Constructions of Nonlinear Covering Codes

Alexander A. Davydov

***Abstract*—Constructions of nonlinear covering codes are given. Using any nonlinear starting code of covering radius $R \geq 2$ these constructions form an infinite family of codes with the same covering radius. A nonlinear code is treated as a union of cosets of a linear code. New infinite families of nonlinear covering codes are obtained. Concepts of R, l-objects, R, l-partitions, and R, l-length are described for nonlinear codes.**

***Index Terms*—Binary codes, covering codes, covering radius, nonbinary codes, nonlinear codes.**

I. Introduction

Covering codes and their constructions are considered, e.g., in [1]–[30], and the references therein. In Sections II and III we develop and generalize linear code constructions of [6]–[8] and [12] and propose new constructions of nonlinear covering codes. Using an arbitrary code of covering radius $R \geq 2$ as a starting code, these constructions form an infinite family of codes with the same covering radius. A nonlinear code is treated as a union of cosets of a linear code. Such treatment is based on the ideas of [1] and [22], their variants [13], [17], [23], [24], and [28], and approaches of [20] and [21]. The new constructions also use structural ideas of the blockwise-direct sum construction [16], [26, Sec. 18.7.2], and [28]. In Section IV, new infinite families of covering codes are obtained. Parameters of the new codes are better than those of known codes with the same length and covering radius.

In [6] a new type of constructions of linear covering codes was proposed. In [7], [8], and [12] the ideas of [6] were modified and developed. The constructions of the type considered in [6]–[8] and [12] can be called "q^m-concatenating constructions" since a parity-check matrix of a starting code is repeated q^m times. In this correspondence, we give variants of q^m-concatenating constructions for q-ary nonlinear codes, $q \geq 2$. Some results of this work were briefly described in [9] and [10]. (Note also that the main ideas of nonlinear constructions of this correspondence were described in the submitted version of [8]. To save space, the final version of [8] contains only linear constructions.)

In [28, Supplement] Struik briefly described a nonlinear generalization of linear q^m-concatenating constructions of [6], [7], and [12]. This generalization is close to Construction B of this work, see Remark 2.

Let E_q^n be the space of n-dimensional row vectors over the Galois field GF(q), $q \geq 2$. Denote by an $(n, M)_q R$ code a q-ary code of length n, cardinality M, and covering radius R. Let an $[n, n-r]_q R$ code be a q-ary linear code of length n, codimension r, and covering radius R. In the notations $(n, M)_q R$ and $[n, n-r]_q R$ we may omit R. Let $d(x, z)$ be the Hamming distance between vectors x and z. Let $d(x, V)$ be the Hamming distance between a vector x and code V, i.e.,

$$d(x, V) = \min_{v \in V} d(x, v).$$

Denote by $t + V$ the translate of an $(n, M)_q$ code V with the leader $t \in E_q^n$. So $t + V = \{t + v : v \in V\}$. Let $\mathrm{wt}\,(g)$ be the weight of a vector g. Denote by F_q^r the space of r-dimensional q-ary column vectors. Denote by

$$C_1 \times C_2 \times \cdots \times C_t = \{(u_1, u_2, \cdots, u_t) : u_i \in C_i,\ i = \overline{1, t}\}$$

the *direct sum* (DS) of codes $C_1, \cdots, C_t$, $t \geq 2$. Let $\mu_q(n, R, C)$ be the density of the covering of an $(n, M(C))_q R$ code C

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

For an infinite family U consisting of $(n, M(U_n))_q R$ codes U_n [8], [12] we consider the value

$$\overline{\mu}_q(R, U) = \liminf_{n \to \infty} \mu_q(n, R, U_n), \qquad U_n \in U.$$

Let $\mu_q^\bullet(n, R)$ be the least *known* density of the covering of a q-ary code of length n, covering radius R. Denote by $M_q^\bullet(n, R)$ the least *known* cardinality of a q-ary code of length n, covering radius R. Let $r = n - \log_q M$ be redundancy of the $(n, M)_q$ code.

Fact 1: If an $(n, M)_q R$ code exists then an $(n+1, qM)_q R$ code exists.

We give parameters of the best known infinite families A_i of $(n_i, M)_2 3$ codes with $R = 3$, $q = 2$.

A_1: $r = 3t - 2$, $n_1 = 48 \times 2^{t-5} - 1$, $M = 2^{n_1 - 3t + 2}$, $t \geq 8$, $\overline{\mu}_2(3, A_1) \approx 2.25$ [12, form. (4.12)]

A_2: $r = 3t - 1$, $n_2 = 51\frac{3}{8} \times 2^{t-5} - 2$, $M = 2^{n_2 - 3t + 1}$, $t \geq 14$, $\overline{\mu}_2(3, A_2) \approx 1.3744$ [12, form. (1.4)]

A_3: $r = 3t$, $n_3 = 64 \times 2^{t-5} - 1$, $M = 2^{n_3 - 3t}$, $t \geq 4$ is even, $\overline{\mu}_2(3, A_3) \approx 4/3$ [13, Theorem 8]

A_4: $r = 3t$, $n_4 = 76 \times 2^{t-5} - 1$, $M = 2^{n_4 - 3t}$, $t \geq 9$ is odd, $\overline{\mu}_2(3, A_4) \approx 2.23$ [12, form. (4.16)].

We can obtain a code of arbitrary length n using a family A_i and Fact 1. But this new code has the density $\mu_2^\bullet(n, 3)$ greater than codes of the used family A_i, e.g., if the length n increases from $64 \times 2^{t-6} - 1$ to $48 \times 2^{t-5} - 2$, where t is large even, then the density $\mu_2^\bullet(n, 3)$ increases from $4/3$ to $9/2$, see (1). In general, $\mu_2^\bullet(n_i - 1, 3) \approx 2\mu_2^\bullet(n_i, 3)$ for large n_i. Note also that asymptotic optimal $(n', M')_q 1$ codes with arbitrary length n' and

$$\lim_{n' \to \infty} M' = q^{n'}/(1 + (q-1)n')$$

Manuscript received September 26, 1995; revised January 4, 1997. This work was supported in part by the International Science Foundation under Grant UAA000 and by the Russian Basic Research Foundation under Grant 95-01-01331a. The material in this correspondence was presented in part at the Israeli–French Workshop on "Coding and Information Integrity," Tel-Aviv, Israel, December 5–8, 1994, and at the VII Joint Swedish–Russian International Workshop on Information Theory, St.-Pertersburg, Russia, June 18–21, 1995.

The author is with the Institute for Problems of Information Transmission of the Russian Academy of Sciences, GSP-4, Moscow, 101447, Russia.

Publisher Item Identifier S 0018-9448(97)05611-3.

are obtained in [21]. DS of these codes gives codes $\mathcal{D}$ with $\mu_q(n,3,\mathcal{D}) \approx 4.5$ for arbitrary q and arbitrary large n.

