Locally Optimal Covering Codes and Minimal Saturating Sets

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

Giorgio Faina, Stefano Marcugini, Fernanda Pambianco
Dipartimento di Matematica e Informatica,
Università degli Studi di Perugia, Via Vanvitelli 1, Perugia, 06123, Italy
faina@dipmat.unipg.it, gino@dipmat.unipg.it, fernanda@dipmat.unipg.it

Abstract. A concept of locally optimal (LO) linear covering codes is introduced in accordance with the concept of minimal saturating sets in projective spaces over finite fields. An LO code is nonshortening in the sense that removing any column from a parity check matrix we increase the code covering radius. Constructions and infinite families of LO codes are described. New bounds on the length function are given. New extremal and classification problems for linear covering codes are investigated, in particular, the spectrum of possible lengths of LO codes and the greatest possible length. The complete computer classification of the minimal saturating sets and of the corresponding LO codes is obtained.

1 Introduction

Let F_q be the Galois field of q elements, $F_q^* = F_q \setminus \{0\}$. 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 at most R columns of a parity check matrix of this code and R is the smallest value with such property.

Let $PG(v,q)$ be the v-dimensional projective space over F_q. For an integer ϱ with $0 \le \varrho \le v$, 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 $PG(v,q)$ in which x lies and ϱ is the smallest value with such property. A ϱ-saturating set S is called *minimal* if for every point $P \in S$ the set $S \setminus \{P\}$ is not ϱ-saturating [2],[3].

Definition 1. A linear covering code is called *locally optimal* (LO) if one cannot remove any column from a code parity check matrix with-

out increasing the code covering radius. An LO code can be called also *nonshortening* in the sense mentioned.

Let $[n, n-r, d]_q R$ be a q-ary linear code of length n, codimension r, minimum distance d, and covering radius R. Here one may omit d. The length function $l(r, R; q)$ is the smallest length of an $[n, n-r]_q R$ code.

The points of a ϱ-saturating n-set in $PG(r-1, q)$ can be considered as columns of a parity check matrix of an $[n, n-r]_q R$ code with $R = \varrho + 1$ [1]-[3]. Points of a minimal saturating set form a parity check matrix of an LO code.

The concept of LO codes essentially extends the region of combinatorial investigations of linear codes. It allows us to introduce new extremal and classification problems. In this paper we study the maximal possible length and the spectrum of possible lengths of LO codes. The length function problem is considered also in the framework of LO codes.

In this work we propose new q^m-concatenating constructions of LO codes based on the ideas of [1],[3]. These constructions take an LO code as a "seed" and produce an infinite family of LO codes of growing codimension with the same covering radius and almost the same covering density as the starting code. Infinite families of LO codes are designed.

2 q^m-concatenating constructions

Definition 2. Let $\mathbf{H}$ be a parity check matrix of an $[n, n-r]_q R$ code. A partition of the column set of $\mathbf{H}$ into nonempty subsets is called an *R-partition* if every nonzero r-positional q-ary column is equal to a linear combination from at most R columns of $\mathbf{H}$ belonging to *distinct subsets*.

Construction $\mathbf{CC}_t$. We use a *starting* $[n_0, n_0 - r_0]_q R$ LO code V_0 with a parity check matrix $\mathbf{H}_0 = [h_1 h_2 \dots h_{n_0}]$ where h_j is a column. Let $m \geq 1$ be an integer parameter. We suppose that $\mathbf{H}_0$ has an R-partition $\mathcal{P}_0$ to p_0 subsets. For every column h_j we assign an *indicator* $\beta_j \in F_{q^m}$ so that if columns h_i and h_j belong to distinct subsets of $\mathcal{P}_0$ then $\beta_i \neq \beta_j$. If h_i and h_j belong to the same subset we may assign either $\beta_i = \beta_j$ or $\beta_i \neq \beta_j$ as well. We denote $\mathcal{B} = \{\beta_1, \beta_2, \dots, \beta_{n_0}\}$. Let $\mathbf{A}_t$ be a matrix. The parity check matrix $\mathbf{H}_V$ of a new $[n, n-(r_0 + Rm)]_q R$ code V has the form

$$\mathbf{H}_V = [\mathbf{A}_t \ \mathbf{B}_\Sigma], \quad \mathbf{B}_\Sigma = [\mathbf{B}_1 \ \mathbf{B}_2 \ \dots \ \mathbf{B}_{n_0}],$$

