Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 53–59*

Multiple coverings of the farthest-off points and multiple saturating sets in projective spaces

Daniele Bartoli daniele.bartoli@dmi.unipg.it
Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, Perugia, 06123, Italy
Alexander A. Davydov adav@iitp.ru
Institute for Information Transmission Problems, Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, Moscow, 127994, Russian Federation
Massimo Giulietti, Stefano Marcugini, Fernanda Pambianco
{giuliet,gino,fernanda}@dmi.unipg.it
Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, Perugia, 06123, Italy

Abstract. For the kind of coverings codes called multiple coverings of the farthest-off points (MCF) we define μ-density as a characteristic of quality. 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 codes is showed. Lower and upper bounds for the smallest possible cardinality of $(1,\mu)$-saturating sets are obtained. In $PG(2,q)$, constructions of small $(1,\mu)$-saturating sets improving the probabilistic bound are proposed. A number of results on the spectrum of sizes of minimal $(1,\mu)$-saturating sets are obtained.

1 Introduction

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

Definition 1. [4, 7, 8] *An $(n,M)_qR$ 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 such that $d(x,c)=R$ is at least μ.*

In the literature, MCF codes are called also multiple coverings of deep holes [4].

Let $V_q(n,R)$ be the size of a sphere or radius R in $\mathbb{F}_q^n$. Recall that

$$V_q(n,R) \;=\; \sum_{i=0}^{R}\binom{n}{i}(q-1)^i.$$

For an $(n, M, d(C))_q R$ code C we denote by $N_R(C)$ the number of words of $\mathbb{F}_q^n$ with distance R from C and by $\gamma(C, R)$ 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. We have

$$\begin{aligned} N_R(C) &= q^n - M \cdot V_q(n, R-1) \text{ if } d(C) \geq 2R-1, \\ N_R(C) &> q^n - M \cdot V_q(n, R-1) \text{ if } d(C) < 2R-1, \\ \gamma(C, R) &= \frac{M \cdot \binom{n}{R} \cdot (q-1)^R}{N_R(C)}. \end{aligned}$$

Definition 2. *Let an $(n, M)_q R$ code C be an (R, μ)-MCF. We define the μ-*density *$\delta_\mu(C, R)$ as follows:*

$$\delta_\mu(C, R) := \frac{\gamma(C, R)}{\mu} = \frac{M \cdot \binom{n}{R} \cdot (q-1)^R}{\mu N_R(C)} \geq 1. \tag{1}$$

If C is a linear $[n, k, d(C)]_q R$ code with $d(C) \geq 2R-1$, then

$$\delta_\mu(C, R) = \frac{\binom{n}{R} \cdot (q-1)^R}{\mu \cdot (q^{n-k} - V_q(n, R-1))}. \tag{2}$$

From now, throughout the paper we consider only *linear* $[n, k, d]_q R$ codes with $d \geq 3$.

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.

We introduce a concept of *multiple saturating sets.*

Definition 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) *every point Q in $PG(N, q)$ not belonging to any subspace of dimension $\rho - 1$ generated by the points of I, is such that the number of subspace 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 $T \cap I$.*

A $(\rho, 1)$-saturating set is a "usual" ρ-saturating set [5].

Definition 4. *An $[n,k]_qR$ code with $R=\rho+1$* ***corresponds*** *to a (ρ,μ)-saturating n-set I in $PG(n-k-1,q)$ if every column of a parity check matrix of the code can be represented as a point of I.*

Note that if any $\rho+1$ points of the set I of Definition 3 are linearly independent (i.e. the corresponding code has minimum distance $d \geq \rho+2$) then the multiplicity m_T of a subspace T is $m_T = \binom{\#(T\cap I)}{\rho+1}$.

Lemma 1. *A linear $[n,k]_qR$ code corresponding to a (ρ,μ)-saturating n-set in $PG(n-k-1,q)$ is a $(\rho+1,\mu)$-MCF code.*

The basic Lemma 1 allows us to consider (ρ,μ)-saturating sets as a linear $(\rho+1,\mu)$-MCF codes and vice versa.

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

Let a linear $[n,n-N-1,d(C)]_q2$ code C with $d(C)\geq 3$ be $(2,\mu)$-MCF. Then relation (2) for μ-density can be written as

$$\delta_\mu(C,2) = \frac{\binom{n}{2}(q-1)^2}{\mu\cdot(q^{N+1}-1-n(q-1))} = \frac{\frac{1}{2}(n-1)(q-1)}{\mu\cdot(\frac{\#PG(N,q)}{n}-1)}. \quad (3)$$

By (3), if q,N,μ are fixed, then the best density is achieved for small n.