To illustrate the new constructions, in Section IV we obtain new infinite families F_i of $(n,M)_2 3$ codes $\mathcal{C}_i$ with the following parameters:

$$F_1\colon R=3,\ q=2,\ r=3t-\log_2 7,\ n=40\frac{1}{2}\times 2^{t-5}-2,$$
$$M=7\times 2^{n-3t}=\frac{7}{8}M_2^\bullet(n,3),\quad t\geq 13,$$
$$\mu_2(n,3,\mathcal{C}_1)=\frac{7}{8}\mu_2^\bullet(n,3),\quad \overline{\mu}_2(3,F_1)\approx 2.7. \tag{2}$$
$$F_2\colon R=3,\ q=2,\ r=3t-2-\log_2\Delta,$$
$$n=\left(46+\frac{2}{\Delta}\right)2^{t-5}-1,\qquad 2>\Delta>1,\quad n \text{ is large},$$
$$M=\Delta\times 2^{n-3t+2}\approx\frac{\Delta}{2}M_2^\bullet(n,3),\quad t>8,$$
$$4.27>\mu_2(n,3,\mathcal{C}_2)\approx\frac{\Delta}{2}\mu_2^\bullet(n,3)>2.25. \tag{3}$$
$$F_3\colon R=3,\ q=2,\ r=3t-1,$$
$$n=50\frac{31}{32}\times 2^{t-5}-1,\quad \text{if } t=\overline{17,20} \text{ and } t\geq 35,$$
$$n=51\times 2^{t-5}-2,\qquad \text{if } t=10,12,14,16,22,24,\cdots,34,$$
$$M=2^{n-3t+1}=\frac{1}{2}M_2^\bullet(n,3),$$
$$\mu_2(n,3,\mathcal{C}_3)=\frac{1}{2}\mu_2^\bullet(n,3),\quad \overline{\mu}_2(3,F_3)\approx 1.3469. \tag{4}$$
$$F_4\colon R=3,\quad q=2,\quad r=3t,$$
$$n=64\times 2^{t-5}+27\times 2^{2\delta+(t-7)/2}-2,$$
$$\delta\equiv(t-1)/2\,(\mathrm{mod}\,2),\qquad \delta\in\{0,1\},$$
$$M=2^{n-3t}=\frac{1}{2}M_2^\bullet(n,3),\quad t\geq 9 \text{ is odd},$$
$$\mu_2(n,3,\mathcal{C}_4)=\frac{1}{2}\mu_2^\bullet(n,3),\quad \overline{\mu}_2(3,F_4)\approx\frac{4}{3}. \tag{5}$$

In (2)–(5) codes with $M_2^\bullet(n,3)$, $\mu_2^\bullet(n,3)$ are obtained by Fact 1 from conventional known families A_i. From (2)–(5) we see that the new families F_i improve coverings in regions of code length of the known families A_1, A_2, A_4. Codes of the family A_3 from [13] have asymptotic density $4/3$ for code length 2^u-1 where u is odd. The obtained family F_4 has the same asymptotical density $4/3$ for code length $2^u+\varepsilon$ where u is even and ε is small compared to 2^u. The family F_2 shows that new constructions can obtain codes in a *region of code length* (for F_2 the region is given by Δ). This new property of the proposed constructions is connected with their nonlinearity and peculiarities of design of Construction A from Section II. Note that the length of the first code of a family obtained by new constructions is usually much greater than 100 or even 1000.

To illustrate a nonbinary application of new constructions, in Section IV we obtain families F_5, F_6 of $(n,M)_3 3$ codes $\mathcal{C}_5,\mathcal{C}_6$ with $R=3$, $q=3$, and the following parameters for $t\geq 9$:

$$F_5\colon n=414\times 3^{t-5}-1,\quad M=3^{n-3t-1}<\frac{1}{2}M_3^\bullet(n,3),$$
$$\mu_3(n,3,\mathcal{C}_5)<\frac{1}{2}\mu_3^\bullet(n,3),\quad \bar{\mu}_3(3,F_5)\approx 2.2. \tag{6}$$
$$F_6\colon n=387\times 3^{t-5}-1,\quad M=5\times 3^{n-3t-2}<\frac{2}{3}M_3^\bullet(n,3),$$
$$\mu_3(n,3,\mathcal{C}_6)<\frac{2}{3}\mu_3^\bullet(n,3),\quad \bar{\mu}_3(3,F_6)<3.0. \tag{7}$$

Here $\mu_3^\bullet(n,3)=4.5$. Codes with $M_3^\bullet(n,3)$, $\mu_3^\bullet(n,3)$ are DS of the codes from [21] for large n. Other known codes with close parameters are the families B_1, B_2 of [8, form. (36), (37)] with

$$r=3t,\ n=321\times 3^{t-5},\ \bar{\mu}_3(3,B_1)\approx 3.074$$

and

$$r=3t+1,\ n=431\times 3^{t-5},\ \bar{\mu}_3(3,B_2)\approx 2.48.$$

For $n=387\times 3^{t-5}-1$, $n=414\times 3^{t-5}-1$, the family B_1 and Fact 1 give density greater than 4.5.

The families F_i illustrate that new constructions can result in codes of smaller cardinality and density than known codes of *the same length*. For an $(n,M)_q 3$ code $\mathcal{C}_i$ we have

$$M=\delta_i M_q^\bullet(n,3),\ \mu_q(n,3,\mathcal{C}_i)=\delta_i\mu_q^\bullet(n,3)$$

with $\delta_1=\frac{7}{8}$, $\delta_2\approx\frac{\Delta}{2}$ if $2>\Delta>1$, $\delta_3=\delta_4=\frac{1}{2}$, $\delta_5<\frac{1}{2}$, $\delta_6<\frac{2}{3}$.

Below all matrices (columns) are q-ary. An element h of GF(q^m) written in a q-ary matrix (column) denotes a column m-dimensional vector that is a q-ary representation of h. We always note the number of *q-ary* rows in a matrix. Let 0^S be a zero matrix (column) with S rows. If $S=0$ then the matrix (column) 0^S is treated as absent. Let GF$^*(q)=$ GF$(q)\backslash\{0\}$. We consider linear combinations of q-ary columns only with *nonzero* q-ary coefficients, i.e., combinations of the form

$$\sum_{u=1}^{Z} a_u f_u$$

where $f_u\in F_q^r$, $a_u\in$ GF$^*(q)$. If the number Z of summands in a linear combination is equal to zero this combination is treated as the zero column. Let T be the symbol of transposition.

Let C be an $[n,n-r]_q$ code with a parity-check matrix H. Denote by $C(\sigma)$ the coset of code C with a syndrome σ of F_q^r, i.e.,

$$C(\sigma)=\{x: x\in E_q^n,\ xH^T=\sigma\}\qquad C(0)=C.$$

Let Σ_p be a set of p syndromes such that

$$\Sigma_p=\{\sigma_1,\cdots,\sigma_p\}\subseteq F_q^r.$$

Denote by $C(\Sigma_p)$ the union of cosets of code C with syndromes of the set Σ_p. We have

$$C(\Sigma_p)=\bigcup_{j=1}^{p}C(\sigma_j).$$

Clearly, $C(\Sigma_p)$ is an $(n,pq^{n-r})_q$ code.

Kabatianskii [20] suggested the following fact.