$$\mathbf{B}_j = \begin{bmatrix} h_j & h_j & \cdots & h_j \\ \xi_1 & \xi_2 & \cdots & \xi_{q^m} \\ \beta_j\xi_1 & \beta_j\xi_2 & \cdots & \beta_j\xi_{q^m} \\ \beta_j^2\xi_1 & \beta_j^2\xi_2 & \cdots & \beta_j^2\xi_{q^m} \\ \cdots & \cdots & \cdots & \cdots \\ \beta_j^{R-1}\xi_1 & \beta_j^{R-1}\xi_2 & \cdots & \beta_j^{R-1}\xi_{q^m} \end{bmatrix}, \ \{\xi_1, \xi_2, \ldots, \xi_{q^m}\} = F_{q^m}.$$

Let $\mathbf{S}_m$ be a parity check matrix of the $[w_{m,q}, w_{m,q} - m]_q 1$ Hamming code, $w_{m,q} = (q^m - 1)/(q-1)$, and let $\mathbf{0}_k$ be the zero matrix with k rows. Then

$$\mathbf{A}_1 = \begin{bmatrix} \mathbf{0}_{r_0} & \mathbf{0}_{r_0} \\ \mathbf{S}_m & \mathbf{0}_m \\ \mathbf{0}_m & \mathbf{S}_m \end{bmatrix}, \mathbf{A}_2 = \begin{bmatrix} \mathbf{0}_{r_0+m} \\ \mathbf{S}_m \end{bmatrix}, \mathbf{A}_3 = \begin{bmatrix} \mathbf{0}_{r_0} & \mathbf{0}_{r_0} & \mathbf{0}_{r_0} \\ \mathbf{S}_m & \mathbf{0}_m & \mathbf{0}_m \\ \mathbf{0}_m & \mathbf{S}_m & \mathbf{0}_m \\ \mathbf{0}_m & \mathbf{0}_m & \mathbf{S}_m \end{bmatrix}, \mathbf{A}_4 = \begin{bmatrix} \mathbf{0}_{r_0+m} & \mathbf{0}_{r_0+m} \\ \mathbf{S}_m & \mathbf{0}_m \\ \mathbf{0}_m & \mathbf{S}_m \end{bmatrix}.$$

Construction CC$_1$. Here $R = 2$, $q^m > p_0$, $\mathcal{B} \subseteq F_{q^m}^*$, $n = n_0 q^m + 2w_{m,q}$.

Construction CC$_2$. Here $R = 2$, $n_0 \geq q^m \geq p_0$, $\mathcal{B} = F_{q^m}$, $n = n_0 q^m + w_{m,q}$.

Construction CC$_3$. Here $R = 3$, $q^m > p_0$, $\mathcal{B} \subseteq F_{q^m}^*$, $n = n_0 q^m + 3w_{m,q}$. Besides, there are not three linear dependent columns of $\mathbf{H}_0$ belonging to distinct subsets of $\mathcal{P}_0$.

Construction CC$_4$. Here $R = 3$, $q^m > p_0$, $\mathcal{B} \subseteq F_{q^m} \setminus \{1\}$, $n = n_0 q^m + 2w_{m,q}$. Besides, there are three linear dependent columns of $\mathbf{H}_0$ belonging to distinct subsets of $\mathcal{P}_0$, there is a column $\overline{h}$ of $\mathbf{H}_0$ that is not equal to a linear combination of at most three other columns of $\mathbf{H}_0$ belonging to distinct subsets of $\mathcal{P}_0$, the indicator assigned to $\overline{h}$ is $\overline{\beta} = 0$.

Theorem 1: The codes V of Constructions CC$_1$-CC$_4$ are LO codes.

3 On new extremal problems

Let $m(r, R; q)$ be the maximal possible length of an $[n, n-r]_q R$ LO code.

Theorem 2: $m(r, R; q) \geq M_q(r, R) = (q^{r-R+1} - 1)/(q-1) + R - 1$, $r \geq R \geq 2$, $q \geq 2$. Besides, $m(r, 2; q) = M_q(r, 2)$.

