Linear Codes With Covering Radius 2, 3 and Saturating Sets in Projective Geometry

Alexander A. Davydov, Stefano Marcugini, and Fernanda Pambianco

***Abstract*—Infinite families of linear codes with covering radius $R = 2$, 3 and codimension $tR + 1$ are constructed on the base of starting codes with codimension 3 and 4. Parity-check matrices of the starting codes are treated as saturating sets in projective geometry that are obtained by computer search using projective properties of objects. Upper bounds on the length function and on the smallest sizes of saturating sets are given.**

***Index Terms*—Covering codes, covering density, covering radius, saturating sets in projective geometry.**

I. Introduction

We consider covering codes, saturating sets in the projective geometry, and connections between these objects.

Let F_q be the Galois field of q elements. A q-ary linear code with codimension r has *covering radius* R if every r-positional q-ary column is equal to a linear combination of R columns of a parity-check matrix of this code and R is the smallest value with such property. For an introduction to coverings of vector spaces over finite fields and to the concept of code covering radius, see [3].

Let $\mathrm{PG}(v, q)$ be the v-dimensional projective space over F_q. For an introduction to such spaces and the geometrical objects therein, see [14], [15]. We say that a set of points $S \subseteq \mathrm{PG}(v, q)$ is ϱ *-saturating* if for any point $x \in \mathrm{PG}(v, q)$ there exist $\varrho + 1$ points in S generating a subspace of $\mathrm{PG}(v, q)$ in which x lies and ϱ is the smallest value with such property, cf. [4, Definition 1.1], [8], [11]. In [2], saturating sets are called "R-spanning sets."

A ϱ-saturating set of n points is called minimal if it does not contain a ϱ-saturating set of $n - 1$ points [8].

Denote by $[n, n-r]_q R$ a q-ary linear code of length n, codimension r, and covering radius R. An $[n, n-r]_q R$ code with minimum distance d is denoted by $[n, n - r, d]_q R$. The points of a ϱ-saturating n-set in $\mathrm{PG}(r-1, q)$ can be considered as r-dimensional columns of a parity-check matrix of an $[n, n-r]_q R$ code with $R = \varrho + 1$[2], [4], [8], [11].

This work is devoted to infinite families of codes with covering radius $R = 2, 3$ and codimension $r = Rt + 1$. The families are constructed on the base of "short" $[n, n - 3]_q 2$ and $[n, n - 4]_q 3$ codes which are used as starting codes in q^m-concatenating constructions. To get these codes, we obtain "small" 1-saturating sets in $\mathrm{PG}(2, q)$ and 2-saturating sets in $\mathrm{PG}(3, q)$ and then we treat them as parity-check matrices of the needed short codes. Saturating sets are obtained by computer search using their geometrical properties. We apply computer results of [8], [11] and new ones obtained in this work.

The q^m-concatenating constructions [3]–[5], [10], [13] take a code of covering radius R with small codimension as a starting code and produce an infinite family of codes with the same covering radius and with almost the same covering density. A parity-check matrix of a starting code is repeated q^m times in a parity-check matrix of a new code.

The length function $l(r, R; q)$ is the smallest length of an $[n, n - r]_q R$ code [2]. Tables of upper bounds on $l(r, 2; q)$, $r \leq 24$, are published in [10] for $q = 3, 5$, in [12] for $q = 4$, in [13] for $q = 7$. Tables of upper bounds on $l(r, 3; 3)$, $r \leq 24$, are given in [4], see also [1].

For $R = 2$, $q \geq 8$ and $R = 3$, $q \geq 4$, a number of general results are described in [4], [5], [13]. Good infinite code families with $R = 2$, $r = 2t + 1$, $q = p^2$, and $R = 2, 3$, $r = tR$, $q \geq 7$, are given in [5], [13]. But results with relatively good parameters for $R = 2$, $q \geq 8$, $q \neq p^2$, and $R = 3$, $q \geq 4$, with $r = tR + 1$ have not been obtained yet (in general, the case $r = tR + 1$ is harder than tR). This work in part fills this gap for some ranges of q. We obtained infinite families of $[n, n-(2t+1)]_q 2$ codes for $7 \leq q \leq 859$, $q = 907, 1009, 1109, 1163$, and $[n, n - (3t + 1)]_q 3$ codes for $4 \leq q \leq 343$, $q = 401, 499$, and $q = p^3$. When code length tends to infinity, covering density of new families is bounded from above by constants. New families with $R = 2$ have code length and covering density smaller than known ones. For $R = 3$, $r = 3t + 1$, we do not know corresponding families described in the literature. Finally, the new code families can be treated as infinite families of saturating sets.

Denote by $k(v, q, \varrho)$ the smallest possible size of a ϱ-saturating set in the geometry $\mathrm{PG}(v, q)$. Obviously, $l(r, R; q) = k(r-1, q, R-1)$. Small saturating sets described in this work give upper bounds on $k(2, q, 1)$, $k(3, q, 2)$, and, therefore, on $l(3, 2; q)$, $l(4, 3; q)$.