Definition 5. *The μ-length function $\ell_\mu(2,r,q)$ is the smallest length n of a linear $(2,\mu)$-MCF code with parameters $[n,n-r,d]_q2$, $d\geq 3$, 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 an usual 1-saturating set in $PG(r-1,q)$ give rise to a $(1,\mu)$-saturating set in $PG(r-1,q)$. Therefore,

$$\ell_\mu(2,r,q) \leq \mu\ell(2,r,q). \quad (4)$$

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 density of a linear code with covering radius 2 and codimension r over $\mathbb{F}_q$. By (3),(4),

$$\delta_\mu(2,r,q) \leq \frac{\frac{1}{2}(\mu\ell(2,r,q)-1)(q-1)}{\mu\cdot(\frac{\#PG(r-1,q)}{\mu\ell(2,r,q)}-1)} \sim \mu\delta(2,r,q). \quad (5)$$

By (4),(5), 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. 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,

$$\ell_\mu(2,3,q) \leq \mu\lfloor 5\sqrt{q\log q}\rfloor. \tag{6}$$

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 (5). 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 $\ell(2,r,q)$ (and hence exact values of $\delta(2,r,q)$) are known only for small q, see [2], [5, Tables 1,3]. Therefore the smallest *known* length $\overline{\ell}(2,r,q)$ of a linear q-ary code with covering radius 2 and codimension r (or equivalently the smallest cardinality of a 1-saturating set in $PG(r-1,q)$) is interesting for comparison. Slightly 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 $\mu\overline{\ell}(2,r,q)$.

Theorem 1. *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 $PG(2,q)$

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 $\mathbb{F}_q$. Also, let

$$L_H(X) = \prod_{h\in H}(X-h) \in \mathbb{F}_q[X]. \tag{7}$$

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

$$\mathcal{M}_H := \left\{ \left(\frac{L_{H_1}(\beta_1)}{L_{H_2}(\beta_2)}\right)^p \mid H_1, H_2 \text{ subgroups of } H \text{ of size } p^{s-1},\ \beta_i \in H\setminus H_i \right\}. \tag{8}$$

Theorem 2. *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 (7), and $\mathcal{M}_H$ be as in (8). 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 2 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

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

Theorem 3. *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 (7), and $\mathcal{M}_H$ be as in (8). Then for any integer $v \geq 1$ there exists a $(1,\mu)$-saturating set T in $PG(2,q)$ such that*

$$\#T \leq (v+1)p^{s+1} + \mu\frac{\#\mathcal{M}_H^v}{(q-1)^{v-1}} + 1 + \mu. \tag{9}$$

Corollary 1. *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*

$$n_\mu(s,p,v) = \min_{v=1,\dots,2s+1}\left\{(v+1)p^{s+1} + \mu\frac{(p^s-1)^{2v}}{(p-1)^v(p^{(2s+1)}-1)^{(v-1)}} + 1 + \mu\right\}. \tag{10}$$

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 $\bar{\ell}(2,3,q)$ of 1-saturating sets in $PG(2,q)$, see [5, Section 4.4]. Moreover, for $\mu \geq 2$, by (10), 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.

4 Minimal $(1,\mu)$-saturating sets

Definition 6. *A (ρ,μ)-saturating n-set in $PG(N,q)$ is* minimal *if it does not contain any (ρ,μ)-saturating $(n-1)$-set of $PG(N,q)$.*

Denote by $m_\mu(\rho+1, N+1, q)$ the maximal size of a minimal (ρ,μ)-saturating set in $PG(N,q)$.

Theorem 4. *Let $q > 2$, $q^2 > \mu$. Then $m_\mu(2,3,q) \leq (q+\mu+1)$. In particular, $m_2(2,3,q) = q+3$.*

Constructions.

• Let $q = p^h$, $h \geq 1$, p prime. In $PG(2,q)$, let A be a point $(q+3)$-set containing a whole line ℓ and two points P_1, P_2 outside of ℓ, i.e. $A = \ell \cup \{P_1, P_2\}$.

• Let $q \geq 4$. In $PG(2,q)$, let B be a point $(q+2)$-set containing a line ℓ without two points P, Q and three non-collinear points R, S, T outside of ℓ such that P, R, S and Q, R, T are collinear. So, $B = (\ell \setminus \{P, Q\}) \cup \{R, S, T\}$.

• Let $q \geq 4$. In $PG(2,q)$, let C be a point $(q+2)$-set constructed similar to the set B above except that the points P, R, S, T are collinear.