Fact 2 [20]: Let I_n be the $n\times n$ identity matrix. Let Z_n be the code consisting of the only word $(0\cdots 0)$ of length n. We treat Z_n as the linear $[n,\ n-n]_q$ code with the parity-check matrix I_n. For any $(n(V),M(V))_q$ code V there exist a linear code C_V and a set of syndromes Σ_p such that $V=C_V(\Sigma_p)$. In any case, one may take $C_V=Z_{n(V)}$, $p=M(V)$, $\Sigma_p=\{v_1^T,\cdots,v_{M(V)}^T\}$ where $\{v_1,\cdots,v_{M(V)}\}=V$, v_i is a codeword of V, $i=\overline{1,M(V)}$, i.e., the set Σ_p contains all transposed codewords. If $\Sigma_p=\{0\}$ then $V=C_V$.

Fact 3 gives versions of construction from [1]. Variants and generalizations of this construction obtain covering codes with good parameters, see, e.g., [13], [17], [23], [24], and [28]. In [24, p. 8] it is remarked that the construction of [1] is a generalization of the constructions of [22], see also [23, p. 9]. The situation $C_V=Z_n$ for Fact 3 is noted in [17] and [24].

Fact 3 [1]: Let V be an $(n,pq^{n-r})_q$ code and let $V=C_V(\Sigma_p)$ where

$$\Sigma_p=\{\sigma_1,\cdots,\sigma_p\}\subseteq F_q^r$$

C_V is a linear $[n,n-r]_q$ code with a parity-check matrix H.

i) The covering radius of the code V is the least integer R such that every column $\pi\in F_q^r$ is a sum of some syndrome $\sigma_{i(\pi)}$ of Σ_p with a linear combination of at most R columns of the matrix H.

ii) Let x be a vector of E_q^n with $xH^T = \pi \in F_q^r$. If and only if the column π is a sum of some syndrome $\sigma_{i(\pi)}$ of Σ_p with a linear combination of t distinct columns of H then there exists a codeword w of V with $d(x,w) = t$. Otherwise,

$$w \in G = \{v \in V : vH^T = \sigma_{i(\pi)}\}$$

and

$$d(x,V) \le d(x,G) \le t.$$

Definition 1 [8], [12]: Let V be an $(n,M)_q R$ code of length n, cardinality M, and covering radius R. Let l be an integer, $R \ge l \ge 0$. The code V is called an R,l*-object* of the space E_q^n and is denoted by an $(n,M)_q R,l$ code if for each vector x of E_q^n there exists a word $w(x)$ of V such that $R \ge d(x,w(x)) \ge l$. If $l \ge 1$ then V is also an R,l_1-object with $l_1 = 0,1,\cdots,l-1$.

Remark 1: R,l-objects are a subclass of R^*,l-subsets of [6, p. 321]. A spherical R,l-capsule with center w in E_q^n is the set $\{x : x \in E_q^n, R \ge d(x,w) \ge l\}$ [6, p. 326]. Spherical R,l-capsules centered at vectors of an R,l-object cover the space E_q^n. The goal of this work is to construct codes covering the space E_q^n by *usual* spheres. Spherical R,l-capsules and R,l-objects are useful for it.

Example 1: The set $\{000000, 111000, 000111\}$ is a $(6,3)_2 3,1$ code. The set $\{0000, 1111, 2222, 0011, 2200\}$ is a $(4,5)_3 2,1$ code. Let $\alpha \in \mathrm{GF}(4)$, $\alpha \ne 0,1$. The set $\{000000,\ 111111,\ 000111,\ \alpha\alpha\alpha\alpha\alpha\alpha,\ \alpha^2\alpha^2\alpha^2\alpha^2\alpha^2\alpha^2,\ \alpha\alpha\alpha\alpha^2\alpha^2\alpha^2\}$ is a $(6,6)_4 4,2$ code. See also Section IV.

Definition 2 [8], [12]: Let $D = \{1,\cdots,n\}$ be the set of codeword positions of an $(n,M)_q R,l$ code C of covering radius R. A partition of the set D into nonempty subsets is called an R,l*-partition* if for each vector x of E_q^n there exists a codeword $g(x)$ of C and a vector $e(x)$ of E_q^n such that $x = g(x) + e(x)$, $R \ge wt(e(x)) \ge l$, and all *nonzero* positions of $e(x)$ belong to *distinct* subsets.

Denote by $h(C,l;K)$ the number of subsets in an R,l-partition K for a code C. The value of R is defined by context. For an $(n,M)_q R,l$ code C we have $h(C,l;K) \le n$ and an R,l-partition K is called *trivial* if $h(C,l;K) = n$. The minimal number of subsets in an R,l-partition for a code C is called an R,l*-length* of the code C and is denoted by $h(C,l)$. So, $h(C,l) = \min_K h(C,l;K)$. For linear codes R,l-partitions and R,l-length were introduced in [8] and [12]. For nonlinear codes an "effective length" corresponding to $R,0$-length was considered in [28, suppl., statement 6].

For codes defined as $C(\Sigma_p)$ Definition 3 is equivalent to Definitions 1 and 2.

Definition 3: Let $V = C_V(\Sigma_p)$ be an $(n, pq^{n-r})_q R$ code of covering radius R where C_V is an $[n, n-r]_q$ code with a parity-check matrix H and

$$\Sigma_p = \{\sigma_1, \cdots, \sigma_p\} \subseteq F_q^r.$$

Let l be an integer, $R \ge l \ge 0$.

i) The code V is called an R,l*-object* of the space E_q^n if for each column π of F_q^r (including the zero column) there exist a syndrome $\sigma_{i(\pi)}$ of Σ_p and a linear combination $L(\pi)$ of at least l and at most R distinct columns of the matrix H such that $\pi = \sigma_{i(\pi)} + L(\pi)$.

ii) Let $D = \{1,\cdots,n\}$ be the set of codeword positions of the code V. We also consider D as the set of column labels in the matrix H. A partition of the set D into nonempty subsets is called an R,l*-partition* if for each column π of F_q^r (including the zero column) there exist a syndrome $\sigma_{i(\pi)}$ of Σ_p and a linear combination $L(\pi)$ of at least l and at most R columns of H with labels from *distinct subsets* such that $\pi = \sigma_{i(\pi)} + L(\pi)$.

For i) and ii) if $l = 0$ we can treat the zero column as the linear combination of 0 columns of H.

II. Construction of Covering Codes

We define $mR \times q^m$ matrices $B_m(b)$ with $b \in \mathrm{GF}(q^m) \cup \{\#, *\}$. The value of R is defined by context.

$$B_m(b) = \begin{bmatrix} e_1 & e_2 & \cdots & e_{q^m} \\ be_1 & be_2 & \cdots & be_{q^m} \\ b^2e_1 & b^2e_2 & \cdots & b^2e_{q^m} \\ \vdots & \vdots & \ddots & \vdots \\ b^{R-1}e_1 & b^{R-1}e_2 & \cdots & b^{R-1}e_{q^m} \end{bmatrix}, \quad \text{if } b \in \mathrm{GF}(q^m)$$

$$B_m(\#) = \begin{bmatrix} 0^{m(R-2)} \\ e_1 e_2 \cdots\ e_{q^m} \\ 0^m \end{bmatrix}$$

$$B_m(*) = \begin{bmatrix} 0^{m(R-1)} \\ e_1 e_2 \cdots\ e_{q^m} \end{bmatrix} \tag{8}$$

where $e_j \in \mathrm{GF}(q^m)$, $j = \overline{1,q^m}$; $\{e_1, e_2, \cdots, e_{q^m}\} = \mathrm{GF}(q^m)$, i.e., $e_i \ne e_j$ if $i \ne j$, $i,j \in \{\overline{1,q^m}\}$; 0^{mU} is the zero $mU \times q^m$ matrix. The element b is called an *indicator* of a matrix $B_m(b)$.

