Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 70-75*

Linear covering codes over nonbinary finite fields

Alexander Davydov adav@iitp.ru
Institute for Information Transmission Problems, Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, Moscow, 127994, RUSSIA

Massimo Giulietti, Stefano Marcugini, Fernanda Pambianco
giuliet, gino, fernanda@dipmat.unipg.it
Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, Perugia, 06123, ITALY

Abstract. For a prime power q and for integers R, η with $R > 0$, $0 \leq \eta \leq R-1$, let $\mathcal{A}^{(\eta)}_{R,q} = (\mathcal{C}_{n_i})_i$ denote an infinite sequence of q-ary linear $[n_i, n_i - r_i]_q R$ codes $\mathcal{C}_{n_i}$ with covering radius R and such that the following two properties hold: (a) the codimension $r_i = Rt_i + \eta$, where $(t_i)_i$ is an increasing sequence of integers; (b) the length n_i of $\mathcal{C}_i$ coincides with $f^{(\eta)}_q(r_i)$, where $f^{(\eta)}_q$ is an increasing function. In this paper, sequences $\mathcal{A}^{(\eta)}_{R,q}$ with asymptotic covering density bounded from above by a constant independent of q are constructed for an arbitrary R, and for each value of $\eta \in \{0, 1, \ldots, R-1\}$, under the condition that $q = (q')^R$. The key tool is the description of new small saturating sets in projective spaces over finite fields, which are the starting point for the q^m-concatenating constructions of covering codes. A new concept of N-fold strong blocking set is introduced. Several upper bounds on the length function of covering codes and on the smallest sizes of saturating sets are improved.

1 Introduction

Denote by F_q the Galois field with q elements. Let F_q^n be the n-dimensional vector space over F_q. Denote by $[n, n-r]_q$ a q-ary *linear code* of length n and codimension r. The *covering radius* of an $[n, n-r]_q$ code is the least integer R such that F_q^n is covered by spheres of radius R centered on codewords. An $[n, n-r]_q R$ code is an $[n, n-r]_q$ code with covering radius R. For an introduction to coverings of vector spaces over finite fields, see [1] .

The covering quality of an $[n, n-r(\mathcal{C})]_q R$ code $\mathcal{C}$ can be measured by its *covering density*

$$\mu_q(n, R, \mathcal{C}) = q^{-r(\mathcal{C})} \sum_{i=0}^{R} (q-1)^i \binom{n}{i} \geq 1. \tag{1}$$

From the point of view of the covering problem, the best codes are those with small covering density.

For given integers R, η with $R > 0$, $0 \le \eta \le R-1$, and for a fixed prime power q, let $\mathcal{A}_{R,q}^{(\eta)} = (\mathcal{C}_{n_i})_i$ denote an infinite sequence of q-ary linear $[n_i, n_i - r_i]_q R$ codes $\mathcal{C}_{n_i}$ with covering radius R and such that the following two properties hold:

(a) the codimension $r_i = Rt_i + \eta$, where $(t_i)_i$ is an increasing sequence of integers;

(b) the length n_i of $\mathcal{C}_i$ coincides with $f_q^{(\eta)}(r_i)$, where $f_q^{(\eta)}$ is an increasing function.

We call $\mathcal{A}_{R,q}^{(\eta)}$ an *infinite family of covering codes* or an *infinite code family,* or simply *infinite family.*

Considering families of type $\mathcal{A}_{R,q}^{(\eta)}$ is a standard method of investigation of *linear* covering codes, see [1]-[5], and the references therein. In particular, it is related to the fact that families with distinct values of η often have distinct properties. Throughout the paper, distinct families $\mathcal{A}_{R,q}^{(\eta)}$ with the same parameters η, R, q will be denoted as follows: $\mathcal{A}_{R,q,1}^{(\eta)}$, $\mathcal{A}_{R,q,2}^{(\eta)}$, and so on.

For an infinite code family $\mathcal{A}_{R,q}^{(\eta)}$, its *asymptotic covering density* is defined as follows:

$$\overline{\mu}_q(R, \mathcal{A}_{R,q}^{(\eta)}) = \liminf_{i \to \infty} \mu_q(n_i, R, \mathcal{C}_{n_i}). \qquad (2)$$

The size q of the base field F_q is fixed for a given family, but, when an infinite set of families is considered, the value of q can infinitely grow. A central problem for covering codes is the following: for fixed R and η *find a set of sequences $\mathcal{A}_{R,q}^{(\eta)}$ of q-ary codes with q running over an infinite set of prime power, such that the asymptotic covering density of every sequence is bounded from above by a constant independent of q.* Each sequence of such a set is said to be *good.* Accordingly, an $[n, n-r]_q R$ covering code is called *good* or *short* if $n = O(q^{\frac{r-R}{R}})$. By (1) and (2), a sequence $\mathcal{A}_{R,q}^{(\eta)}$ consisting of good codes is good. So far, the problem has been solved only for $\eta = 0$ and arbitrary R and q, for $R = 2$, $\eta = 1$ and q a square [3, formula (33)], and for $R = 3$, $\eta = 1$ and q a cube [4, p. 540].

