Available online at www.sciencedirect.com

SciVerse ScienceDirect

Electronic Notes in Discrete Mathematics 40 (2013) 289–293

Electronic Notes in DISCRETE MATHEMATICS

www.elsevier.com/locate/endm

A note on multiple coverings of the farthest-off points

Fernanda Pambianco [a,1] Alexander A. Davydov [b,2]
Daniele Bartoli [a,1] Massimo Giulietti [a,1] Stefano Marcugini [a,1]

[a] *Dipartimento di Matematica e Informatica*
Università di Perugia
Perugia, Italy

[b] *Institute for Information Transmission Problems (Kharkevich institute)*
Russian Academy of Sciences
Moscow, Russia

Abstract

In this work we summarize some recent results, to be included in a forthcoming paper [1]. We define μ-density as a characteristic of quality for the kind of coverings codes called multiple coverings of the farthest-off points (MCF). A concept of multiple saturating sets ((ρ, μ)-saturating sets) in projective spaces $PG(N, q)$ is introduced. A fundamental relationship of these sets with MCF is showed. Bounds for the smallest possible cardinality of $(1, \mu)$-saturating sets are obtained. Constructions of small $(1, \mu)$-saturating sets improving the probabilistic bound are proposed.

Keywords: Multiple coverings, covering codes, farthest-off points, saturating sets

[1] Email: {fernanda,daniele.bartoli,giuliet,gino}@dmi.unipg.it
[2] Email: adav@iitp.ru

http://dx.doi.org/10.1016/j.endm.2013.05.051

1 Introduction

Let $(n, M, d)_q R$ be a code of length n, cardinality M, minimum distance d, covering radius R, over the Galois field $\mathbb{F}_q$. Let $[n, k, d]_q R$ be a q-ary linear code of length n, dimension k, minimum distance d, covering radius R. One may omit "d" if it is not relevant. Let $\mathbb{F}_q^n$ be the space of n-dimensional q-ary vectors.

Definition 1.1 i) [4] An $(n, M)_q R$ code C is said to be an (R, μ) *multiple covering of the farthest-off points* ((R, μ)-MCF for short) if for all $x \in \mathbb{F}_q^n$ such that $d(x, C) = R$ the number of codewords c with $d(x, c) = R$ is at least μ. Here $d(x, C)$ and $d(x, c)$ are the Hamming distances of x from C and c, respectively.

ii) Let an $(n, M)_q R$ code C be an (R, μ)-MCF. Let $\gamma(C, R)$ be the *average number* of spheres of radius R centered in words of C containing a fixed element in $\mathbb{F}_q^n$ with distance R from C. Define a μ-*density* $\delta_\mu(C, R)$ as follows:

$$\delta_\mu(C, R) = \frac{1}{\mu}\gamma(C, R) \geq 1.$$

Theorem 1.2 *Let an (R, μ)-MCF code C be a linear $[n, k, d(C)]_q R$ code. Denote by $A_w(C)$ the number of codewords of C of weight w. Then*

$$\delta_\mu(C, R) = \frac{\binom{n}{R}(q-1)^R - \binom{2R-1}{R-1} A_{2R-1}(C)}{\mu\left(q^{n-k} - \sum_{i=0}^{R-1}\binom{n}{i}(q-1)^i\right)} \text{ if } d(C) \geq 2R-1. \qquad (1)$$

Let $PG(N, q)$ be a projective space of dimension N over the field $\mathbb{F}_q$. For an introduction to ρ-saturating sets in $PG(N, q)$ and their connections with linear covering codes, see e.g. [5] and references therein.

Definition 1.3 Let $I = \{P_1, \ldots, P_n\}$ be a subset of points of $PG(N, q)$. Let $N \geq \rho \geq 1$, $\mu \geq 1$. Then I is said to be (ρ, μ)-saturating if:

(M1) I generates $PG(N, q)$;

(M2) there exists a point Q in $PG(N, q)$ which does not belong to any subspace of dimension $\rho - 1$ generated by the points of I;

(M3) for every point Q in $PG(N, q)$ not belonging to any subspace of dimension $\rho - 1$ generated by the points of I, the number of subspaces of dimension ρ generated by the points of I and containing Q is at least μ, counted with multiplicity. The multiplicity m_T of a subspace T is computed as the number of distinct sets of $\rho + 1$ independent points contained in $T \cap I$.

Lemma 1.4 *Let C be an $[n, k]_q R$ code. Consider every column of a parity check matrix of C as homogenous coordinates of a point of an n-set I in*

$PG(n-k-1,q)$. Then C is a (R,μ)-MCF if and only if I is $(R-1,\mu)$-saturating.

