346011
13121111011
11011111011
01011110011

There is a (1422,3)-cap in PG(5,7) invariant under S_6 acting on the points. The orbit lengths are $360, 180, 180, 120, 90, 60, 60, 60, 60, 60, 60, 30, 30, 30, 15, 15, 6, 6$. Representatives of the point orbits are:

556566524544646613
324466413512236101
212241413111111001
112131101101111001
101111101101111001
001110101001111001

The table below summarizes our knowledge on the best lower and upper bounds on the sizes of caps with $n = 3$ over some small fields.

Table 1. Maximal sizes of $(k, 3)$-caps in PG(t, q), $t = 3, 4, 5$, $q = 4, 5, 7$.

	$q = 4$	$q = 5$	$q = 7$
PG$(3, q)$	31	44	70–96
PG$(4, q)$	95–115	145–209	300–663
PG$(5, q)$	285–451	484–1034	1422–4632

The table can be extended to geometries of larger dimension and over larger fields. Unfortunately, we do not know results that are better than the general bounds provided by Theorem 1, Theorem 3 and Theorem 6.

4.2 Caps with $n = 4$

It has been mentioned already that there is a $(76, 4)$-cap in PG$(3, 5)$ constructed as a Griesmer code in [2]. Let us note that the only possible intersection numbers of this cap are 1, 6, 11, and 16. There is a trivial upper bound of 376 on the size of a $(k, 4)$-cap in PG$(4, 5)$. The divisibility property of the caps with parameters $(76, 4)$ implies an improvement on this bound.

Theorem 9. *Let $\mathfrak{K}$ be a $(k,4)$-cap in* $\mathrm{PG}(4,5)$*. Then $k \leq 371$.*

Proof. Assume $\mathfrak{K}$ is a $(372,4)$-cap in $\mathrm{PG}(4,5)$. By the Griesmer bound, such a cap should have a hyperplane (solid) of multiplicity 76 which can be viewed as a $(76,4)$-cap in $\mathrm{PG}(3,5)$. Such a cap is associated with a $[76,4,60]_5$-code which is divisible with weights 60,65,70,75. Actually the code from [2] does not have words of weight 75. Hence the multiplicities of the planes in a 76-solid are 16, 11, 6, and, possibly 1. By a counting of the number of points through a plane of maximal multiplicity contained in a w-solid, $0 \leq w \leq 76$, we get that the only admissible multiplicities for solids are $0, 1, 22, \ldots, 26, 72, \ldots, 76$. Now note that a $(76,4)$-cap in $\mathrm{PG}(3,5)$ necessarily has a plane π of multiplicity 11. (If we assume the opposite we arrive at a contradiction by counting the multiplicities of the planes through a 1-line in a 6-plane, or through a 0-line in a 1-plane.) Count the multiplicities of the points in the solids S_i, $i = 0, \ldots, 5$, through π. Clearly,

$$372 = \sum_{i=0}^{5} \mathfrak{K}(S_i) - 5\mathfrak{K}(\pi) \geq 6 \cdot 72 - 5 \cdot 11 = 377,$$

a contradiction. □

There exists a $(123,4)$-cap in $\mathrm{PG}(3,7)$. It can be obtained by acting with the symmetric group S_4 on the coordinates of the following points:

556245632366
211133511116
111011111111
000011101111

A $(168,4)$-cap in $\mathrm{PG}(3,8)$ can be obtained by acting with the same group on the coordinates of the points

7342357556567
4111222344111
2001111111111
1000111111000

Here the field with eight elements is obtained as $\mathbb{F}_2[x]/(x^3+x+1)$. The coefficients of the binary representation of the integers in the matrix are the coefficients of the field element represented as element in $\mathbb{F}_2[x]/(x^3+x+1)$. So, 0 represents 0, 1 represents 1, 2 represents x, 3 represents $1+x$ etc.

A $(312, 4)$-cap in $\mathrm{PG}(4, 5)$ is obtained by acting on the points

$$\begin{array}{c}121223241200\\000000000000\\000000000000\\110011223341\\001111111111\end{array}$$

with the elements of a cyclic group of order 31 generated by the matrix

$$\begin{pmatrix} 1 & 3 & 3 & 0 & 0 \\ 2 & 1 & 3 & 0 & 0 \\ 4 & 4 & 3 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

A $(526, 4)$-cap in $\mathrm{PG}(4, 7)$ is obtained by acting on the points

$$\begin{array}{c}1021601520534132431420\\0100012346122301232230\\0010000000111122223330\\0000000000000000000000\\0001111111111111111111\end{array}$$

with the elements of a cyclic group of order 25 generated by

$$\begin{pmatrix} 2 & 3 & 1 & 0 & 0 \\ 2 & 6 & 2 & 1 & 0 \\ 0 & 1 & 1 & 2 & 0 \\ 5 & 4 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Similarly, an $(846, 4)$-cap in $\mathrm{PG}(4, 8)$ is obtained by acting on the points

$$\begin{array}{c}12041410312000\\00112267747010\\00000000011440\\00000000000000\\11111111111111\end{array}$$

with a cyclic group of order 65 generated by

$$\begin{pmatrix} 5 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 4 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