The main result of the paper is the construction of good infinite families $\mathcal{A}_{R,q}^{(\eta)}$ for arbitrary R and all $\eta = 0, 1, 2, \ldots, R-1$, under the condition $q = (q')^R$. A key tool in our investigation is the connection between linear covering codes and *saturating sets* in projective spaces over finite fields.

Let $PG(v, q)$ be the v-dimensional projective space over F_q. We say that a set of points $S \subseteq PG(v, q)$ is *ϱ-saturating* if for any point $x \in PG(v, q)$ there exist $\varrho + 1$ points in S generating a subspace of $PG(v, q)$ containing x, and ϱ is the smallest value with such property [2, Definition 1.1], [6]. In the literature *saturating sets* are also called *saturated sets* [2],[3], *spanning sets*, and *dense sets.*

Points of an $(R-1)$-saturating set K of size n in $PG(r-1, q)$ can be viewed as columns of a *parity check matrix* of an $[n, n-r]_q R$ *related* covering code $\mathcal{C}_K$ [2]-[6]. A saturating set K will be said to be *small* if the related covering code $\mathcal{C}_K$ if short.

A basic tool to obtain an infinite family of codes with good covering properties from a covering code are the so-called q^m-concatenating constructions [1, Section 5.4]-[5].

The good infinite families of covering codes provided in this paper are obtained by applying the q^m-concatenating constructions to covering codes related to new small saturating sets. The construction of such sets relies on a new notion of N-fold *strong* blocking set.

The *length function* $\ell_q(r, R)$ is the smallest length of a q -ary linear code with codimension r and covering radius R [1]. Existence of an $[n, n-r]_q R$ code or, equivalently, of an $(R-1)$ -saturating n-set in $PG(r-1, q)$, implies the upper bounds $\ell_q(r, R) \leq n$. Denote by $k_q(v, \varrho)$ the smallest possible size of a ϱ-saturating set in the space $PG(v, q)$. Clearly, $\ell_q(r, R) = k_q(r-1, R-1)$.

The small saturating sets and the infinite code families obtained in this paper provide an improvement on the previously known upper bounds on the length function $\ell_q(r, R)$, and on the corresponding value of $k_q(v, \varrho)$.

2 Infinite families $\mathcal{A}_{R,q}^{(0)}$ of $[n, n-Rt]_q R$ codes

The best known families $\mathcal{A}_{2,q}^{(0)}$ and $\mathcal{A}_{3,q}^{(0)}$ are given in [5]. By using them in the direct sum construction [1], we obtain an infinite family $\mathcal{A}_{R,q}^{(0)}$ of $[n, n-r]_q R$ codes with parameters

$$\mathcal{A}_{R,q}^{(0)} \; : \; R \geq 4, \; r = Rt \geq 5R, \; q \geq 7, \; q \neq 9, \; n = Rq^{\frac{r-R}{R}} + \left\lceil \frac{R}{3} \right\rceil q^{\frac{r-2R}{R}}, \; r \neq 6R.$$

The main term of the asymptotic density $\overline{\mu}_q(R, \mathcal{A}_{R,q}^{(0)})$ is $\frac{R^R}{R!}$ and it does not depend of q.

The codes of the family $\mathcal{A}_{R,q}^{(0)}$ are shorter than those of the family arising from the direct sum of the $[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1} - m]_q 1$ perfect Hamming codes, see, e.g., [2, formula (5)].

3 Small ρ-saturating sets in the spaces $PG(\rho+1, q)$

We introduce a new concept of N-fold *strong* blocking set.

Definition 3.1 *A subset B of a projective space $PG(N, q)$ is an N-*fold strong blocking set* if every hyperplane of $PG(N, q)$ is spanned by N points in B.*

Theorem 3.2 *Let $q = (q')^{\rho+1}$. Any $(\rho+1)$-fold strong blocking set in a subspace*
$PG(\rho+1, q') \subset PG(\rho+1, q)$ is a ρ-saturating set in the space $PG(\rho+1, q)$.