2 $(1,\mu)$-saturating sets and $(2,\mu)$-MCF codes

For $\rho = 1$, the conditions (M2),(M3) can be read as follows:

(M2) I is not the whole $PG(N,q)$;

(M3) for every point Q in $PG(N,q) \setminus I$ the number of secants of I from Q is at least μ, counted with multiplicity. The multiplicity m_ℓ of a secant ℓ is computed as $m_\ell = \binom{\#(\ell \cap I)}{2}$.

Definition 2.1 The μ-length function $\ell_\mu(2,r,q)$ is the smallest length n of a linear $(2,\mu)$-MCF code with parameters $[n,n-r,d]_q 2$, $d \geq 3$, or equivalently the smallest cardinality of a $(1,\mu)$-saturating set in $PG(r-1,q)$. For $\mu = 1$, we denote $\ell_\mu(2,r,q)$ as $\ell(2,r,q)$; it is the "usual" length function [4,5].

It is obvious that μ disjoint copies of a usual 1-saturating set in $PG(r-1,q)$ give rise to a $(1,\mu)$-saturating set in $PG(r-1,q)$. Therefore,

$$\ell_\mu(2,r,q) \leq \mu\ell(2,r,q). \tag{2}$$

Denote by $\delta_\mu(2,r,q)$ the minimum μ-density of a linear $(2,\mu)$-MCF code of codimension r over $\mathbb{F}_q$. Let $\delta(2,r,q)$ be the minimum covering density [4,5] of a linear code with covering radius 2 and codimension r over $\mathbb{F}_q$. By (1),(2),

$$\delta_\mu(2,r,q) \leq \frac{\frac{1}{2}(\mu\ell(2,r,q)-1)(q-1)}{\mu \cdot \left(\frac{\#PG(r-1,q)}{\mu\ell(2,r,q)} - 1\right)} \sim \mu\delta(2,r,q). \tag{3}$$

By (2),(3), estimates for $\ell_\mu(2,r,q)$ and $\delta_\mu(2,r,q)$ can be immediately obtained from the vast body of literature on 1-saturating sets in finite projective spaces. If q is not square, the best result in this direction is the existence of 1-saturating $\lfloor 5\sqrt{q \log q} \rfloor$-sets in $PG(2,q)$ which was shown by means of probabilistic methods, see [3] and references therein. Therefore,

$$\ell_\mu(2,3,q) \leq \mu\lfloor 5\sqrt{q \log q} \rfloor. \tag{4}$$

The *aim of the present paper* is to construct $(1,\mu)$-saturating sets in $PG(N,q)$ giving rise to $(2,\mu)$-MCF codes with μ-density smaller with respect to that derived from (3). Equivalently, it can be said that our goal is to obtain $(1,\mu)$-saturating sets in $PG(r-1,q)$ with cardinality smaller than $\mu\ell(2,r,q)$.

The exact values of $\ell(2,r,q)$ are known only for small q, see [2,5]. Therefore reformulating the foregoing, we can say that the *aim of the present paper* is to construct $(1,\mu)$-saturating sets in $PG(r-1,q)$ with cardinality smaller than $\mu\bar{\ell}(2,r,q)$ where $\bar{\ell}(2,r,q)$ is the smallest *known* length of a linear q-ary code with covering radius 2 and codimension r.

Theorem 2.2 *The following lower bound on the μ-length function holds:*

$$\ell_\mu(2,3,q) \geq \sqrt{2\mu q}.$$

3 Constructions of small $(1,\mu)$-saturating sets in $PG(2,q)$

The constructions of this section essentially use the ideas and results of [6].

Let $q = p^\ell$ with p prime, and let H be an additive subgroup of $\mathbb{F}_q$. Let

$$L_H(X) = \prod_{h\in H}(X-h) \in \mathbb{F}_q[X]. \tag{5}$$

Assume that the size of H is p^s with $2s < \ell$. Let

$$\mathcal{M}_H := \left\{ \left(\frac{L_{H_1}(\beta_1)}{L_{H_2}(\beta_2)} \right)^p \mid H_1, H_2 \text{ subgroups of } H \text{ of size } p^{s-1},\ \beta_i \in H \setminus H_i \right\}. \tag{6}$$