A $(1232,4)$-cap in $\mathrm{PG}(5,5)$ and a $(2933,4)$-cap in $\mathrm{PG}(5,7)$ can be obtained under the action of S_6 on the coordinates of the points given by the matrices

$$\begin{array}{c}
443432334443444343411 \\
232221122342231340 1 \\
\end{array}$$

$$\begin{array}{c}
4545656566566646665266461 \\
3333336523461436242661111 \\
\end{array}$$

In $\mathrm{PG}(5,8)$, we obtain a $(4704,4)$-cap by using the product construction (Theorem 3) with ingredients an affine $(28,4)$-arc in $\mathrm{PG}(2,8)$ and an $(168,4)$-cap in $\mathrm{PG}(3,8)$. Since the latter cap is affine, the resulting $(4704,4)$-cap has also an empty plane and can be further used in the recursive constructions.

We summarize our knowledge on the $(k,4)$-caps in the table below.

Table 2. Maximal sizes of $(k,4)$-caps in $\mathrm{PG}(t,q)$ for $t=3,4,5$, $q=5,7,8$.

	$q=5$	$q=7$	$q=8$
$\mathrm{PG}(3,q)$	76	123–148	168–220
$\mathrm{PG}(4,q)$	312–371	526–1030	846–1756
$\mathrm{PG}(5,q)$	1232–1876	2933–7204	4704–14044

5 Caps and Linear Codes

Some of the results in the previous section can help us to solve some open problems on optimal linear codes.

A linear code is a k-dimensional subspace C of the vector space of all n-tuples $\mathbb{F}_q^n$ over the field $\mathbb{F}_q$. The minimum distance between two different codewords with respect to the Hamming metric is called the minimum distance of the linear code. A linear code of length n, dimension k and minimum distance d is referred to as an $[n,k,d]_q$-code. It is well-known that the existence of an $[n,k,d]_q$-linear code C is equivalent to that of a $(n,n-d)$-multiarc in $\mathrm{PG}(k-1,q)$. More precisely, one can associate a multiset in $\mathrm{PG}(k-1,q)$ with every ordered basis of C in such a way that two multisets in $\mathrm{PG}(k-1,q)$ are projectively equivalent if and only if they are associated with codes that are semilinearly isomorphic. The problem of optimizing one of the parameters n, k, d for fixed values of the other two is sometimes called the main problem of coding theory. It might turn out that a code is optimal with respect to one of the parameters, but not optimal with respect to some of the others. However, if a code is optimal with respect to the length it is also optimal with respect to the dimension and the minimum distance. The smallest length for which there exists a linear code over $\mathbb{F}_q$ of fixed dimension k and fixed minimum distance d is denoted by $n_q(k,d)$. The Griesmer bound [5] is a natural lower bound on the function $n_q(k,d)$:

$$n_q(k,d) \geq g_q(k,d) := \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil.$$

Let C be an $[n,k,d]_q$-code and let $\mathfrak{K}$ be an $(n, n-d)$-arc associated with C. Important invariants of the weight function of $\mathfrak{K}$ are the non-negative integers γ_i, $i = 0, \ldots, k-2$, defined as the maximal multiplicity of a subspace in $\mathrm{PG}(k-1,q)$ of projective dimension i. It is easily checked that if $n = t + g_q(k,d)$ then

$$\gamma_j \leq t + \sum_{i=0}^{j} \lceil \frac{d}{q^i} \rceil.$$

The problem of finding the exact value of $n_q(k,d)$ has been resolved for small fields and small dimensions only. In case of $q = 5$ the exact values of $n_5(k,d)$ are known for $k \leq 3$ for all d and for $k = 4$ for all $d \neq 31, 32, 36, 37, 81, 82, 161, 162$. The bounds on $n_5(4,d)$ in these eight open cases are listed in the table below.

d	$g_5(4,d)$	$n_5(4,d)$	$n_5(4,d)$ this paper
31	41	41 – 42	42
32	42	42 – 43	43
36	47	47 – 48	48
37	48	48 – 49	49
81	103	103 –104	103 –104
82	104	104 –105	104 –105
161	203	203 –204	203 –204
162	204	204 –205	204 –205

For the first four cases, we have the following simple observation.