Notation 1: Let m be a parameter. We introduce vectors g_ρ and Γ_u and a code $\mathcal{D}_u$. Let $g_\rho = (\rho_1, \cdots, \rho_\gamma)$ where $\rho_j > 0$ is an integer, $j = \overline{1,\gamma}$

$$\sum_{j=1}^{\gamma} \rho_j = \rho.$$

We denote $Q_j = q^{m\rho_j}$, $j = \overline{1,\gamma}$

$$Q = q^{m\rho} = \prod_{j=1}^{\gamma} Q_j.$$

Let $\mathcal{A}_j^v$ be a translate of an $(N_j, M_j)_q \rho_j$ code $\mathcal{A}_j$ of covering radius ρ_j so that $\mathcal{A}_j^v = t_v + \mathcal{A}_j$, $t_v \in E_q^{N_j}$, $v = \overline{1,Q_j}$, $j = \overline{1,\gamma}$. Let

$$\bigcup_{v=1}^{Q_j} \mathcal{A}_j^v = E_q^{N_j}, \qquad j = \overline{1,\gamma}$$

i.e., the union of Q_j translates $\mathcal{A}_j^v$ is the whole space $E_q^{N_j}$. It is possible that translates $\mathcal{A}_j^1, \cdots, \mathcal{A}_j^{Q_j}$ are not disjoint. If all translates $\mathcal{A}_j^v$, $v = \overline{1,Q_j}$, are disjoint then $\mathcal{A}_j$ is a code with redundancy $m\rho_j$ and $M_j = q^{N_j - m\rho_j}$. We have such situation, e.g., when $\mathcal{A}_j$ is a linear $[N_j,\ N_j - m\rho_j]_q \rho_j$ code and the translates are its *cosets*.

Let $\xi_w^{(j)}$ be the wth element of the field $\mathrm{GF}(Q_j)$, i.e.,

$$\mathrm{GF}(Q_j) = \{\xi_1^{(j)}, \cdots, \xi_{Q_j}^{(j)}\}.$$

There exist Q *distinct* vectors $(w_1 \cdots w_\gamma)$ with $w_j \in \{\overline{1,Q_j}\}$. We number these vectors in arbitrary order and denote by

$$W_u = (w_1(u) \cdots w_\gamma(u))$$

the uth vector with $w_j(u) \in \{\overline{1,Q_j}\}$, $j = \overline{1,\gamma}$, $u = \overline{1,Q}$, $W_u \ne W_k$ if $u \ne k$. Let

$$\Gamma_u = [\xi_{w_1(u)}^{(1)} \xi_{w_2(u)}^{(2)} \cdots \xi_{w_\gamma(u)}^{(\gamma)}]^T, \qquad u = \overline{1,Q}.$$

Then $\Gamma_u \ne \Gamma_k$ if $u \ne k$, $F_q^{m\rho} = \{\Gamma_1, \cdots, \Gamma_Q\}$. Let

$$\mathcal{D}_u = \mathcal{A}_1^{w_1(u)} \times \mathcal{A}_2^{w_2(u)} \times \cdots \times \mathcal{A}_\gamma^{w_\gamma(u)}$$

be DS of translates. Then $\mathcal{D}_u$ is an $(N, \overline{M})_q \rho$ code with

$$N = \sum_{j=1}^{\gamma} N_j, \quad \overline{M} = \prod_{j=1}^{\gamma} M_j, \quad \bigcup_{u=1}^{Q} \mathcal{D}_u = E_q^N$$
$$\overline{M} = q^{N - m\rho}, \qquad \text{if } M_j = q^{N_j - m\rho_j}, \ \ j = \overline{1,\gamma}. \tag{9}$$

Construction A: Let

$$V_0 = C_{V_0}(\Sigma_p^0)$$

be a *starting* $(n_0, pq^{n_0-r_0})_q R, l_0$ code of length n_0, cardinality $pq^{n_0-r_0}$, and covering radius R, where

$$\Sigma_p^0 = \{\sigma_1, \cdots, \sigma_p\} \subseteq F_q^{r_0}$$

and C_{V_0} is an $[n_0, n_0 - r_0]_q$ code with a parity-check matrix $H_0 = [f_1 \cdots f_{n_0}]$, $f_\kappa \in F_q^{r_0}$, $\kappa = \overline{1, n_0}$. Let K_0 be an R, l_0-partition for the starting code V_0. We denote $h_0 = h(V_0, l_0; K_0)$. Let m, Λ be parameters, $\Lambda \in \{\overline{0, R}\}$. We set $\rho = R - \Lambda$, $Q = q^{m\rho}$, and use Notation 1. We form a *new* code V by *two steps*.

1) We form an *auxiliary* $(n_1, pQq^{n_1-r_1})_q R_1$ code V_1 of length n_1, cardinality $pQq^{n_1-r_1}$, and covering radius R_1, where $V_1 = C_{V_1}(\Sigma_\Pi^1)$, $n_1 = n_0 q^m$, $r_1 = r_0 + mR$, $\Pi = pQ$, $\Sigma_\Pi^1 = \bigcup_{i=1}^p \bigcup_{u=1}^Q \{\delta_u^{(i)}\} \subseteq F_q^{r_1}$,

$$\delta_u^{(i)} = \begin{bmatrix} \sigma_i \\ 0^{m\Lambda} \\ \Gamma_u \end{bmatrix}, \qquad \text{if } 0 < \Lambda < R$$

$$\delta_u^{(i)} = \begin{bmatrix} \sigma_i \\ \Gamma_u \end{bmatrix}, \qquad \text{if } \Lambda = 0$$

$$\delta_u^{(i)} = \begin{bmatrix} \sigma_i \\ 0^{mR} \end{bmatrix}, \qquad \text{if } \Lambda = R,\ \sigma_i \in \Sigma_p^0 \tag{10}$$

$\Gamma_u \in F_q^{m\rho}$, $i = \overline{1, p}$, $u = \overline{1, Q}$, C_{V_1} is an $[n_1, n_1 - r_1]_q$ code with the parity-check matrix Ω

$$\Omega = [\Omega_1 \cdots \Omega_{n_0}]$$
$$\Omega_\kappa = \begin{bmatrix} P(f_\kappa) \\ B_m(b_\kappa) \end{bmatrix}$$
$$P(f_\kappa) = [f_\kappa \cdots f_\kappa], \qquad \kappa = \overline{1, n_0} \tag{11}$$

f_κ is a column of H_0, $P(f_\kappa)$ is an $r_0 \times q^m$ matrix of equal columns f_κ, $\kappa = \overline{1, n_0}$, the assignment of indicators b_i depends on the partition K_0 as follows: if numbers i, j belong to distinct subsets of K_0 then the inequality $b_i \neq b_j$ must be true, if numbers u, t belong to the same subset of K_0 then we are free to assign the equality $b_u = b_t$ or the inequality $b_u \neq b_t$. We denote