A linear code with $R \leq d - 2$ can be called nonlengthening since one cannot add any column to a parity-check matrix without reducing the code distance d. Nonlengthening $[n, n-3, 4]_q 2$ quasi-perfect minimum-distance separable (MDS) [3] codes correspond to complete arcs in $\mathrm{PG}(2, q)$, their short variants have been widely studied [7], [14], [15]. Nonlengthening $[n, n - 4, 5]_q 3$ quasi-perfect MDS codes correspond to complete arcs in $\mathrm{PG}(3, q)$ [15]. But our knowledge on short $[n, n - 4, 5]_q 3$ codes or on small complete arcs in $\mathrm{PG}(3, q)$ is insufficient [15]. In the process of finding small 2-saturating sets we obtained small complete arcs (i.e., short $[n, n - 4, 5]_q 3$ MDS codes) for all spaces $\mathrm{PG}(3, q)$ considered in this correspondence. For $q \leq 9$, we showed by computer that these arcs and codes have the smallest possible sizes.

In Section II, upper bounds on $k(2, q, 1) = l(3, 2; q)$ are given. With the use of these bounds, infinite families of $[n, n-(2t+1)]_q 2$ codes are constructed. In Section III, upper bounds on $k(3, q, 2) = l(4, 3; q)$ are obtained. In Section IV, a q^m-concatenating construction is described and infinite families of $[n, n - (3t + 1)]_q 3$ codes are formed on the basis of this construction and the bounds of Section III. The Appendix gives the classification of some minimal 2-saturating sets in $\mathrm{PG}(3, q)$. The classification is obtained in the process of forming the required saturating sets and has independent importance.

II. Families of Codes With Covering Radius 2 and Codimension $2t + 1$

At first, we consider small 1-saturating sets in $\mathrm{PG}(2, q)$. Let $\overline{l}(r, R; q)$ and $\overline{k}(v, q, \varrho)$ be the *smallest known* values of $l(r, R; q)$ and $k(v, q, \varrho)$. Evidently, $\overline{l}(r, R; q) = \overline{k}(r - 1, q, R - 1)$. Values of $\overline{k}(2, q, 1)$ for $3 \leq q \leq 587$ are given in [8, Tables 1, 4]. For $593 \leq q \leq 809$, we can consider the table in [7] with the smallest known sizes of complete arcs in $\mathrm{PG}(2, q)$ as such arcs are minimal 1-saturating sets [8]. In this work, for $593 \leq q \leq 859$, $q = 907, 1009, 1109, 1163$, by computer search [6] we obtained minimal 1-saturating sets with smaller sizes than arcs of [7]. So, sets of [6] for $q \geq 593$ give values of $\overline{k}(2, q, 1) = \overline{l}(3, 2; q)$, see Table I.

Manuscript received December 26, 2002; revised July 13, 2003. A part of this work was carried out while A. A. Davydov was twice visiting the University of Perugia.

A. A. Davydov is with the Institute for Information Transmission Problems, Russian Academy of Sciences, GSP-4, Moscow 127994, Russia (e-mail: adav@iitp.ru).

S. Marcugini and F. Pambianco are with the Department of Mathematics and Informatics, Perugia University, Perugia 06123, Italy (e-mail: gino@dipmat.unipg.it; fernanda@dipmat.unipg.it).

Communicated by S. Litsyn, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2004.825503

TABLE I
NEW UPPER BOUNDS $\overline{l} = \overline{l}(3,2;q)$ ON THE LENGTH FUNCTION $l(3,2;q)$ FOR $q \geq 593$

q	$\overline{l}$	q	$\overline{l}$	q	$\overline{l}$	q	$\overline{l}$	q	$\overline{l}$
593	90	643	95	709	101	769	106	839	111
599	91	647	95	719	102	773	106	853	113
601	91	653	96	727	102	787	107	857	113
607	91	659	96	729	80	797	108	859	113
613	92	661	96	733	102	809	109	907	117
617	92	673	98	739	103	811	110	1009	124
619	92	677	98	743	104	821	110	1109	132
625	74	683	99	751	105	823	110	1163	135
631	94	691	99	757	105	827	110		
641	95	701	100	761	105	829	110		

For $q = p^2$, we apply [4, Theorem 5.2]. In [6] randomized greedy algorithms [7], [8] are used.

Using [8, Tables 1, 4] and Table I of this work, one can obtain (counting $3\sqrt{q}$ and $4\sqrt{q}$) the following result.

Theorem 1: Let $Q_2 = \{907, 1009, 1109, 1163\}$. For $l(3,2;q) = k(2,q,1)$ it holds that

$$l(3,2;q) \leq a_q\sqrt{q}, \quad \begin{array}{ll} a_q < 3, & \text{if } 2 \leq q \leq 109 \\ a_q < 4, & \text{if } 113 \leq q \leq 859,\ q \in Q_2. \end{array} \quad (1)$$

In [5, Example 6] under the condition that there exists a starting $[n_q, n_q - 3]_q 2$ code with $n_q < q$, an infinite family of $[n, n-r]_q 2$ codes is designed with parameters

$$\begin{array}{l} R = 2, \quad r = 2t-1, \quad t = 4, 6 \text{ and } t \geq 8, \quad n_q < q \\ n = n_q q^{t-2} + 2q^{t-3}, \qquad \text{if } 2n_q \leq q+1 \\ n = n_q q^{t-2} + 2q^{t-3} + q^{t-4}, \qquad \text{if } 2n_q > q+1. \end{array} \quad (2)$$