Theorem 3: $m(r, R; q) = M_q(r, R)$ for the following sets of parameters:
$R = 3$, $r = 4$, $q = 2, 3, 4, 7$; $R = 3$, $r = 5$, $q = 2, 3$; $R = 3$, $r = 6$, $q = 2$.
$R = 4$, $r = 5$, $q = 2, 3, 4$; $R = 4$, $r = 6$, $q = 2, 3$; $R = 4$, $r = 7$, $q = 2$.

Theorem 4: $m(R+1,R;5) = M_5(R+1,R)+1 = R+6,\ R=3,4;$
$m(R+1,R;5) \geq M_5(R+1,R)+1 = R+6,\ R \geq 5.$

4 New classification problems. Spectrum of possible lengths of locally optimal codes

In Tables 1 - 4 we give LO codes with distinct lengths obtained as minimal saturating sets by geometrical computer methods. In Table 1, only code lengths $n \leq q$ are considered as codes with $n = q+1, q+2$ always exist [2]. The dot means that all possible lengths n for the given q are known. In Tables 2 - 4, t is the number of distinct $[n, n-r, d]_q R$ LO codes.

Table 1. Lengths n of the known $[n, n-3]_q 2$ LO codes with $n \leq q$

q	lengths n	q	lengths n	q	lengths n
7.	$6 \leq n \leq 7$	37	$16 \leq n \leq 36$	83	$26 \leq n \leq 79,\ n \neq 71, 72$
8.	$6 \leq n \leq 8$	41	$16 \leq n \leq 39$	89	$28 \leq n \leq 84$
9.	$6 \leq n \leq 9$	43	$16 \leq n \leq 41$	97	$29 \leq n \leq 91$
11.	$7 \leq n \leq 11$	47	$18 \leq n \leq 45$	101	$30 \leq n \leq 95,\ n \neq 86, 87$
13.	$8 \leq n \leq 13$	49	$18 \leq n \leq 47$	103	$30 \leq n \leq 97$
16.	$9 \leq n \leq 16$	53	$18 \leq n \leq 50$ $n \neq 19$	107	$31 \leq n \leq 100,\ n \neq 94$
17	$10 \leq n \leq 17$	59	$20 \leq n \leq 56$	109	$31 \leq n \leq 102,\ n \neq 95$
19	$10 \leq n \leq 19$	61	$20 \leq n \leq 57$	113	$32 \leq n \leq 106,\ n \neq 98, 99$
23	$10 \leq n \leq 23$ $n \neq 11$	64	$19 \leq n \leq 61$ $n \neq 20, 21$	121	$32 \leq n \leq 113,\ n \neq 103, 107$
25	$12 \leq n \leq 25$	67	$23 \leq n \leq 63$	125	$34 \leq n \leq 117,\ n \neq 108-110$
27	$12 \leq n \leq 26$	71	$22 \leq n \leq 67$	127	$35 \leq n \leq 119,\ n \neq 110-113$
29	$13 \leq n \leq 28$	73	$24 \leq n \leq 69$	128	$34 \leq n \leq 120,\ n \neq 110-115$
31	$14 \leq n \leq 30$	79	$26 \leq n \leq 74$	131	$35 \leq n \leq 123,\ n \neq 113, 114$
32	$13 \leq n \leq 31$	81	$26 \leq n \leq 76$ $n \neq 70$	137	$36 \leq n \leq 129,\ n \neq 108-120$

Using the constructions described in Section 2 and starting from some LO codes of Tables 1, 2 and 4 we obtained infinite families of $[n, n-r]_q R$ LO codes with parameters

$$R = 2,\ q \geq 2,\ r = 3+2m,\ n = n_0 q^m + 2(q^m-1)/(q-1),\ m \geq 2.$$

$$R = 2,\ q \geq 5,\ r = 2m+1,\ n = (q^{m+1}-1)/(q-1).$$

$$R = 3,\ q = 7, r = 4+3m,\ n = ((2n_0+1)\cdot 7^m - 1)/2,\ n_0 = 7,8,9,\ m \geq 2.$$

$$R = 3,\ q = 5,\ r = 4+3m,\ n = (13\cdot 5^m - 1)/2,\ m \geq 2.$$

$$R = 2,\ q = 17,\ r \geq 3,\ n = (7\cdot 17^{r-2} + 73)/16,\ n = (5\cdot 17^{r-2} + 107)/16.$$

$$R = 2,\ q \geq 3,\ r \geq 3,\ n = q^{r-2}+1,\ n = (2q^{r-2} + q^2 - 2q - 1)/(q-1).$$

$$R = 2,\ q \geq 3,\ r \geq 3,\ n = q^{r-2} + (q^{r-3}-1)/(q-1) + 1.$$

For the 1-st family we suppose that there exists an $[n_0, n_0-3]_q 2$ code.