Theorem 3.3 *Let $q = (q')^4$. In $PG(2, q)$ there is a 1 -saturating set of size $2\sqrt{q} + 2\sqrt[4]{q} + 2$.*

Theorem 3.4 *Let $q = (q')^6$, q' prime, $q' \leq 73$. In $PG(2, q)$ there is a 1-saturating set of size $2\sqrt{q} + 2\sqrt[3]{q} + 2\sqrt[6]{q} + 2$.*

Let x_0, x_1, x_2, x_3 be homogenous coordinates for the points in $PG(3, q)$ and let l_1, l_2, l_3 be lines in $PG(3, q)$ with equations $l_1 : x_0 = x_2 = 0$; $l_2 : x_1 = x_3 = 0$; $l_3 : x_0 = x_3,\ x_1 = x_2$. The lines are contained in the hyperbolic quadric $\mathcal{Q} : x_0x_1 = x_2x_3$. Let g be any line disjoint from $\mathcal{Q}$. We denote $B = l_1 \cup l_2 \cup l_3 \cup g$. The following can be proved.

Theorem 3.5 *The set B of size $4q + 4$ is a 3-fold strong blocking set in $PG(3, q)$.*

The following result shows that N-fold strong blocking sets can be obtained by an *inductive construction* . Each inductive steps consists of embedding the blocking set in a higher dimensional space, and then adding the union of some properly chosen lines.

Theorem 3.6 *Assume that there exists an N-fold strong blocking set in $PG(N, q)$ of size k. Then there exists an $(N+1)$-fold strong blocking set in $PG(N+1, q)$ of size*
$k + 1 + (N+1)(q-1)$.

Corollary 3.7 *In $PG(N, q)$, $N \geq 3$, there exists an N-fold strong blocking set of size*

$$(q-1)\left(\frac{N(N+1)}{2} - 2\right) + N + 5.$$

Corollary 3.8 *Let $q = (q')^{\rho+1}$, $\rho > 1$. Then there exists a ρ-saturating set in $PG(\rho+1, q)$ of size*

$$(\sqrt[\rho+1]{q} - 1)\left(\frac{(\rho+1)(\rho+2)}{2} - 2\right) + \rho + 6.$$

4 Infinite families $\mathcal{A}_{R,q}^{(1)}$ of $[n, n-(Rt+1)]_q R$ codes

We use ρ-saturating sets in the spaces $PG(\rho+1, q)$, obtained in the previous section, as starting points for the q^m-concatenating constructions of [2]-[5]. To this end, it is useful that the set B described in Section 3 and the ρ-saturating set of Corollary 3.8 consist of lines.

Theorem 4.1 *There exist infinite families $\mathcal{A}^{(1)}_{R,q}$ of $[n, n-r]_q R$ codes with the following parameters:*

$$\mathcal{A}^{(1)}_{2,q,1} \ : \ R = 2,\ r = 2t+1 \geq 3,\ q = (q')^4,\ n = 2(\sqrt{q} + \sqrt[4]{q} + 1)q^{\frac{r-3}{2}} + \left\lfloor q^{\frac{r-5}{2}} \right\rfloor,$$

$$\overline{\mu}_q(2, \mathcal{A}^{(1)}_{2,q,1}) \approx 2 + \frac{4}{\sqrt[4]{q}} + \frac{6}{\sqrt{q}} + \frac{4}{\sqrt[4]{q^3}} - \frac{4}{q}.$$

$$\mathcal{A}^{(1)}_{2,q,2} \ : \ R = 2,\ r = 2t+1 \geq 3,\ q = (q')^6,\ q' \text{ prime},\ q' \leq 73,\ r \neq 9, 13,$$

$$n = 2(\sqrt{q} + \sqrt[3]{q} + \sqrt[6]{q} + 1)q^{\frac{r-3}{2}} + 2\lfloor q^{\frac{r-5}{2}} \rfloor.$$

$$\mathcal{A}^{(1)}_{3,q} \ : \ R = 3,\ r = 3t+1 \geq 7,\ q = (q')^3 \geq 64,\ n = 4(\sqrt[3]{q} + 1)q^{\frac{r-4}{3}},$$

$$\overline{\mu}_q(3, \mathcal{A}^{(1)}_{3,q}) \approx \frac{32}{3} - \frac{96}{\sqrt[3]{q}} + \frac{96}{\sqrt[3]{q^2}} - \frac{64}{3q}.$$

$$\mathcal{A}^{(1)}_{R,q} \ : \ R \geq 4,\ r = Rt+1,\ q = (q')^R,\ n = n_{R,q} q^{\frac{r-(R+1)}{R}} + (R-3)\frac{q^{\frac{r-(R+1)}{R}} - 1}{q-1},$$

$$n_{R,q} = (\sqrt[R]{q} - 1)\left(\frac{R(R+1)}{2} - 2\right) + R + 5,\ t = 1 \text{ and } t \geq t_0,\ q^{t_0 - 1} \geq n_{R,q}.$$

The main term of the asymptotic density $\overline{\mu}_q(R, \mathcal{A}^{(1)}_{R,q})$ is $\frac{(R^2+R)^R}{2^R R!}$. Significantly, it does not depend on q.