Lemma 10. *(i) Let $\mathfrak{K}$ be a $(41,10)$- or $(42,10)$-arc in $\mathrm{PG}(3,5)$. Then $\gamma_0 = 1, \gamma_1 = 3, \gamma_2 = 10$.*

(*ii*) *Let* $\mathfrak{K}$ *be a* $(47,11)$- *or* $(48,11)$-*arc in* $\mathrm{PG}(3,5)$. *Then* $\gamma_0 = 1, \gamma_1 = 3, \gamma_2 = 10$.

By theorems 7 and 8, we get immediately the following corollaries.

Corollary 11. *There exist no* $(41,10)$-*arcs and no* $(42,10)$-*arcs in* $\mathrm{PG}(3,5)$. *Equivalently, there are no* $[41,4,31]_5$-*codes and no* $[42,4,32]_5$-*codes and* $n_5(4,31) = 42$, $n_5(4,32) = 43$.

Corollary 12. *There exist no* $(47,11)$-*arcs and no* $(48,11)$-*arcs in* $\mathrm{PG}(3,5)$. *Equivalently, there are no* $[47,4,36]_5$-*codes and no* $[48,4,37]_5$-*codes and* $n_4(4,36) = 48$, $n_5(4,37) = 49$.

These results have implications also in the larger dimensions.

Corollary 13. *There exist no* $(43,11)$-*arcs, no* $(48,12)$-*arcs and no* $(49,12)$-*arcs in* $\mathrm{PG}(4,5)$. *Equivalently, there exist no Griesmer* $[43,5,32]_5$-, $[48,5,36]_5$- *and* $[49,5,37]_5$-*codes.*

Proof. Let $\mathfrak{K}$ be a $(43,11)$-arc in $\mathrm{PG}(4,5)$. The projection from a 1-point is a $(42,10)$-arc in $\mathrm{PG}(3,5)$ which does not exist. The same argument applies for the other parameter sets. □

Corollary 14. *There exist no* $(198+i,42)$-*arcs in* $\mathrm{PG}(4,5)$ *for* $i = 0,\ldots,4$. *Equivalently, there exist no Griesmer* $[198+i,5,156+i]_5$-*codes,* $i = 0,\ldots,4$.

Corollary 15. *There exist no* $(223+i,47)$-*arcs and no* $(229+i,48)$-*arcs in* $\mathrm{PG}(4,5)$ *for* $i = 0,\ldots,4$. *Equivalently, there exist no* $[223+i,5,176+i]_5$- *and no* $[229+i,5,181+i]_5$ *codes,* $i = 0,\ldots,4$.

Acknowledgements. The research of the first author takes place within the project “Linear codes and cryptography” of the Fund for Scientific Research Flanders (FWO-Vlaanderen), Project Nr. G.0317.06, and is supported by the Interuniversitary Attraction Poles Programme – Belgian State – Belgian Science Policy: project P6/26-BCrypt. The second author gratefully acknowledges the support by the Strategic Development Fund of The New Bulgarian University under Contract 357/14.05.2009. This research was also supported by the Project *Combined algorithmic and theoretical study of combinatorial structures* between the Fund for Scientific Research Flanders-Belgium and the Bulgarian Academy of Sciences.

References

[1] J. Bierbrauer, Introduction to Coding Theory, Chapman & Hall/ CRC Press, 2005.

[2] I. Boukliev, S. Kapralov, T. Maruta, M. Fukui, Optimal quaternary linear codes of dimension five, IEEE Trans. Inf. Theory 43(1997), 308–313.

[3] D. L. Bramwell, B. J. Wilson, Cubic caps in three-dimensional Galois space, Proc. Royal Irish Acad., Sect. A 73(1973), 279–283.

[4] Y. Edel, J. Bierbrauer, Recursive constructions for large caps, Bull. Belgian Math. Society - Simon Stevin 6(1999), 249–258.

[5] J. H. Griesmer, A bound for error-correcting codes, IBM J. Res. Develop. 4(1960), 532–542.

[6] R. Hill, Some results concerning linear codes and $(k, 3)$-caps in three-dimensional Galois space, Math. Proc. Cambridge Philosophical Society 84(1978), 191–205.

[7] J. W. P. Hirschfeld, Projective Geometries over Finite Fields, Oxford University Press, 1998.

[8] J. W. P. Hirschfeld, L. Storme, The Packing problem in statistics, coding theory and finite projective spaces: update 2001, in: *Finite Geometries*, A. Blokhuis et al. (eds.), 2001, 201–246.

[9] I. Landjev, A. Rousseva, T. Maruta, R. Hill, On optimal codes over the field with five elements, Des. Codes Cryptogr. 29(2003), 165–175.

[10] T. Maruta, M. Shinohara, A. Kikui, On optimal linear codes over $\mathbb{F}_5$, Discrete Math., to appear.