Theorem 5. *In $PG(2,q)$, the sets A, B, C of constructions above are minimal $(1,2)$-saturating. Also, the stabilizer of the set A in $P\Gamma L(3,q)$ has size $hp(p-1)$.*

By computer search and by constructions we obtained Table 1.

Table 1. The number of nonequivalent minimal (1,2)-saturating n-sets in $PG(2,q)$ and the spectrum of sizes n

q	$\bar{\ell}(2,3,q)$	$\lceil 2\sqrt{q} \rceil$	$m_2(2,3,q)$	Spectrum of n
3	4^1.	4	6	6^4 . $*$
4	5^1.	4	7	$6^2 7^5$. $*$
5	6^6.	5	8	$6^1 7^4 8^{18}$. $*$
7	6^3.	6	10	$8^{13} 9^{564} 10^{424}$. $*$
8	6^1.	6	11	$8^2 9^{154} 10^{3372} 11^{611}$. $*$
9	6^1.	6	12	$8^1 9^{57} 10^{12145} 11^{76749} 12^{3049}$. $*$
11	7^1.	7	14	$10^{1348}[11-14]$.
13	8^2.	8	16	$10^2 11^{50794}[12-16]$.
16	9^4.	8	19	$11^{52}[12-19]$.
17	10^{3640}.	9	20	$[12-20]$.
19	10^{36} .	9	22	$[13-22]$
23	10^1.	10	26	$[15-26]$
25	12	10	28	$[17-28]$
27	12	11	30	$[17-30]$
29	13	11	32	$[19-32]$
31	14	12	34	$[19, 21-34]$
32	13	12	35	$[20-35]$
37	15	13	38	$[23, 26-40]$
41	16	13	44	$[25, 29-44]$
43	16	14	46	$[25, 30-46]$
47	18	14	50	$[27, 34-50]$
49	18	14	52	$[29, 34-52]$

In the 2-nd column of Table 1, the values $\bar{\ell}(2,3,q)$ of the smallest cardinality of a 1-saturating set in $PG(2,q)$, taken from [2, 5], are given. The cases when $\ell(2,3,q) = \bar{\ell}(2,3,q)$ are marked by the dot ".". In the 5-th column, we give some values of n for which minimal $(1,2)$-saturating n-sets in $PG(2,q)$ exist.

For $3 \leq q \leq 17$, we have found the *complete spectrum* of sizes n. This situation is marked by the dot "**.**". In the 2-nd and the 5-th columns, the superscript notes the numbers of nonequivalent sets of the corresponding size. For $3 \leq q \leq 9$, we obtain the *complete classification* of the spectrum of sizes n of minimal $(1,2)$-saturating n-sets in $PG(2,q)$. This situation is marked by the asterisk *.

By some constructions, considering several points on a conic, we obtained (1,2)-saturating n-sets in $PG(2,q)$, with sizes described in Table 2.

Table 2. Sizes small (1,2)-saturating n-sets in $PG(2,q)$

q	53	59	61	67	71	73	79	81	83	89	97	101	103	107	109	113	125	127	131	139
n	31	33	35	37	39	41	39	45	45	49	53	55	55	57	59	61	67	67	69	73

The smallest cardinalities of $(1,2)$-saturating sets for each q in Table 1 and sizes n in Table 2 are smaller than $2\bar{\ell}(2,3,q)$. So, for $\mu = 2$, $r = 3$, q from Tables 1 and 2, the goal formulated in Section 2 is achieved (as well as for $2 \leq \mu \leq p$, $r = 3$, $q = p^{2s+1}$ with the special values of s, p mentioned after Corollary 1).

References

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

[2] D. Bartoli, G. Faina, S. Marcugini, and F. Pambianco, Classification of minimal 1-saturating sets in $PG(2,q)$, $q \leq 23$, in *Proc. XIII Int. Workshop on Algebraic and Combin. Coding Theory, ACCT2012, Pomorie, Bulgaria, 2012*, to appear.

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

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

[5] A. A. Davydov, M. Giulietti, S. Marcugini, and F. Pambianco, Linear non-binary covering codes and saturating sets in projective spaces, *Advances Math. Commun.* **5**, 119–147, 2011.

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

[7] H. Hämäläinen, I. Honkala, S. Litsyn, and P. Östergård, Football pools – a game for mathematicians, *Amer. Math. Monthly*, **102**, 579–588, 1995.

[8] H. O. Hämäläinen, I. S. Honkala, S. N. Litsyn, and P. R.J. Östergård, Bounds for binary codes that are multiple coverings of the farthest-off points, *SIAM J. Discrete Math.* **8**, 196–207, 1995.