By [8, Tables 1, 4] and Table I, there are $[n_{q,2}, n_{q,2} - 3]_q 2$ codes $\mathcal{W}_q$ where $n_{q,2} = \overline{l}(3,2;q) = a_q\sqrt{q} < q$, the estimates of a_q are given by (1), $2n_{q,2} \leq q+1$ if $19 \leq q \leq 859$, $q \in Q_2$, $2n_{q,2} > q+1$ if $7 \leq q \leq 17$. So, we may use results of (2) taking $\mathcal{W}_q$ as the starting codes. We change $r = 2t-1$ by $r = 2t+1$ and obtain the infinite families $\mathcal{A}_1$, $\mathcal{A}_2$ of $[n, n-r]_q 2$ codes with parameters

$$R = 2, \ \ r = 2t+1, \ \ t = 3, 5 \text{ and } t \geq 7, \ \ n_{q,2} = a_q\sqrt{q} < q$$

$$\mathcal{A}_1 \colon n = n_{q,2} q^{t-1} + 2q^{t-2}, \ \ 19 \leq q \leq 859 \text{ and } q \in Q_2 \quad (3)$$

$$\mathcal{A}_2 \colon n = n_{q,2} q^{t-1} + 2q^{t-2} + q^{t-3}, \ \ 7 \leq q \leq 17. \quad (4)$$

Let

$$\mu_q(n, R, C) = \sum_{i=0}^{R} (q-1)^i \binom{n}{i} \Big/ q^{r(C)}$$

be the covering density of an $[n, n-r(C)]_q R$ code C. For an infinite family $\mathcal{A}_j$ consisting of $[n, n-r(\mathcal{A}_{j,n})]_q R$ codes $\mathcal{A}_{j,n}$ we consider the value

$$\overline{\mu}_q(R, \mathcal{A}_j) = \limsup_{n \to \infty} \mu_q(n, R, \mathcal{A}_{j,n}).$$

In $\overline{\mu}_q(R, \mathcal{A}_j)$ one may omit $\mathcal{A}_j$.

By (1), (3), and (4), we can obtain the estimates $\overline{\mu}_q(2, \mathcal{A}_j) < n_{q,2}^2/2q = a_q^2/2$, $j = 1, 2$, i.e.,

$$\begin{array}{ll} \overline{\mu}_q(2, \mathcal{A}_1) \approx \overline{\mu}_q(2, \mathcal{A}_2) < 4.5, & \text{if } 7 \leq q \leq 109 \\ \overline{\mu}_q(2, \mathcal{A}_1) < 8, & \text{if } 113 \leq q \leq 859, \quad q \in Q_2. \end{array}$$

So, in the infinite families $\mathcal{A}_1$, $\mathcal{A}_2$ with $7 \leq q \leq 859$, $q \in Q_2$, the covering density is bounded from above by constants, e.g., $\overline{\mu}_{593}(2, \mathcal{A}_1) \approx 6.8$, $\overline{\mu}_{701}(2, \mathcal{A}_1) \approx 7.1$.

In [5, Example 6] for $q \neq p^2$, the densities

$$\overline{\mu}_q(2) \approx (q + 4 + 6q^{-1} - 11q^{-3})/8$$

for q odd, and

$$\overline{\mu}_q(2) \approx (q + 6 + 9q^{-1} - 4q^{-2})/8$$

for q even, are given. Densities from [5] depend on q and are essentially greater than those in this work, e.g., by [5], $\overline{\mu}_{593}(2) \approx 74$, $\overline{\mu}_{701}(2) \approx 88$.

III. SMALL 2-SATURATING SETS IN PG$(3,q)$ AND STARTING CODES WITH $R = 3$

An n-arc in a space PG$(3,q)$ is a set of n points, no four of which are coplanar [15]. An n-arc is called complete if it is not contained in an $(n+1)$-arc. A complete arc in PG$(3,q)$ is a minimal 2-saturating set [8]. A cap is a set of points, no three of which are collinear [14], [15]. We call a set of type C a 2-saturating set in PG$(3,q)$ that is a cap but not an arc since it contains four coplanar points. Finally, we call a *usual set* a 2-saturating set in PG$(3,q)$ that is neither a cap nor an arc since it contains three collinear points.

So, to find small 2-saturating sets in PG$(3,q)$ we should research three directions: complete arcs, sets of type C, and usual sets. Points of a 2-saturating set in PG$(3,q)$ treated as four-dimensional columns form a parity-check matrix of an $[n, n-4, 3]_q 3$ code for a usual set, an $[n, n-4, 4]_q 3$ code for a set of type C, and an $[n, n-4, 5]_q 3$ quasi-perfect MDS code for a complete arc.