$$\beta = \bigcup_{i=1}^{n_0} \{b_i\}.$$

2) We form the *new* $(n_V, M_V)_q R_V, l_V$ code V of length n_V, cardinality M_V, and covering radius R_V. If $\Lambda = R$ then $V = V_1$, $M_V = pq^{n_1-r_1}$. If $\Lambda < R$ we partition words of the auxiliary code V_1 into Q groups G_u so that

$$G_u = \{v \in V_1 : v\Omega^T = \delta_u^{(i)},\ i = \overline{1, p}\}$$

$u = \overline{1, Q}$

$$\bigcup_{u=1}^{Q} G_u = V_1.$$

We choose a vector $g_\rho = (\rho_1, \cdots, \rho_\gamma)$, $(N_j, M_j)_q \rho_j$ codes $\mathcal{A}_j$, and translates $\mathcal{A}_j^v$ for $v = \overline{1, Q_j}$, $Q_j = q^{m\rho_j}$, $j = \overline{1, \gamma}$, and put

$$V = \bigcup_{u=1}^{Q} \mathcal{D}_u \times G_u, \quad n_V = N + n_0 q^m$$
$$M_V = \overline{M} pQq^{n_1-r_1} = \overline{M} pq^{n_0 q^m - r_0 - m\Lambda} \tag{12}$$

where

$$\sum_{j=1}^{\gamma} \rho_j = \rho, \quad N = \sum_{j=1}^{\gamma} N_j, \quad \overline{M} = \prod_{j=1}^{\gamma} M_j$$
$$M_V = pq^{n_V - r_1} = pq^{N + n_0 q^m - r_0 - mR}, \qquad \text{if } \overline{M} = q^{N - m\rho}.$$

Lemma 1: In Construction A for covering radii of codes V, V_1, and V_0 it holds that $R_V \geq R_1 \geq R$.

Proof: Let $Z < R$. By Fact 3i), there exists a column $\pi \in F_q^{r_0}$ that cannot be represented by a sum of a syndrome $\sigma_j \in \Sigma_p^0$ and a linear combination of Z columns of H_0. We take this π and an arbitrary $\lambda \in F_q^{mR}$. Then, by (10) and (11), the column $[\pi \lambda]^T \in F_q^{r_1}$ cannot be represented by a sum of a syndrome $\delta_u^{(j)} \in \Sigma_\Pi^1$ and a linear combination of Z columns of Ω. So, $R_1 \geq R$. Finally, by (12), $R_V \geq R_1$. □

Examples of Conditions Sufficient for the Equality $R_V = R$ in Construction A (always $\rho = R - \Lambda$):

1) $R \geq 2$, $l_0 = 0$, $\Lambda = 0$, $\beta \subseteq \mathrm{GF}(q^m) \cup \{*\}$, $q^m + 1 \geq h_0$, $g_\rho = (1, \cdots, 1)$, $\quad q \geq 2$.
2) $R \geq 2$, $l_0 = 0$, $\Lambda = 0$, $\beta \subseteq \mathrm{GF}(q^m) \backslash \{0\}$, $q^m - 1 \geq h_0$, $g_\rho = (1, \cdots, 1, \lceil \frac{R}{2} \rceil)$, $\quad q \geq 2$.
3) $R \geq 2$, $l_0 \geq 1$, $\Lambda = l_0$, $\beta \subseteq \mathrm{GF}(q^m)$, $q^m \geq h_0$, $g_\rho = (1, \cdots, 1)$, $\quad q \geq 2$.
4) $R \geq 2$, $l_0 = R$, $\Lambda = R$, $\beta \subseteq \mathrm{GF}(q^m) \cup \{*\}$, $q^m + 1 \geq h_0$, $q \geq 2$.
5) $R \geq 2$, $l_0 = 0$, $\Lambda = 1$, $\beta = \mathrm{GF}(q^m)$, $n_0 \geq q^m \geq h_0$, $g_\rho = (1, \cdots, 1)$, $\quad q \geq 2$.
6) $R = 3$, $l_0 = 0$, $\Lambda = 2$, $\beta = \mathrm{GF}(q^m) \cup \{\#\}$, $n_0 \geq q^m + 1 \geq h_0$, $g_\rho = (1)$, $q = 2^t$, $\quad t \geq 1$.

Comment 1: Under Conditions 1)–4) the parameter m does not have an upper bound. So, we have an *infinite family* of the *new codes* V. Under Conditions 5) and 6), an infinite family can be obtained by an iteration using Construction A, see Examples 3 and 5. Under Conditions 5) and 6), we *must* use *all* elements of $\mathrm{GF}(q^m)$ or $\mathrm{GF}(q^m) \cup \{\#\}$ as indicators b_i. Conditions 5) and 6) are constructions with a *complete set of indicators*. For all conditions, the parameter m is bounded from below. The inequality $q^m + 1 \geq h_0$ is better than $q^m \geq h_0$ or $q^m - 1 \geq h_0$ in respect to restrictions for m. These *inequalities permit us to assign distinct indicators* $b_i \neq b_k$ if the numbers i, k belong to distinct subsets of K_0. Besides, we want to decrease the density of the covering $\mu_q(n_V, R, V)$ of the new code V. For the case $M_V = pq^{n_V - r_1}$ for fixed r_1 we should reduce the length n_V of V, see (1). Increasing Λ causes reduction of N and n_V. Conditions 1)–4) give $\Lambda = l_0$, Conditions 5) and 6) give $\Lambda = l_0 + 1$, $\Lambda = l_0 + 2$. If $\Lambda = R$ then $N = 0$. For decreasing of N and n_V vector $g_\rho = (1, \cdots, 1, \lceil R/2 \rceil)$ is preferential to $g_\rho = (1, \cdots, 1)$.

Theorem 1: If any of Conditions 1)–6) holds then the new code V obtained by Construction A has the same covering radius as the starting code V_0, i.e., $R_V = R$. Besides, $l_V \geq l_0$ for all Conditions 1)–6).

Proof: By Lemma 1, it is sufficient to prove that $R_V \leq R$. It means that $d((c\phi), V) \leq R$, where $(c\phi)$ is an arbitrary vector of $E_q^{n_V}$, $\phi \in E_q^{n_1}$, $c = (c_1 \cdots c_\gamma) \in E_q^N$, $c_j \in E_q^{N_j}$, $j = \overline{1, \gamma}$. We have

$$\phi \Omega^T = \begin{bmatrix} \pi \\ \lambda \end{bmatrix} \in F_q^{r_1}, \quad \pi \in F_q^{r_0}, \quad \lambda = \begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_R \end{bmatrix} \in F_q^{mR},$$
$$\lambda_i \in F_q^m, \quad i = \overline{1, R}. \tag{13}$$

We consider Condition 1 with $\Lambda = l_0 = 0$, $\gamma = \rho = R$, $\rho_j = 1$, $Q_j = q^m$, $j = \overline{1, R}$. By Definition 3, we can find a syndrome $\sigma_{i(\pi)}$, an index collection $J = \{j_1, \cdots, j_Z\}$, and coefficients a_k such that

$$\pi = \sigma_{i(\pi)} + \sum_{k=1}^{Z} a_k f_{j_k}, \quad \sigma_{i(\pi)} \in \Sigma_p^0, \quad R \geq Z \geq l_0, \qquad a_k \in \mathrm{GF}^*(q), \quad k = \overline{1, Z} \tag{14}$$

where f_{j_k} are columns of the matrix H_0, all numbers j_k of columns f_{j_k} belong to *distinct subsets* of the partition K_0. Then $b_{j_y} \neq b_{j_k}$ if $y, k \in \{\overline{1, Z}\}$, $y \neq k$, see the assignment of indicators b_i in (11).

