Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 51–56*

A probabilistic construction of low density quasi-perfect linear codes

Daniele Bartoli, Stefano Marcugini, Fernanda Pambianco
{daniele.bartoligino,fernanda}@dmi.unipg.it
Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, Perugia, 06123, Italy

Abstract. In this work $[n, n-N-1, 4]_q 2$ covering codes with $n = O(q^{\frac{N-1}{2}} \log^{300} q)$ are obtained by probabilistic methods. This construction gives a new upper bound for $l(m, 2, q)_4$, that is the minimal length n for which there exists an $[n, n-m, 4]_q 2$ covering code with given m and q. The result has been obtained via the connection with Projective Geometry and it gives an upper bound on the minimum size of complete caps in projective spaces $\mathrm{PG}(N, q)$.

1 Introduction

Let $\mathbb{F}_q$ be the finite field with q elements. A q-ary linear code $\mathcal{C}$ of length n and dimension k is a k-dimensional linear subspace of $\mathbb{F}_q^n$. The Hamming weight $w(\mathbf{x})$ of $\mathbf{x}$ is the number of nonzero positions in a vector $\mathbf{x} \in \mathcal{C}$. The minimum distance of $\mathcal{C}$ is defined as

$$d(\mathcal{C}) := \min\{w(\mathbf{x}) | \mathbf{x} \in \mathcal{C}, \mathbf{x} \neq 0\}$$

and a q-ary linear code of length n, dimension k, and minimum distance d is denoted as an $[n, k, d]_q$-code. An $[n, k, d]_q$-code can correct at most t errors, where t is $\lfloor \frac{d-1}{2} \rfloor$. The covering radius of $\mathcal{C}$ is the minimum integer $R(\mathcal{C})$ such that for any vector $v \in \mathbb{F}_q^n$ there exists $x \in \mathcal{C}$ with $w(v - x) \leq R$. An $[n, k, d]_q$-code with covering radius R is denoted by $[n, k, d]_q R$. If $R = t$ then $\mathcal{C}$ is said to be perfect. As there are only finitely many classes of linear perfect codes, of particular interest are those codes $\mathcal{C}$ with $R = t + 1$, called quasi-perfect codes; see [4, 6, 7]. The covering density $\mu(\mathcal{C})$, introduced in [8], is one of the parameters characterizing the covering quality of an $[n, k, d]_q R$-code $\mathcal{C}$ and it is defined by $\mu(\mathcal{C}) = \frac{1}{q^{n-k}} \sum_{i=0}^{R} (q-1)^i \binom{n}{i}$. Note that $\mu(\mathcal{C}) \geq 1$, and that equality holds when $\mathcal{C}$ is perfect. Clearly, among codes with the same codimension and covering radius the shortest ones have the best covering density. Therefore the problem of determining the minimal length n for which there exists an $[n, n-m, d]_q R$-code with given m, q, d, and R, has been widely investigated; see [5]. Throughout, such minimal length will be denoted $l(m, R, q)_d$.

This paper deals with estimating $l(m, R, q)_d$ for $R = 2$ and $d = 4$, that is, quasi-perfect linear codes that are both 1-error correcting and 2-error detecting. The columns of a parity check matrix of an $[n, n-m, 4]_q$2-code can be considered as points of a complete n-cap in the finite projective space $\mathrm{PG}(m-1, q)$. For this reason these codes have been investigated also through their connection with Projective Geometry; see e.g. [15].

A n-cap in an (affine or projective) Galois space over the finite field $\mathbb{F}_q$ is a set of n points no three of which are collinear. A n-cap is said to be complete if it is not contained in a $(n+1)$-cap. A plane n-cap is also called a n-arc.

A central problem concerning caps is determining the spectrum of the possible sizes of complete caps in a given space, see the survey paper [16] and the references therein. As mentioned above, of particular interest for applications to Coding Theory is the lower part of the spectrum.

For the size of the smallest complete cap in the projective space $\mathrm{PG}(N, q)$ of dimension N over $\mathbb{F}_q$, the trivial lower bound is $\sqrt{2}q^{\frac{N-1}{2}}$. General constructions of complete caps whose size is close to this lower bound are known only for q even and N odd; see [10, 12, 13, 18]. When N is even, complete caps of size of the same order of magnitude as $cq^{N/2}$, with c a constant independent of q, are known for both the odd and the even order case, see [10, 11, 13–15].

If q is odd and $N \equiv 0 \pmod 4$, small complete caps can be obtained via the product method for caps from bicovering plane arcs. It has been shown in [14] that the cartesian product of a bicovering k-arc A in the affine plane $\mathrm{AG}(2, q)$ and the cap of size $q^{\frac{N-2}{2}}$ in the affine space $\mathrm{AG}(N-2, q)$ arising from the blow-up of a parabola of $\mathrm{AG}(2, q^{(N-2)/2})$ is a complete cap in $\mathrm{AG}(N, q)$. Via the natural embedding of $\mathrm{AG}(N, q)$ in $\mathrm{PG}(N, q)$ it is possible to obtain from a complete cap in $\mathrm{AG}(N, q)$ a complete cap in $\mathrm{PG}(N, q)$ of the same magnitude.