Let $t(3,q)$ be the smallest size of a complete arc in PG$(3,q)$. Denote by $n(4,q)$ the smallest length of a nonlengthening $[n, n-4, 5]_q 3$ MDS code, see Introduction. Let $\overline{t}(3,q)$ and $\overline{n}(4,q)$ be the *smallest known* values of $t(3,q)$ and $n(4,q)$. Obviously, $t(3,q) = n(4,q)$, and

$$l(4,3;q) = k(3,q,2) \leq t(3,q) = n(4,q) \leq \overline{t}(3,q) = \overline{n}(4,q).$$

In [11] for $q \leq 16$, a table of $\overline{k}(3,q,2)$ is given without notes on the corresponding code distances. Therefore, we performed a computer search [9] by the three directions mentioned for $2 \leq q \leq 59$. We again applied randomized greedy algorithms, see [7], [8]. Besides, other approaches close to [7], [8], [17] were used. For small q, exhaustive algorithms based on backtracking have been applied. To reduce the search space, equivalence properties among sets of points of PG$(3,q)$ have been exploited. To find interesting examples for greater values of q we used a backtracking algorithm that works with sets of points of PG$(3,q)$ consisting of orbits of special subgroups of the collineation group $P\Gamma L(4,q)$.

The results of computer search of [9] for $q \leq 59$ are summarized in Table II. Besides, some results having independent importance are given in the Appendix. In Table II, we denote $\overline{t} = \overline{t}(3,q)$, $\overline{l} = \overline{l}(4,3;q)$. Subscripts indicate the minimum distance d of corresponding $[\overline{l}(4,3;q), \overline{l}(4,3;q) - 4, d]_q 3$ codes. Entries "$3,4,5$," "$3,4$," "$4,5$" mean that distinct types of 2-saturating sets give the same result. The point indicates the exact bounds with $l(4,3;q) = \overline{l}(4,3;q)$ or $t(3,q) = \overline{t}(3,q)$. Bounds with $l(4,3;q) = \overline{l}(4,3;q)$ are known by [16], quoted in [11], and confirmed by exhaustive computer search in this work [9], see the Appendix. Bounds with $t(3,q) = \overline{t}(3,q)$ are obtained in this work, again see the Appendix.

Let $Q_3 = \{401, 499\}$. For $61 \leq q \leq 343$, $q \in Q_3$, a computer search is executed in [9] only for complete arcs to save computer time. In this case, $\overline{t}(3,q) = \overline{l}(4,3;q)$. The results are summarized in Table III where $\overline{l} = \overline{l}(4,3;q) = \overline{t}(3,q)$ and all code distances $d = 5$. Note that all 2-saturating sets used for determining values in Tables II and III are minimal.

Using Tables II and III one can obtain (counting $4\sqrt[3]{q}$ and $5\sqrt[3]{q}$) the following.

TABLE II
UPPER BOUNDS $\bar{l} = \bar{l}(4,3;q)$ ON THE LENGTH FUNCTION $l(4,3;q)$ FOR $q \le 59$

q	$\bar{l}$	$\bar{t}$	q	$\bar{l}$	$\bar{t}$	q	$\bar{l}$	$\bar{t}$
2	$5_{3,4}$.		16	$9_{3,4,5}$	9	37	$12_{4,5}$	12
3	$5_{4,5}$.	5.	17	$9_{3,4,5}$	9	41	$13_{3,4,5}$	13
4	5_5.	5.	19	$9_{4,5}$	9	43	$13_{4,5}$	13
5	$6_{3,4,5}$.	6.	23	$10_{4,5}$	10	47	$14_{3,4,5}$	14
7	$7_{3,4}$.	8.	25	$11_{3,4,5}$	11	49	$14_{3,4,5}$	14
8	$7_{3,4,5}$.	7.	27	$11_{3,4,5}$	11	53	$15_{3,4,5}$	15
9	7_4.	8.	29	$11_{4,5}$	11	59	$15_{4,5}$	15
11	$8_{3,4,5}$	8	31	11_4	12			
13	$8_{4,5}$	8	32	$12_{3,4,5}$	12			

TABLE III
UPPER BOUNDS $\bar{l} = \bar{l}(4,3;q)$ ON THE LENGTH FUNCTION $l(4,3;q)$ FOR $q \ge 61$

q	$\bar{l}$	q	$\bar{l}$	q	$\bar{l}$	q	$\bar{l}$	q	$\bar{l}$
61	16	109	20	167	24	233	27	289	30
64	16	113	20	169	24	239	28	293	30
67	16	121	21	173	24	241	28	307	30
71	16	125	21	179	24	243	28	311	31
73	17	127	21	181	25	251	28	313	31
79	17	128	21	191	25	256	28	317	31
81	18	131	22	193	25	257	28	331	32
83	18	137	22	197	25	263	28	337	33
89	18	139	22	199	25	269	29	343	33
97	19	149	23	211	27	271	29	401	34
101	19	151	23	223	27	277	29	499	37
103	19	157	23	227	27	281	30		
107	20	163	24	229	27	283	29		

Theorem 2: For $l(4,3;q) = k(3,q,2)$ and $t(3,q) = n(4,q)$ it holds that

$$\begin{aligned} l(4,3;q) \le b_q \sqrt[3]{q}, \quad & b_q < 4, \quad \text{if } 4 \le q \le 59 \\ & b_q < 5, \quad \text{if } 61 \le q \le 343, \ q \in Q_3 \\ t(3,q) \le c_q \sqrt[3]{q}, \quad & c_q < 4, \quad \text{if } 4 \le q \le 59, \ q \ne 7 \\ & c_q < 5, \quad \text{if } q = 7, \ 61 \le q \le 343, \ q \in Q_3. \end{aligned} \tag{5}$$

IV. FAMILIES OF CODES WITH COVERING RADIUS 3 AND CODIMENSION $3t+1$

All matrices and columns below are q-ary. An element of F_{q^m} written in a q-ary matrix denotes an m-dimensional column vector that is a q-ary representation of this element, and *vice versa*, we can treat an m-dimensional column vector as an element of F_{q^m}.