Let $c_i \in E_q^{N_i}$. Denote by $\Psi_i(c_i)$ the least integer such that $c_i \in \mathcal{A}_i^{\Psi_i(c_i)}$, see Notation 1. We take the *least* integer for definiteness. Let $t_{j\mu}$ be the μth column of the submatrix $B_m(b_j)$ in (11).

Let $R > Z \geq 1$. For the index collection J we will find columns $t_{j_k \mu_k}$ and a vector Γ_X such that

$$\begin{bmatrix} \pi \\ \lambda \end{bmatrix} = \begin{bmatrix} \sigma_{i(\pi)} \\ \Gamma_X \end{bmatrix} + \sum_{k=1}^{Z} a_k \begin{bmatrix} f_{j_k} \\ t_{j_k \mu_k} \end{bmatrix} \tag{15}$$

where $\sigma_{i(\pi)}$, a_k, j_k, $k = \overline{1, Z}$, are taken from (14), and besides the vector Γ_X must satisfy the relations

$$\xi_{w_i(X)}^{(i)} = \xi_{\Psi_i(c_i)}^{(i)}, \qquad i = \overline{1, Z}. \tag{16}$$

Let $b_{j_k} \neq *$, $k = \overline{1, Z}$. "Locations" e_{μ_k} of columns $t_{j_k \mu_k}$ in (15) are a solution of the system

$$\sum_{k=1}^{Z} a_k e_{\mu_k} b_{j_k}^{i-1} = \lambda_i - \xi_{\Psi_i(c_i)}^{(i)}, \qquad i = \overline{1, Z}, \quad b_{j_y} \neq b_{j_k}, \qquad \text{if } y \neq k. \tag{17}$$

The determinant of the system is not equal to zero since we have the Vandermonde matrix with consecutive degrees of *distinct* elements of GF (q^m). Having obtained e_{μ_k} from (17), we calculate

$$\xi_{w_i(X)}^{(i)} = \lambda_i - \sum_{k=1}^{Z} a_k e_{\mu_k} b_{j_k}^{i-1}, \qquad i = \overline{Z+1, R}. \tag{18}$$

Now the relations (16) and (18) together give the desired vector Γ_X. We have obtained columns $t_{j_k \mu_k}$ and the vector Γ_X simultaneously satisfying (15) and (16). The columns $t_{j_k \mu_k}$ are given by locations e_{μ_k}. By (15), we have the representation of the column $\phi \Omega^T$ of (13) by the sum of the syndrome $\delta_X^{(i(\pi))}$ of Σ_Π^1, see (10), and a linear combination of Z columns of the matrix Ω. By Fact 3ii), $d(\phi, G_X) \leq Z$. The obtained vector Γ_X exactly gives a code $\mathcal{D}_X$, see Notation 1. By (16),

$$c_i \in \mathcal{A}_i^{\Psi_i(c_i)} = \mathcal{A}_i^{w_i(X)}, \qquad i = \overline{1, Z}$$

i.e.,

$$(c_1 c_2 \cdots c_Z) \in \mathcal{A}_1^{w_1(X)} \times \mathcal{A}_2^{w_2(X)} \times \cdots \times \mathcal{A}_Z^{w_Z(X)}.$$

Since $\mathcal{A}_j^v$ is a code with covering radius ρ_j, we have $d(c, \mathcal{D}_X) \leq R - Z$. Finally,

$$\begin{aligned} d((c\phi), V) &\leq d((c\phi), \mathcal{D}_X \times G_X) \\ &= d(c, \mathcal{D}_X) + d(\phi, G_X) \leq (R - Z) + Z = R. \end{aligned}$$

If $Z = R$ then calculations of (18) are not executed

$$d(c, \mathcal{D}_X) = 0 \qquad d((c\phi), V) \leq d(\phi, G_X) \leq R.$$

Let $Z = 0$, $\pi = \sigma_{i(\pi)}$, see (14). We put $\Gamma_X = \lambda$. Then

$$\phi \Omega^T = [\pi \lambda]^T = [\sigma_{i(\pi)} \Gamma_X]^T = \delta_X^{(i(\pi))}, \qquad \phi \in G_X, \quad d((c\phi), V) \leq d(c, \mathcal{D}_X) \leq \gamma = \rho = R.$$

Let $R > Z \geq 2$, $b_{j_Z} = *$. In (16) we put $i = 1, 2, \cdots, Z-1, R$. Hence $c_i \in \mathcal{A}_i^{w_i(X)}$, $i = 1, 2, \cdots, Z-1, R$, and $d(c, \mathcal{D}_X) \leq R - Z$. The system of (17) has the form

$$\begin{aligned} &\sum_{k=1}^{Z-1} a_k e_{\mu_k} b_{j_k}^{i-1} = \lambda_i - \xi_{\Psi_i(c_i)}^{(i)} \\ &i = \overline{1, Z-1}, \quad b_{j_y} \neq b_{j_k}, \qquad \text{if } y \neq k, \\ &\sum_{k=1}^{Z} a_k e_{\mu_k} = \lambda_R - \xi_{\Psi_R(c_R)}^{(R)}. \end{aligned} \tag{19}$$

The determinant of the system of (19) is not equal to zero since we add the column $(0 \cdots 01)^T$ to the Vandermonde matrix. By (19), we obtain e_{μ_k}. Then, instead of (18), we calculate

$$\xi_{w_i(X)}^{(i)} = \lambda_i - \sum_{k=1}^{Z-1} a_k e_{\mu_k} b_{j_k}^{i-1}, \qquad i = \overline{Z, R-1}.$$

So, we obtain Γ_X and $t_{j_k \mu_k}$ for (15). By Fact 3ii), $d(\phi, G_X) \leq Z$. So

$$d((c\phi), V) \leq (R - Z) + Z = R.$$

Other conditions can be considered similarly. We consider some distinctive situations.

Condition 2: We have $\rho_j = 1$, $Q_j = q^m$, $j = \overline{1, \gamma - 1}$, $\rho_\gamma = \lceil R/2 \rceil$, $\gamma = \lfloor R/2 \rfloor + 1$, $\rho = R$. Let $Z \geq 1$, see (14). We denote

$$\xi_{w_\gamma(X)}^{(\gamma)} = (E_{1,X} E_{2,X} \cdots E_{\lceil R/2 \rceil, X}), \quad E_{l,X} \in \mathrm{GF}(q^m), \qquad l = \overline{1, \lceil R/2 \rceil}.$$

If $R - Z \geq \lceil R/2 \rceil$ then we use (15)–(17). Instead of (18) we have

$$\begin{aligned} \xi_{w_i(X)}^{(i)} &= \lambda_i - \sum_{k=1}^{Z} a_k e_{\mu_k} b_{j_k}^{i-1}, \qquad \text{if } i = \overline{Z+1, \gamma - 1} \\ E_{i-\gamma+1, X} &= \lambda_i - \sum_{k=1}^{Z} a_k e_{\mu_k} b_{j_k}^{i-1}, \qquad \text{if } i = \overline{\gamma, R}. \end{aligned} \tag{20}$$