5 Infinite families $\mathcal{A}^{(\eta)}_{R,q}$ of $[n, n-(Rt+\eta)]_q R$ codes, $\eta = 2, 3, \ldots, R-1$

We construct small ρ-saturating sets in $PG(N, (q')^{\rho+1})$, $N = \rho+2, \rho+3, \ldots, 2\rho-1$.

Lemma 5.1 *Fix $1 \leq k < N$. Let B_k be the subset of $PG(N, q)$ consisting of points whose weight is at most $N - k + 1$, i.e. B_k is the union of the $(N-k)$-dimensional subspaces of equation $x_{i_1} = \ldots = x_{i_k} = 0$. Then every k-dimensional subspace of $PG(N, q)$ is generated by $k+1$ independent points in B_k.*

Theorem 5.2 *Let ρ be any positive integer. Let $q = (q')^{\rho+1}$. Let $N > \rho + 1$. Then in $PG(N, q)$ there exists a ρ -saturating set of size*

$$\frac{V_{q'}(N+1, N-\rho+1) - 1}{q' - 1} \sim \binom{N+1}{\rho} q^{\frac{N-\rho}{\rho+1}},\ \textit{where } V_{q'}(a, b) = \sum_{i=0}^{b} (q'-1)^i \binom{a}{i}.$$

For a parameter $\eta \in \{2, 3, \dots, \rho\}$ we take $N = \rho + \eta$. Then the length of the $[\overline{n}_{R,q,\eta}, \overline{n}_{R,q,\eta} - (R+\eta)]_q R$ code related to the ρ-saturating set of Theorem 5.2 is equal to

$$\overline{n}_{R,q,\eta} = \frac{\left(\sum_{i=0}^{\eta+1} (\sqrt[R]{q} - 1)^i \binom{R+\eta}{i}\right) - 1}{\sqrt[R]{q} - 1} \sim \binom{R+\eta}{R-1} q^{\frac{\eta}{R}}.$$

The code is an (R, ℓ)-object with $\ell \geq 3$, see [2, Section II] for definitions of (R, ℓ)-objects and (R, ℓ)-partitions. We use it as the starting code of the q^m-concatenating constructions of [2, Th. 3.1, Condition A2] with the trivial (R, ℓ) -partition.

Theorem 5.3 *Let $q = (q')^R$ and let $R \geq 4$. We fix the parameter $\eta \in \{2, 3, \dots, R-1\}$. Then there is an infinite family $\mathcal{A}_{R,q}^{(\eta)}$ of $[n, n-r]_q R$ codes with the following parameters*

$$\mathcal{A}_{R,q}^{(\eta)} : R \geq 4,\ r = Rt + \eta,\ q = (q')^R,\ n = \overline{n}_{R,q,\eta} q^{\frac{r-(R+\eta)}{R}} + (R-3) \frac{q^{\frac{r-(R+\eta)}{R}} - 1}{q-1},$$

$$t = 1 \text{ and } t \geq t_0,\ q^{t_0 - 1} \geq \overline{n}_{R,q,\eta}.$$

The main term of the asymptotic covering density $\overline{\mu}_q(R, \mathcal{A}_{R,q}^{(\eta)})$ is $\frac{(R+\eta)^{R^2-R}}{((R-1)!)^R R!}$, which does not depend of q.

References

[1] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein, *Covering Codes*, Amsterdam, The Netherlands: North-Holland, 1997.

[2] A. A. Davydov, Constructions and families of covering codes and saturated sets of points in projective geometry, *IEEE Trans. Inform. Theory* 41, 1995, 2071-2080.

[3] A. A. Davydov, Constructions and families of nonbinary linear codes with covering radius 2, *IEEE Trans. Inform. Theory* 45, 1999, 1679-1686.

[4] A. A. Davydov, S. Marcugini, F. Pambianco, Linear codes with covering radius 2, 3 and saturating sets in projective geometry, *IEEE Trans. Inform. Theory* 50, 2004, 537-541.

[5] A. A. Davydov, P. R. J. Östergård, Linear codes with covering radius $R = 2, 3$ and codimension tR, *IEEE Trans. Inform. Theory* 47, 2001, 416-421.

[6] A. A. Davydov, P. R. J. Östergård, On saturating sets in small projective geometries, *Europ. J. Combin.* 21, 2000 563-570.