We give a q^m-concatenating construction based on the ideas of [4, Theorem 3.1]. We use an $[n_0, n_0 - r_0]_q 3$ starting code V_0 with a parity-check matrix $\boldsymbol{H}_0 = [f_1 f_2 \cdots f_{n_0}]$ where columns $f_j \in F_{q^{r_0}}$. Let $m \ge 1$ be an integer such that $q^m - 1 \ge n_0$. The parity-check matrix $\boldsymbol{H}$ of a new code V contains $r_0 + 3m$ rows and has the form

$$\boldsymbol{H} = [\, \boldsymbol{A} \quad \boldsymbol{B}_1 \quad \boldsymbol{B}_2 \quad \ldots \quad \boldsymbol{B}_{n_0} \,] \tag{6}$$

where $\boldsymbol{A}$ and $\boldsymbol{B}_j$ are matrices which we now define.

Let $\mathbf{0}^v$ be the zero matrix with v rows. Denote by $\boldsymbol{W}_m$ a parity-check matrix of the $[w_{m,q}, w_{m,q} - m]_q 1$ Hamming code with $w_{m,q} = (q^m - 1)/(q-1)$. Let $\boldsymbol{T}_{2m}$ be a parity-check matrix of a $[t_{2m,q}, t_{2m,q} - 2m]_q 2$ code V_{2m}. Then

$$\boldsymbol{A} = \left[\begin{array}{c|c} \mathbf{0}^{r_0} & \mathbf{0}^{r_0} \\ \boldsymbol{W}_m & \mathbf{0}^m \\ \mathbf{0}^{2m} & \boldsymbol{T}_{2m} \end{array}\right].$$

We denote $\{\xi_1, \xi_2, \ldots, \xi_{q^m}\} = F_{q^m}$, $\beta_j \in F_{q^m}^*$, $j = 1, 2, \ldots, n_0$, $F_{q^m}^* = F_{q^m} \setminus \{0\}$. We put $\beta_i \ne \beta_j$ when $i \ne j$ (it is possible since $q^m - 1 \ge n_0$). Then

$$\boldsymbol{B}_j = \begin{bmatrix} f_j & f_j & \cdots & f_j \\ \xi_1 & \xi_2 & \cdots & \xi_{q^m} \\ \beta_j \xi_1 & \beta_j \xi_2 & \cdots & \beta_j \xi_{q^m} \\ \beta_j^2 \xi_1 & \beta_j^2 \xi_2 & \cdots & \beta_j^2 \xi_{q^m} \end{bmatrix}, \qquad j = 1, 2, \ldots, n_0.$$

Theorem 3: The matrix $\boldsymbol{H}$ of (6) is a parity-check matrix of an $[n, n-r]_q 3$ code V with covering radius 3 and parameters $n = q^m n_0 + w_{m,q} + t_{2m,q}$, $r = r_0 + 3m$.

Proof: We prove that the code V has covering radius 3. We show that any arbitrary nonzero column $(a,b,c,d) \in F_{q^{r_0}} F_{q^m} F_{q^m} F_{q^m}$ can be represented by a linear combination of at most three columns of $\boldsymbol{H}$. Since the starting code V_0 has covering radius 3, we always have $a = sf_i + tf_j + uf_k$ with distinct i, j, k and $s, t, u \in F_q$. We consider four cases.

Case 1) $s \ne 0, t \ne 0, u \ne 0$. We find the values of ξ_x, ξ_y, ξ_z from the equation system

$$\begin{cases} s\xi_x + t\xi_y + u\xi_z = b \\ s\beta_i \xi_x + t\beta_j \xi_y + u\beta_k \xi_z = c \\ s\beta_i^2 \xi_x + t\beta_j^2 \xi_y + u\beta_k^2 \xi_z = d \end{cases}$$

the determinant of which

$$stu(\beta_j - \beta_i)(\beta_k - \beta_i)(\beta_k - \beta_j) \ne 0$$

since $\beta_i \ne \beta_j$ if $i \ne j$. As a result

$$\begin{aligned} (a,b,c,d) = {} & s(f_i, \xi_x, \beta_i \xi_x, \beta_i^2 \xi_x) \\ & + t(f_j, \xi_y, \beta_j \xi_y, \beta_j^2 \xi_y) + u(f_k, \xi_z, \beta_k \xi_z, \beta_k^2 \xi_z). \end{aligned}$$

Case 2) $s \ne 0, t \ne 0, u = 0$. We find the values of ξ_x, ξ_y from the system

$$\begin{cases} s\beta_i \xi_x + t\beta_j \xi_y = c \\ s\beta_i^2 \xi_x + t\beta_j^2 \xi_y = d. \end{cases}$$

The determinant $st\beta_i\beta_j(\beta_j - \beta_i) \ne 0$ as $\beta_i, \beta_j \in F_{q^m}^*$, $\beta_i \ne \beta_j$. If $b = s\xi_x + t\xi_y$ then

$$(a,b,c,d) = s(f_i, \xi_x, \beta_i \xi_x, \beta_i^2 \xi_x) + t(f_j, \xi_y, \beta_j \xi_y, \beta_j^2 \xi_y).$$

Else to get b we add to the linear combination for (a,b,c,d) one column of the left submatrix of $\boldsymbol{A}$ with some q-ary coefficient.