Theorem 3.1 *Let $q = p^\ell$, and let H be any additive subgroup of $\mathbb{F}_q$ of size p^s, with $2s < \ell$. Let μ be any integer with $1 \leq \mu \leq p^{2\ell-s}$, and let $\tau_1, \tau_2, \ldots, \tau_\mu$ be a set of distinct non-zero elements in $\mathbb{F}_q$. Let $L_H(X)$ be as in (5), and $\mathcal{M}_H$ be as in (6). Then the set*

$$D = \{(L_H(a):1:1), (L_H(a):0:1) \mid a \in \mathbb{F}_q\} \cup \{(\tau_i : m : 1) \mid m \in \mathcal{M}_H, \\ i = 1,\ldots,\mu\} \cup \{(1:\tau_i:0) \mid i = 1,\ldots,\mu\} \cup \{(1:0:0)\}$$

is a $(1,\mu)$-saturating set of size at most

$$\frac{2q}{p^s} + \mu\frac{(p^s-1)^2}{p-1} + \mu.$$

The order of magnitude of the size of D of Theorem 3.1 is p^a where $a = \max\{\ell - s, \log_p \mu \cdot (2s-1)\}$. If s is chosen as $\lceil \ell/3 \rceil$, then the size of D satisfies

$$\#D \leq \begin{cases} 2q^{\frac{2}{3}} + \mu + \mu\frac{q^{\frac{2}{3}} - 2q^{\frac{1}{3}} + 1}{p-1}, & \text{if } \ell \equiv 0 \pmod 3 \\ 2\left(\frac{q}{p}\right)^{\frac{2}{3}} + \mu + \mu\frac{p^2\left(\frac{q}{p}\right)^{\frac{2}{3}} - 2p\left(\frac{q}{p}\right)^{\frac{1}{3}} + 1}{p-1}, & \text{if } \ell \equiv 1 \pmod 3 \\ 2\frac{1}{p}(qp)^{\frac{2}{3}} + \mu + \mu\frac{(qp)^{\frac{2}{3}} - 2(qp)^{\frac{1}{3}} + 1}{p-1}, & \text{if } \ell \equiv 2 \pmod 3 \end{cases} \cdot$$

Theorem 3.2 *Let $q = p^\ell$, with ℓ odd. Let $1 \leq \mu \leq p$, and let H be any additive subgroup of $\mathbb{F}_q$ of size p^s, with $2s+1 = \ell$. Let $L_H(X)$ be as in (5), and $\mathcal{M}_H$ be as in (6). Then for any integer $v \geq 1$ there exists a $(1,\mu)$-saturating set T in $PG(2,q)$ such that*

$$\#T \leq (v+1)p^{s+1} + \mu\frac{\#\mathcal{M}_H^v}{(q-1)^{v-1}} + 1 + \mu.$$

Corollary 3.3 *Let $q = p^{2s+1}$, and let $1 \leq \mu \leq p$. Then there exists a $(1,\mu)$-saturating set in $PG(2,q)$ of size less than or equal to*

$$n_\mu(s,p,v) = \min_{v=1,\dots,2s+1}\left\{(v+1)p^{s+1} + \mu\frac{(p^s-1)^{2v}}{(p-1)^v(p^{(2s+1)}-1)^{(v-1)}} + 1 + \mu\right\}. \quad (7)$$

Several triples (s,p,v) such that $n_1(s,p,v) < 5\sqrt{q\log q}$ are given in [6, Table 1]. For the corresponding $q = p^{2s+1}$, these values of $n_1(s,p,v)$ are the smallest known cardinalities $\overline{\ell}(2,3,q)$ of 1-saturating sets in $PG(2,q)$, see [5, Section 4.4]. Moreover, for $\mu \geq 2$, by (7) it holds that $n_\mu(s,p,v) < \mu n_1(s,p,v)$. Thus, in the cases provided by the triples (s,p,v), the goal formulated in Section 2 is achieved. Other general constructions and classification results of $(1,\mu)$-saturating sets are given in [1].

References

[1] D. Bartoli, A. A. Davydov, M. Giulietti, S. Marcugini, and F. Pambianco, Multiple coverigns of the farthest-off points with small density from projective geometry, *preprint.*

[2] D. Bartoli, S. Marcugini, A. Milani and F. Pambianco, On the minimum size of complete arcs and minimal saturating sets in $PG(2,q)$, q small, *preprint.*

[3] Boros, E., T. Szőnyi and K. Tichler, *On defining sets for projective planes*, Discrete Math. **303** (2005) 17–31.

[4] Cohen, G., I. Honkala, S. Litsyn and A. Lobstein, "Covering Codes", North-Holland, Amsterdam, 1997.

[5] Davydov, A. A., M. Giulietti, S. Marcugini and F. Pambianco, *Linear nonbinary covering codes and saturating sets in projective spaces*, Adv. Math. Commun. **5** (2011) 119–147.

[6] Giulietti, M., *On small dense sets in Galois planes*, Electron. J. Combin. **14** (2007) R-75.