Theorem 5: For $R = 2$, $2 \leq q \leq 16$, $R = 3$, $2 \leq q \leq 7$, $R = 4$, $2 \leq q \leq 5$, there exist $[n, n-(R+1)]_q R$ LO codes of all possible lengths in the region $l(R+1, R; q) \leq n \leq m(R+1, R; q)$.

Table 2. Complete classification of $[n, n-r, d]_q 3$ LO codes for small r, q

q	r	n	d	t	q	r	n	d	t	q	r	n	d	t	q	r	n	d	t
2	4	5	3 4	1 1	2	6	11	3 4	10 3	3	5	11	3 4	7 2	5	4	8	3	1
2	5	6	5 6	1 1	2	6	12	3 4	1 1	3	5	12	3	2	5	4	9	3	1
2	5	7	3	2	2	6	17	3 4	1 1	3	5	15	3	1	7	4	7	3 4	15 54
2	5	9	3 4	1 1	3	4	5	4 5	1 1	4	4	5	5	1	7	4	8	3 4 5	174 3 1
2	6	7	7	1	3	4	6	3	1	4	4	6	3	1	7	4	9	3 4	38 1
2	6	8	3 5	1 1	3	5	8	3 4	8 3	4	4	7	3 4	2 2	7	4	10	3	5
2	6	9	3	1	3	5	9	3 4	14 11	5	4	6	3 4 5	1 2 1					
2	6	10	3 4	1 2	3	5	10	3	3	5	4	7	3 4	6 2					

Table 3. Classification of $[n, n-r, d]_q R$ LO codes of the smallest length

R	q	r	n	d	t	R	q	r	n	d	t	R	q	r	n	d	t	R	q	r	n	d	t
3	8	4	7	3 4 5	3 19 1	3	11	4	8	3 4 5	≥ 1 ≥ 1 ≥ 1	3	5	5	10			4	7	5	7	4 5	1 3
3	9	4	7	4	27	3	4	5	9	3 4	1 21	3	3	6	11	3	8	4	8	5	7	5	1
																		4	2	8	9	9	1

Table 4. Complete classification of $[n, n-r, d]_q 4$ LO codes for small r, q

q	r	n	d	t	q	r	n	d	t	q	r	n	d	t	q	r	n	d	t
2	5	6	3 4	1 1	5	5	8	3 4	6 3	3	6	9	3 4	12 2	2	7	10	3	2
3	5	6	4 5 6	1 1 1	5	5	9	3	1	3	6	10	3 4	15 11	2	7	11	3 4	1 2
3	5	7	3	1	5	5	10	3	1	3	6	11	3	3	2	7	12	3 4	1 1
4	5	6	5 6	1 1	2	6	7	5 6	1 1	3	6	12	3 4 5	7 2 1	2	7	13	3 4	1 1
4	5	7	3	1	2	6	8	3 4	2 1	3	6	13	3	2	2	7	18	3 4	1 1
4	5	8	3 4	2 2	2	6	10	3 4	1 1	3	6	16	3	1					
5	5	6	6	1	3	6	7	7	1	2	7	8	7 8	1 1					
5	5	7	3 4 5	1 3 1	3	6	8	4	2	2	7	9	3 4 5 6	2 1 1 1					

5 New bounds on the length function

By Tables 3 and 4 we have the new exact values, cf. [3, Tab. 2],

$$l(5,3;4) = 9,\ l(5,3;5) = 10,\ l(4,3;11) = 8,$$
$$l(5,4;4) = l(5,4;5) = 6,\ l(5,4;7) = l(5,4;8) = 7.$$

In Table 5 we give the lengths of the $[l_q, l_q - 4, d]_q 3$ LO codes obtained by geometrical computer methods. The subscript indicates the code distance d. The dot notes the exact bounds $l(4,3;q) = l_q$.