In [1] the authors obtain caps of size $(k+1)q^{\frac{N-2}{2}}$ in $\mathrm{AG}(N, q)$ when the k-arc A is almost bicovering, that is, a complete arc which bicovers all points in $\mathrm{AG}(2, q) \setminus A$ but one.

By similar methods, in [2] the authors provide new complete caps in $\mathrm{AG}(N, q)$ with roughly $q^{(4N-1)/8}$ points, studying both plane cubics with a node and plane cubics with an isolated double point.

In [1] the existence of complete caps in $\mathrm{AG}(N, q)$, $N \equiv 0 \pmod 4$, of size of the same order of magnitude as $2pq^{\frac{1}{2}(N-\frac{1}{4})}$, provided that the characteristic p of $\mathbb{F}_q$ is large enough and $\log_p q > 8$, is established.

The exact value $t_2(N, q)$ of the minimum size of a complete cap in $\mathrm{PG}(N, q)$ is known only for few pairs (N, q): for instance in the case $N = 3$, $t_2(3, q)$ is known only for $q \leq 7$; see [9, Table 3].

In the case $N = 3$ according to the survey paper [16], the smallest known complete caps in $\mathrm{PG}(3, q)$, with q arbitrary large, have size approximately $q^{3/2}/2$ and were presented by Pellegrino in 1998 [19]. However, Pellegrino's completeness proof appears to present a major gap, and counterexamples can be found;

see [3, Section 2].

In this work, the existence of complete caps of size

$$O(q^{\frac{N-1}{2}} \log^{300} q) \tag{1}$$

in projective spaces $\mathrm{PG}(N,q)$, with $N \geq 3$, is established by probabilistic methods. This bound is asymptotically very close to the trivial lower bound. The construction of these complete caps gives, via the connection between Coding Theory and Projective Geometry, the following upper bound on $l(N+1,2,q)_4$.

Theorem 1. *There exists a positive constant M such that for every $q \geq M$*

$$l(N+1,2,q)_4 = O(q^{\frac{N-1}{2}} \log^{300} q).$$

In term of complete caps in any projective space $\mathrm{PG}(N,q)$ we proved the following theorem.

Theorem 2. *There are positive constants c and M such that in every projective space of order $q \geq M$ and dimension N, there is a complete cap of size at most*

$$O\left(q^{\frac{N-1}{2}} log^c q\right).$$

Also, as in [17], a randomized algorithm to construct the desired complete caps can be easily deduced.

2 Algorithm

2.1 The algorithm

The cap is constructed in the following way. At the beginning, the starting cap A_0 is empty. Let $\Omega_0 = S_0$ be the set of all the points of the projective space $\mathrm{PG}(N,q)$. Roughly speaking, at each step Ω_i is essentially the set of points which are not covered by the cap A_i, while S_i is a subset of Ω_i. At step i a random subset $B_i \subset S_i$ is selected, choosing each point from S_i independently with the same probability p_i. The set B_i is the *nibble* (see also [17, Section 2.1]) and only a subset of B_i is added to A_i to obtain the new cap A_{i+1}. This subset $M_i \subset B_i$ is the set of the points not causing any conflict. At the subsequent step, Ω_{i+1} is obtained from Ω_i by deleting all the points covered by the secants of A_{i+1} or in B_i, while S_{i+1} is obtained by deleting from S_i the points covered by the secants of A_{i+1} or in B_i plus a few more points, chosen randomly: in this way certain structural properties of the S_i's are preserved. The process is repeated until all but $q^{\frac{N-1}{2}} \log^c q$ points are covered by the secants of the current cap. In the following we set $\theta = \log^{-2} q$.

The algorithm acts as follows. At each step we use three different subphases: **choose**, **delete**, and **compensate**.

Start : Ω_0, S_0 are both $\mathrm{PG}(N,q)$, $A_0 = \emptyset$. We also consider the quantity b_i. At the beginning $b_0 = 1$, while at the i-th step

$$b_i = \frac{|S_i|}{q^N + q^{N-1} + \cdots + q + 1}.$$

Choose : At each step a point v in S_i is chosen with probability

$$p_i = \theta(b_i q^{\frac{N+1}{2}})^{-1}.$$

The set of all the chosen points is B_i. A point x in B_i is *good* in $A_i \cup B_i$ if there are no two points in $A_i \cup B_i$ collinear with x. The set M_i is the set of all the good points. So $A_{i+1} = A_i \cup M_i$.

Delete : Delete from Ω_i all the points in bisecants of A_{i+1} or in B_i. Let D_i be the set of deleted points and, if $v \in \Omega_i$, let $P_i(v) = Pr(v \in D_i)$. Let P_i^u and P_i^ℓ be the upper and the lower bounds for these probabilities.