Case 3) $s \ne 0, t = u = 0$. We find ξ_x putting $s\xi_x = b$. If $c = s\beta_i \xi_x$ and $d = s\beta_i^2 \xi_x$ then

$$(a,b,c,d) = s(f_i, \xi_x, \beta_i \xi_x, \beta_i^2 \xi_x).$$

Else, to get c and d we add to the linear combination for (a,b,c,d) one or two columns from the right submatrix of $\boldsymbol{A}$ with some q-ary coefficients.

Case 4) $s = t = u = 0$. Hence $a = 0$. By the direct sum construction [3], the last $3m$ rows of $\boldsymbol{A}$ are a parity-check matrix of a code with covering radius 3 and $(0,b,c,d)$ is a linear combination of at most three columns of $\boldsymbol{A}$. □

TABLE IV
ALL SIZES k OF MINIMAL 2-SATURATING k-SETS IN PG$(3,q)$ AND VALUES OF $N^d_{q,k}$

q	2			3			4			5		
k	$N^3_{2,k}$	$N^4_{2,k}$	$N^5_{2,k}$	$N^3_{3,k}$	$N^4_{3,k}$	$N^5_{3,k}$	$N^3_{4,k}$	$N^4_{4,k}$	$N^5_{4,k}$	$N^3_{5,k}$	$N^4_{5,k}$	$N^5_{5,k}$
5	1	1	0	0	1	1	0	0	1			
6				1	0	0	1	0	0	1	2	1
7							2	2	0	6	2	0
8										1	0	0
9										1	0	0

TABLE V
CLASSIFICATION OF THE SMALLEST MINIMAL 2 -SATURATING k -SETS IN PG$(3,q)$

q	k	no.	l_2	l_3	π_3	π_4	5th point	6th point	Order of stab.	d
2	5	1	10	-	6	1	1110			4
		2	7	1	3	2	1100			3
3	5	1	10	-	10	-	1111		120	5
		2	10	-	6	1	1220		48	4
4	5	1	10	-	10	-	1112		240	5
5	6	1	15	-	20	-	1232	1443	120	5
		2	15	-	16	1	1220	1343		4
		3	15	-	12	2	1220	0122		4
		4	12	1	10	3	1232	1141		3

As the codes V_{2m} one can use results of [5, Example 5], [13] where by q^m-concatenating constructions infinity families of $[t_{2m,q}, t_{2m,q}-2m]_q 2$ codes are obtained with parameters

$$R=2, \quad t_{2m,q}=2q^{m-1}+q^{m-2}, \quad \text{if } m=2,3,5 \text{ and } m\geq 7, \quad q=7,8 \text{ and } q\geq 11 \tag{7}$$

$$R=2, \quad t_{2m,q}=2q^{m-1}+q^{m-2}+q^{m-3}, \quad \text{if } m=3,5,8,9 \text{ and } m\geq 11, \quad q=4,5,9. \tag{8}$$

Let there exist an $[n_{q,3}, n_{q,3}-4]_q 3$ code with $n_{q,3}\leq q^M-1$. We can use it as the starting code V_0 for Theorem 3, put $m\geq M$, and obtain an infinite family of $[n, n-r]_q 3$ codes with

$$R=3, \quad r=3(m+1)+1, \quad n=n_{q,3}q^m+\frac{q^m-1}{q-1}+t_{2m,q} \quad n_{q,3}\leq q^M-1, m\geq M. \tag{9}$$

By Tables II and III, there exist $[n_{q,3}, n_{q,3}-4]_q 3$ codes $\mathcal{K}_q$ where $n_{q,3}=\bar{l}(4,3;q)=b_q \sqrt[3]{q}$, the estimates of b_q are given by (5), $n_{q,3}\leq q-1$ if $8\leq q\leq 343$, $q\in Q_3$, $n_{q,3}\leq q^2-1$ if $4\leq q\leq 7$. The codes $\mathcal{K}_q$ can be used as the starting codes V_0 for Theorem 3. We substitute (7) and (8) into (9), change $3(m+1)$ by $3t$, and obtain the infinite families $\mathcal{A}_3$, $\mathcal{A}_4$ of $[n, n-r]_q 3$ codes with parameters

$$\mathcal{A}_3: R=3, \quad r=3t+1, \quad t=3,4,6 \text{ and } t\geq 8, \quad q=7,8 \text{ and } 11\leq q\leq 343, \quad q\in Q_3,$$
$$n=n_{q,3}\,q^{t-1}+3q^{t-2}+2q^{t-3}+\frac{q^{t-3}-1}{q-1} \tag{10}$$

$$\mathcal{A}_4: R=3, r=3t+1, \quad t=4,6,9,10 \text{ and } t\geq 12, \quad q=4,5,9,$$
$$n=n_{q,3}\,q^{t-1}+3q^{t-2}+2q^{t-3}+2q^{t-4}+\frac{q^{t-4}-1}{q-1}. \tag{11}$$