By (20), we obtain $\xi_{w_i(X)}^{(i)}$ for $i = \overline{Z+1, \gamma}$. So

$$d(\phi, G_X) \leq Z, \quad d(c, \mathcal{D}_X) \leq R - Z, \quad d((c\phi), V) \leq R.$$

If $R - Z < \lceil R/2 \rceil$ then in (16) we put $i = \overline{R - Z + 1, \gamma}$. Instead of (17) we solve the system

$$\begin{aligned} &\sum_{k=1}^{Z} a_k e_{\mu_k} b_{j_k}^{i-1} = \lambda_i - \Phi_i, \\ &\Phi_i = \xi_{w_i(X)}^{(i)}, \qquad \text{if } i = \overline{R - Z + 1, \gamma - 1} \\ &\Phi_i = E_{i-\gamma+1, X}, \qquad \text{if } i = \overline{\gamma, R}. \end{aligned} \tag{21}$$

Then we use (18) with $i = \overline{1, R - Z}$, and obtain values of $\xi_{w_i(X)}^{(i)}$ for $i = \overline{1, R - Z}$. By Fact 3ii), $d(\phi, G_X) \leq Z$. By (16) with $i = \overline{R - Z + 1, \gamma}$, we have $d(c, \mathcal{D}_X) \leq R - Z$. So, $d((c\phi), V) \leq R$.

Condition 3: We have $\Lambda = l_0 \geq 1$, $\rho_j = 1$, $Q_j = q^m$, $j = \overline{1, \gamma}$, $\gamma = \rho$. Let $L = Z - \Lambda$, $\rho > L \geq 1$. In (16) we put $i = \overline{1, L}$. Instead of (15), (17), and (18) we use (22)–(24), respectively.

$$\begin{bmatrix} \pi \\ \lambda \end{bmatrix} = \begin{bmatrix} \sigma_{i(\pi)} \\ 0^{m\Lambda} \\ \Gamma_X \end{bmatrix} + \sum_{k=1}^{Z} a_k \begin{bmatrix} f_{j_k} \\ t_{j_k \mu_k} \end{bmatrix}. \tag{22}$$

$$\begin{aligned} &\sum_{k=1}^{Z} a_k e_{\mu_k} b_{j_k}^{i-1} = \lambda_i, \qquad \text{if } i = \overline{1, \Lambda} \\ &\sum_{k=1}^{Z} a_k e_{\mu_k} b_{j_k}^{\Lambda + i - 1} = \lambda_{\Lambda + i} - \xi_{\Psi_i(c_i)}^{(i)}, \qquad \text{if } i = \overline{1, L}. \end{aligned} \tag{23}$$

$$\xi_{w_i(X)}^{(i)} = \lambda_{\Lambda + i} - \sum_{k=1}^{Z} a_k e_{\mu_k} b_{j_k}^{\Lambda + i - 1}, \quad i = \overline{L + 1, \gamma}. \tag{24}$$

Condition 4: We have $V = V_1$, $l_0 = \Lambda = R$, $n_V = n_1$. Instead of $(c\phi)$ we consider a vector ϕ. The relation (14) always holds for $Z = R$. We use (15) with $[\sigma_{i(\pi)}\ 0^{mR}]^T$ instead of $[\sigma_{i(\pi)}\ \Gamma_X]^T$ (see (10)). Put that the right side of the equations of (17) is λ_i, obtain e_{μ_k}, $k = \overline{1, R}$, and show that $d(\phi, V_1) \le R$.

For Conditions 5 and 6, the matrix Ω of (11) always contains a submatrix $B_m(b_\varphi)$ with a calculated indicator b_φ since $\beta = \mathrm{GF}(q^m)$ or $\beta = \mathrm{GF}(q^m) \cup \{\#\}$. For Conditions 5 and 6 we use the relation (22).

Condition 5: Here $\gamma = \rho = R - 1$. Let $\pi = \sigma_{i(\pi)}$, $\lambda_1 \ne 0$. We put $\xi^{(1)}_{w_1(X)} = \xi^{(1)}_{\Psi_1(c_1)}$. Now $c_1 \in \mathcal{A}_1^{w_1(X)}$ and

$$d(c, \mathcal{D}_X) \le \gamma - 1 = R - 2.$$

We calculate $b_\varphi = (\lambda_2 - \xi^{(1)}_{w_1(X)})/\lambda_1$ and put

$$-\xi^{(i)}_{w_i(X)} = \lambda_1 b^i_\varphi - \lambda_{i+1}, \qquad i = \overline{2, \gamma}.$$

So we obtain Γ_X. We have

$$[\pi\lambda]^T = [\sigma_{i(\pi)}\ 0^m\ \Gamma_X]^T + [f_\varphi, \lambda_1, \lambda_1 b_\varphi, \cdots, \lambda_1 b_\varphi^{R-1}]^T - [f_\varphi, 0, \cdots, 0]^T.$$

By Fact 3ii), $d(\phi, G_X) \le 2$. So

$$d((c\phi), \mathcal{D}_X \times G_X) \le (R - 2) + 2 = R.$$

Condition 6: Here $\Gamma_X = \xi^{(1)}_{w_1(X)}$. Let $\pi = \sigma_{i(\pi)} + a_1 f_{j_1}$, see (14). If $b_{j_1} \ne \#$, $\lambda_2 \ne \lambda_1 b_{j_1}$, or $b_{j_1} = \#$, $\lambda_1 \ne 0$, we put $\xi^{(1)}_{w_1(X)} = \xi^{(1)}_{\Psi_1(c_1)}$. Now

$$c_1 \in \mathcal{A}_1^{w_1(X)}, \quad d(c, \mathcal{D}_X) = 0, \quad d((c\phi), V) \le d(\phi, G_X).$$

Let $b_{j_1} \ne \#$, $\lambda_2 \ne \lambda_1 b_{j_1}$, $\lambda_3 + \xi^{(1)}_{w_1(X)} \ne \lambda_1 b^2_{j_1}$. We calculate

$$b_\varphi = (\lambda_3 + \xi^{(1)}_{w_1(X)} + \lambda_2 b_{j_1})/(\lambda_2 + \lambda_1 b_{j_1}) \ne b_{j_1}.$$

We put

$$a_1 t = (\lambda_1 b_\varphi + \lambda_2)/(b_{j_1} + b_\varphi)$$
$$y = (\lambda_1 b_{j_1} + \lambda_2)/(b_{j_1} + b_\varphi).$$

Then

$$[\pi\lambda]^T = \delta_X^{(i(\pi))} + a_1[f_{j_1}, t, t b_{j_1}, t b^2_{j_1}]^T + [f_\varphi, y, y b_\varphi, y b^2_\varphi]^T + [f_\varphi, 0, 0, 0]^T.$$

By Fact 3ii), $d(\phi, G_X) \le 3$.

Let $b_{j_1} \ne \#$, $\lambda_2 \ne \lambda_1 b_{j_1}$, $\lambda_3 + \xi^{(1)}_{w_1(X)} = \lambda_1 b^2_{j_1}$. We take $b_\varphi = \#$, $a_1 W = \lambda_1$. Then

$$[\pi\lambda]^T = \delta_X^{(i(\pi))} + a_1[f_{j_1}, W, W b_{j_1}, W b^2_{j_1}]^T + [f_\varphi, 0, \lambda_2 + \lambda_1 b_{j_1}, 0]^T + [f_\varphi, 0, 0, 0]^T.$$

Again $d(\phi, G_X) \le 3$.