Compensate : S_{i+1} is obtained from S_i deleting the points of D_i and independently the points of S_i with probability

$$P_i^{com}(v) = \frac{P_i^u - P_i(v)}{1 - P_i(v)}.$$

Let R_i be the set of the removed points, then

$$\Omega_{i+1} = \Omega_i \setminus D_i, \quad S_{i+1} = S_i \setminus (D_i \cup R_i), \quad A_{i+1} = A_i \cup M_i$$

and

$$b_{i+1} = b_i(1 - P_i^u) = \prod_{j=1}^{i}(1 - P_j^u).$$

Stop : The algorithm stops after K steps, where K is the smallest integer such that

$$b_K \leq q^{-\frac{N+1}{2}} \log^c q,$$

for some constant c (we will set $c = 300$, as in [17]).

The importance of the subphase of Compensation is explained in the following remark.

Remark 3. The operation of compensation is made in order to give the same probability to the points in S_i to be in S_{i+1}. In fact, if $p = P_i(v)$, then

$$P(v \notin S_{i+1} | v \in S_i) = p + (1-p)\frac{P_i^u - p}{1-p} = P_i^u.$$

So,

$$\mathbb{E}(|S_{i+1}|) = |S_i|(1 - P_i^u).$$

References

[1] N. Anbar, D. Bartoli, M. Giulietti, and I. Platoni, Small complete caps from singular cubics, *J. Combin. Des.*, DOI:10.1002/jcd.21366, 2013.

[2] N. Anbar, D. Bartoli, M. Giulietti, and I. Platoni, Small complete caps from singular cubics II, *J. Algebraic Combin.*, DOI:10.1007/s10801-014-0532-7, 2014.

[3] D. Bartoli, G. Faina, and M. Giulietti, Small complete caps in three-dimensional Galois spaces, *Finite Fields Appl.*, vol. 24, pp. 184–191, 2013.

[4] R. A. Brualdi, S. Litsyn, and V. S. Pless, *Handbook of Coding Theory.* Eds. Amsterdam, The Netherlands, 1998, vol. 1, ch. Covering radius, pp. 755–826.

[5] R. A. Brualdi, V. S. Pless, and R. M. Wilson, Short codes with a given covering radius, *IEEE Trans. Inf. Theory*, vol. 35, no. 1, pp. 99–109, 1989.

[6] G. D. Cohen, S. Honkala, I. S. Litsyn, and A. C. Lobstein, *Covering Codes.* Amsterdam, The Netherlands: Elsevier, 1997.

[7] G. D. Cohen, M. G. Karpovsky, H. F. Mattson Jr., and J. R. Schatz, Covering radius - survey and recent results, *IEEE Trans. Inf. Theory*, vol. 31, no. 3, pp. 328–343, 1985.

[8] G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, Further results on the covering radius of codes, *IEEE Trans. Inf. Theory*, vol. 32, no. 5, pp. 680–694, 1986.

[9] A. A. Davydov, G. Faina, S. Marcugini, and F. Pambianco, On sizes of complete caps in projective spaces $\mathrm{PG}(n,q)$ and arcs in planes $\mathrm{PG}(2,q)$, *J. Geom.*, vol. 94, no. 1-2, pp. 31–58, 2009.

[10] A. A. Davydov, M. Giulietti, S. Marcugini, and F. Pambianco, New inductive constructions of complete caps in $\mathrm{PG}(n,q)$, q even, *J. Combin. Des.*, vol. 18, no. 3, pp. 177–201, 2010.

[11] A. A. Davydov and P. R. J. Östergård, Recursive constructions of complete caps, *J. Statist. Planning Infer.*, vol. 95, no. 1, pp. 167–173, 2001.

[12] E. M. Gabidulin, A. A. Davydov, and L. M. Tombak, Linear codes with covering radius 2 and other new covering codes, *IEEE Trans. Inform. Theory*, vol. 37, pp. 219–224, 1991.

[13] M. Giulietti, Small complete caps in $\mathrm{PG}(n,q)$, q even, *J. Combin. Des.*, vol. 15, no. 5, pp. 420–436, 2007.

[14] M. Giulietti, Small complete caps in Galois affine spaces, *J. Algebraic Combin.*, vol. 25, no. 2, pp. 149–168, 2007.

[15] M. Giulietti and F. Pasticci, Quasi-perfect linear codes with minimum distance 4, *IEEE Trans. Inform. Theory*, vol. 53, no. 5, pp. 1928–1935, 2007.

[16] J. W. P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces: update 2001, *Developments in Mathematics*, vol. 3, pp. 201–246, 2001.

[17] J. H. Kim and V. H. Vu, Small complete arcs in projective planes, *Combinatorica*, vol. 23, no. 2, pp. 311–363, 2003.

[18] F. Pambianco and L. Storme, Small complete caps in spaces of even characteristic, *J. Combin. Theory Ser. A*, vol. 75, no. 1, pp. 70–84, 1996.

[19] G. Pellegrino, On complete caps, not ovaloids, in the space $\mathrm{PG}(3, q)$ with q odd, *Rend. Circ. Mat. Palermo*, vol. 47, pp. 141–168, 1998.