TABLE VI
CLASSIFICATION OF THE GREATEST MINIMAL 2 -SATURATING k -SETS IN PG$(3,q)$

q	k	no.	l_2	l_3	l_4	l_5	π_3	π_4	π_5	π_6	5th-9th points	Order of stab.	d
3	6	1	9	-	1	-	4	-	2	-	1100 1200	192	3
4	7	1	21	-	-	-	15	-	-	1	1210 1120 1330	2160	4
4	7	2	21	-	-	-	7	7	-	-	1210 1013 1203	336	4
4	7	3	11	-	-	1	5	-	-	2	1100 1200 1300	2160	3
4	7	4	9	4	-	-	3	4	-	1	1100 0110 1110	144	3
5	9	1	18	6	-	-	6	-	9	-	0011 0110 1203 1220 1003	72	3

By (5), (10), and (11), we can get the estimates

$$\overline{\mu}_q(3,\mathcal{A}_3)\approx \overline{\mu}_q(3,\mathcal{A}_4)<n^3_{q,3}/6q=b^3_q/6$$

i.e.,

$$\overline{\mu}_q(3,\mathcal{A}_3)\approx \overline{\mu}_q(3,\mathcal{A}_4)<11, \quad \text{if } 4\leq q\leq 59$$
$$\overline{\mu}_q(3,\mathcal{A}_3)<21, \quad \text{if } 61\leq q\leq 343, \quad q\in Q_3.$$

Let $q=p^3$. As the code V_0 for Theorem 3 we take the $[6p-2, 6p-6]_q 3$ code based on [11, Theorem 6]. As V_{2m} we use codes of (7) and obtain the infinite code family $\mathcal{A}_5$ with

$$\mathcal{A}_5: R=3, \quad r=3t+1, \quad t=3,4,6 \text{ and } t\geq 8, \quad q=p^3, \quad v_q=6p-2, \quad \overline{\mu}_q(3,\mathcal{A}_5)<v^3_q/6q<36,$$
$$n=v_q q^{t-1}+3q^{t-2}+2q^{t-3}+(q^{t-3}-1)/(q-1).$$

So, for the infinite families $\mathcal{A}_3$, $\mathcal{A}_4$ with $4\leq q\leq 343$, $q\in Q_3$, and $\mathcal{A}_5$ with $q=p^3$ the covering density is bounded from above by constants.

APPENDIX

We give results on the classification of minimal 2-saturating sets in PG$(3,q)$. Let $d\in\{3,4,5\}$ be the distance of a $[k,k-4,d]_q 3$ code obtained when points of a 2-saturating k-set are treated as columns of a parity-check matrix, see Section III. By $N^d_{q,k}$ we denote in PG$(3,q)$ the number of projectively distinct minimal 2-saturating k-sets corresponding to a $[k,k-4,d]_q 3$ code.

In the 2-saturating sets written in tables, similarly to [7], [8], [11], we represent elements of F_q as follows. If q is prime, $F_q=\{0,1,\ldots,q-1\}$ and we operate on these elements modulo q. If q is a power of a prime, we denote

$$F_q=\{0,1=\alpha^0,2=\alpha^1,\ldots,q-1=\alpha^{q-2}\}$$

where α is a primitive element. For $q=4$ we use the polynomial x^2+x+1.

TABLE VII
SIZES k OF THE SMALLEST MINIMAL k-SATURATING k-SETS IN PG $(3, q)$ AND THE NUMBERS $N^d_{q,k}$ OF PROJECTIVELY DISTINCT SETS, $q = 7, 8, 9$

q	k	$N^3_{q,k}$	$N^4_{q,k}$	$N^5_{q,k}$
7	7	15	54	0
8	7	3	19	1
9	7	0	27	0

All 2-saturating sets in tables have $0001, 0010, 0100, 1000$ as the first four points. We denote by l_i (resp., π_i) the number of lines (resp., planes) having i intersections with the given set. "Order of stab." means the order of stabilizer group for the given set.

Contents of Tables IV–VII are given in their captions, for Tables IV–VI we have $q \leq 5$.

ACKNOWLEDGMENT

The authors wish to thank the anonymous referees for their useful comments. A. A. Davydov gratefully acknowledges the University of Perugia for their hospitality.