Theorem 6: For the length function $l(4,3;q)$ we have the upper bound

$$l(4,3;q) \le b_q \sqrt[3]{q}, \;\; b_q \le 4 \text{ if } q \le 83, \; b_q \le 4.5 \text{ if } q \le 343, \; b_q \le 5 \text{ if } q \le 563.$$

Using Construction CC_4 for every $[l_q, l_q - 4, 3]_q 3$ LO code of Table 5 we design an infinite family of $[n, n-r]_q R$ LO codes giving new upper bounds on the length function $l(3t+1,3;q)$, cf. [3, form. (10),(11)]. Here

$$R = 3, \; r = 3t+1, \; n = l_q q^{t-1} + 2\frac{q^{t-1}-1}{q-1}, \; t \ge 2 \text{ if } q \ge 8, \; t \ge 3 \text{ if } q \le 7.$$

Table 5. New upper bounds l_q on the length function $l(4,3;q)$, $q \le 563$

q	l_q	q	l_q	q	l_q	q	l_q	q	l_q	q	l_q	q	l_q
2	$5_{3,4}$.	37	$12_{4,5}$	103	19_5	179	24_5	269	$29_{3,5}$	361	32_3	463	36_3
3	$5_{4,5}$.	41	$13_{3,4,5}$	107	19_4	181	24_4	271	$29_{3,5}$	367	32_4	467	36_3
4	5_5.	43	$13_{4,5}$	109	$20_{3,5}$	191	$25_{3,5}$	277	$29_{3,5}$	373	$33_{3,5}$	479	36_3
5	$6_{3,4,5}$.	47	$14_{3,4,5}$	113	$20_{3,5}$	193	$25_{3,5}$	281	$29_{3,5}$	379	$33_{3,5}$	487	$36_{3,5}$
7	$7_{3,4}$.	49	$14_{3,4,5}$	121	20_4	197	$25_{3,5}$	283	$29_{3,5}$	383	$33_{3,5}$	491	36_4
8	$7_{3,4,5}$.	53	$15_{3,4,5}$	125	$21_{3,5}$	199	25_5	289	29_4	389	33_4	499	$37_{3,5}$
9	7_4.	59	$15_{3,4,5}$	127	$21_{3,5}$	211	$26_{3,5}$	293	29_4	397	$34_{3,5}$	503	$37_{3,5}$
11	$8_{3,4,5}$.	61	15_4	128	$21_{3,5}$	223	$27_{3,5}$	307	$30_{3,5}$	401	$34_{3,5}$	509	$37_{3,5}$
13	$8_{4,5}$	64	$16_{3,4,5}$	131	$21_{3,5}$	227	$27_{3,5}$	311	30_4	409	$34_{3,5}$	512	37_5
16	$9_{3,4,5}$	67	$16_{3,4,5}$	137	$22_{3,5}$	229	$27_{3,5}$	313	30_4	419	34_3	521	37_4
17	$9_{3,4,5}$	71	$16_{4,5}$	139	$22_{3,5}$	233	$27_{3,5}$	317	30_4	421	34_3	523	38_3
19	$9_{4,5}$	73	16_4	149	22_5	239	$27_{3,5}$	331	$31_{3,5}$	431	$35_{3,5}$	529	38_5
23	$10_{3,4,5}$	79	$17_{3,5}$	151	22_4	241	$28_{3,5}$	337	31_3	433	35_3	541	38_5
25	$11_{3,4,5}$	81	17_4	157	$23_{3,5}$	243	$28_{3,5}$	343	31_4	439	$35_{3,5}$	547	38_4
27	$11_{3,4,5}$	83	17_4	163	23_5	251	$28_{3,5}$	347	$32_{3,5}$	443	$35_{3,5}$	557	39_5
29	$11_{3,4,5}$	89	$18_{3,5}$	167	$24_{3,5}$	256	$28_{3,5}$	349	$32_{3,5}$	449	$35_{3,5}$	563	39_5
31	11_4	97	$19_{3,5}$	169	$24_{3,5}$	257	$28_{3,5}$	353	$32_{3,5}$	457	35_4		
32	$12_{3,4,5}$	101	19_5	173	$24_{3,5}$	263	$28_{3,5}$	359	$32_{3,5}$	461	$36_{3,5}$		

References

[1] 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.

[2] A. A. Davydov, S. Marcugini, F. Pambianco, On saturating sets in projective spaces, *J. Combin. Theory, Ser. A* 103, 2003, 1-15.

[3] 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.