REFERENCES

[1] T. S. Baicheva and E. D. Velikova, "Covering radii of ternary linear codes of small dimensions and codimensions," *IEEE Trans. Inform. Theory*, vol. 43, pp. 2057–2061, Nov. 1997.
[2] R. A. Brualdi, V. S. Pless, and R. M. Wilson, "Short codes with a given covering radius," *IEEE Trans. Inform. Theory*, vol. 35, pp. 99–109, Jan. 1989.
[3] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Amsterdam, The Netherlands: North-Holland, 1997.
[4] A. A. Davydov, "Constructions and families of covering codes and saturated sets of points in projective geometry," *IEEE Trans. Inform. Theory*, vol. 41, pp. 2071–2080, Nov. 1995.
[5] ——, "Constructions and families of nonbinary linear codes with covering radius 2," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1679–1686, July 1999.
[6] ——, "1-Saturating sets in projective planes obtained by computer," preprint, Institute for Information Transmission Problems, Moscow, Russia, 2003.
[7] A. A. Davydov, G. Faina, S. Marcugini, and F. Pambianco, "Computer search in projective planes for the sizes of complete arcs," *J. Geom.*, to be published.
[8] A. A. Davydov, S. Marcugini, and F. Pambianco, "On saturating sets in projective spaces," *J. Combin. Theory, Ser. A*, vol. 103, pp. 1–15, 2003.
[9] ——, "2-saturating sets in projective spaces PG $(3, q)$," preprint, Università degli Studi di Perugia, Perugia, Italy, 2003.
[10] A. A. Davydov and P. R. J. Östergård, "New linear codes with covering radius 2 and odd basis," *Des., Codes Cryptogr.*, vol. 16, pp. 29–39, 1999.
[11] ——, "On saturating sets in small projective geometries," *Europ. J. Combin.*, vol. 21, pp. 563–570, 2000.
[12] ——, "New quaternary linear codes with covering radius 2," *Finite Fields and Their Applications*, vol. 6, pp. 164–174, 2000.
[13] ——, "Linear codes with covering radius $R = 2, 3$ and codimension tR," *IEEE Trans. Inform. Theory*, vol. 47, pp. 416–421, Jan. 2001.
[14] J. W. P. Hirschfeld, *Projective Geometries Over Finite Fields*, 2nd ed. Oxford, U.K.: Clarendon, 1998.
[15] J. W. P. Hirschfeld and L. Storme, "The packing problem in statistics, coding theory, and finite projective spaces: Update 2001," in *Developments in Mathematics*. Norwell, MA: Kluwer, 2000, vol. 3, Finite Geometries, pp. 201–246.
[16] T. Penttila, private communication.
[17] T. Penttila and I. Pinneri, "Irregular hyperovals in $PG(2, 64)$," *J. Geom.*, vol. 51, pp. 89–100, 1994.

Linear Codes From Narrow Ray Class Groups of Algebraic Curves

Chaoping Xing

***Abstract*—By employing the narrow ray class groups of algebraic curves and the Hurwitz genus formula, we construct a class of linear codes over prime fields with reasonable parameters. In particular, we obtain some new codes compared with Brouwer's table [1].**

***Index Terms*—Class number, codes, curves, divisors, ray class group.**

I. INTRODUCTION

Since the discovery of the Goppa geometry codes [4], various constructions of codes from algebraic curves and varieties have been studied [11], [2], [6], [14]–[16]. In terms of asymptotic results, the constructions by Goppa [4], Katsman–Tsfasman [11], Vlăduţ [13], Elkies [3], and Xing [14] are quite powerful and interesting. However, not every construction achieving the asymptotically good codes is also powerful for codes with finite parameters or over small alphabets. Because of this, researchers have been looking for other constructions based on algebraic curves to obtain good codes with finite parameters (see [2], [6], [15], [16]).

In this correspondence, we make use of the narrow ray class groups to give a construction of linear codes over prime fields. It turns out that the codes have reasonable parameters and some new codes are found.

II. CONSTRUCTIONS

Before proceeding to our construction, we introduce narrow ray class groups of algebraic curves.

When we speak of an algebraic curve over the finite field $\boldsymbol{F}_q$, we always mean a smooth, projective, absolutely irreducible algebraic curve defined over $\boldsymbol{F}_q$. If $\mathcal{X}$ is such a curve, simply denoted by $\mathcal{X}/\boldsymbol{F}_q$, then we write $g(\mathcal{X})$ for the genus of $\mathcal{X}$. A point of $\mathcal{X}$ is called $\boldsymbol{F}_q$-rational if it has homogeneous coordinates which all belong to $\boldsymbol{F}_q$. Let $N(\mathcal{X}/\boldsymbol{F}_q)$ denote the number of $\boldsymbol{F}_q$-rational points of $\mathcal{X}/\boldsymbol{F}_q$. According to the Weil bound

$$N(\mathcal{X}) \leq q + 1 + 2g(\mathcal{X})\sqrt{q}$$

the following definition makes sense.

For any prime power q and any integer $g \geq 0$, put

$$N_q(g) := \max N(\mathcal{X}/\boldsymbol{F}_q),$$

where the maximum is extended over all curves $\mathcal{X}/\boldsymbol{F}_q$ with $g(\mathcal{X}) = g$.

We fix an $\boldsymbol{F}_q$-rational point P of $\mathcal{X}/\boldsymbol{F}_q$. Then every element in the divisor class group $\mathcal{C}\ell(\mathcal{X}/\boldsymbol{F}_q)$ of $\mathcal{X}/\boldsymbol{F}_q$ can be represented as a divisor

Manuscript received August 3, 2002; revised October 30, 2003. This work was supported in part by the Singapore MOE-ARF under Grant R-146-000-029-112 and the Hundred Talents Program of the Chinese Academy of Sciences.

The author is with the Department of Mathematics, National University of Singapore, Singapore 117543 and the Department of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, China (e-mail: matxcp@nus.edu.sg).

Communicated by R. Koetter, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2004.824922