Let $b_{j_1} = \#$, $\lambda_1 \ne 0$. For $q = 2^t$ we always can calculate $b_\varphi = ((\lambda_3 + \xi^{(1)}_{w_1(X)})/\lambda_1)^{1/2}$. Then

$$[\pi\lambda]^T = \delta_X^{(i(\pi))} + a_1[f_{j_1}, 0, a_1^{-1}(\lambda_2 + \lambda_1 b_\varphi), 0]^T + [f_\varphi, \lambda_1, \lambda_1 b_\varphi, \lambda_1 b^2_\varphi]^T + [f_\varphi, 0, 0, 0]^T, \quad d(\phi, G_X) \le 3.$$

Now we use the fact that $c = (c_1)$, $d(c, \mathcal{D}_X) \le 1$. If $b_{j_1} = \#$, $\lambda_1 = 0$, we put $\xi^{(1)}_{w_1(X)} = \lambda_3$. Then

$$[\pi\lambda]^T = \delta_X^{(i(\pi))} + a_1[f_{j_1}, 0, \lambda_2 a_1^{-1}, 0]^T, \qquad d(\phi, G_X) \le 1, \quad d((c\phi), V) \le 2.$$

If $b_{j_1} \ne \#$, $\lambda_2 = \lambda_1 b_{j_1}$, we take $\xi^{(1)}_{w_1(X)} = \lambda_3 + \lambda_1 b^2_{j_1}$, $a_1 W = \lambda_1$. Then

$$[\pi\lambda]^T = \delta_X^{(i(\pi))} + a_1[f_{j_1}, W, W b_{j_1}, W b^2_{j_1}]^T, \qquad d((c\phi), V) \le 2.$$

Now let $\pi = \sigma_{i(\pi)}$, $\lambda_1 \ne 0$. We calculate $b_\varphi = \lambda_2/\lambda_1$ and take $\xi^{(1)}_{w_1(X)} = \lambda_3 + \lambda_1 b^2_\varphi$. Then

$$[\pi\lambda]^T = \delta_X^{(i(\pi))} + [f_\varphi, \lambda_1, \lambda_1 b_\varphi, \lambda_1 b^2_\varphi]^T + [f_\varphi, 0, 0, 0]^T, \qquad d(\phi, G_X) \le 2, \quad d((c\phi), V) \le 3.$$

Finally we consider values of l_V. Clearly, $l_V \ge l_0$ if $l_0 = 0$. For Conditions 3 and 4 we have $Z \ge l_0$ in (14) and (15). By Fact 3ii), there is a codeword w of V_1 with $d(\phi, w) = Z \ge l_0$. So, $l_V \ge l_0$. □

Comment 2: From the proof one can see the following. Let $(c\phi) \in E_q^{n_V}$ where ϕ is an arbitrary vector of $E_q^{n_1}$, $c = (c_1 \cdots c_\gamma) \in E_q^N$, $c_j \in E_q^{N_j}$, $j = \overline{1, \gamma}$. For Conditions 1–4 there exists a value Z such that $R \ge Z \ge l_0 = \Lambda$ and at least $q^{Z-\Lambda}$ distinct groups G_X have the following property: each group G_X contains a word $r_X(\phi)$ with $d(\phi, r_X(\phi)) = Z$ (and hence $d(\phi, G_X) \le Z$). The value Z depends on ϕ, see (13) and (14). Nonzero positions of the vector $\phi - r_X(\phi)$ can be given by locations of Z columns $t_{j_k \mu_k}$ in the matrix (11), see (15), (22), and Fact 3ii). If $Z = \Lambda$ then there is only one such group G_X. Condition 4 always implies $Z = \Lambda$. If $Z > \Lambda$ the groups G_X can be given by vectors Γ_X in which, e.g., the following *components* $\xi^{(i)}_{w_i(X)}$ *can be chosen arbitrarily*: $i = \overline{1, Z - \Lambda}$ for Condition 1 with $b_{j_k} \ne *$, Condition 2 with $R - Z \ge \lceil R/2 \rceil$, and Condition 3; $i = 1, 2, \cdots, Z - 1, R$ for Condition 1 with $Z \ge 2$, $b_{j_Z} = *$; $i = \overline{R - Z + 1, \gamma}$ for Condition 2 with $R - Z < \lceil R/2 \rceil$; etc. It is naturally to put for these "free" components $\xi^{(i)}_{w_i(X)} = \xi^{(i)}_{\Psi_i(c_i)}$, see (16) and changes of values of i in (16) for distinct Conditions. Now $c_i \in \mathcal{A}_i^{w_i(X)}$, $d(c, \mathcal{D}_X) \le R - Z$, and

$$d((c\phi), \mathcal{D}_X \times G_X) \le (R - Z) + Z = R.$$

Locations of columns $t_{j_k \mu_k}$ providing the equality $\xi^{(i)}_{w_i(X)} = \xi^{(i)}_{\Psi_i(c_i)}$ are values of e_{μ_k} obtained from the systems in (17), (19), (21), and (23).

For Conditions 5 and 6 we have $\Lambda > l_0$ and it is possible in (14) that $\Lambda > Z \ge l_0$. Then we calculate b_φ and find a desired group G_X using the equalities $\beta = \mathrm{GF}(q^m)$ or $\beta = \mathrm{GF}(q^m) \cup \{\#\}$. Again, for some $Z' > Z$ we have $d(\phi, G_X) \le Z'$, $d(c, \mathcal{D}_X) \le R - Z'$. Note that Condition 6 is connected with an oval of $q^m + 2$ points in a projective plane $\mathrm{PG}(2, q^m)$, $q = 2^t$ [26].

By structure, the construction

$$V = \bigcup_{u=1}^{Q} \mathcal{D}_u \times G_u$$

is similar to the blockwise direct sum (BDS) construction [16], [28]. But the approaches to calculation of covering radius are distinct. For the BDS construction, the radius is connected with the values $\min_u d(c, \mathcal{D}_u) + \max_u d(c, \mathcal{D}_u)$ and $\min_u d(\phi, G_u) + \max_u d(\phi, G_u)$ whenever, for Construction A, the radius is estimated with the help of the relation $(R - Z) + Z$, see above.

III. Modification of Construction

Construction B: Let

$$V_0 = C_{V_0}(\Sigma^0_p)$$

be a *starting* $(n_0, pq^{n_0 - r_0})_q R, l_0$ code of covering radius R where

$$\Sigma^0_p = \{\sigma_1, \cdots, \sigma_p\} \subseteq F_q^{r_0}$$

C_{V_0} is an $[n_0, n_0 - r_0]_q$ code with a parity-check matrix

$$H_0 = [f_1 \cdots f_{n_0}], \qquad f_\kappa \in F_q^{r_0},\ \kappa = \overline{1, n_0}.$$

Let K_0 be an R, l_0-partition for the code V_0. We denote $h_0 = h(V_0, l_0; K_0)$. We form a *new* $(n_V, M_V)_q R_V, l_V$ code V of covering radius R_V where $V = C_V(\Sigma_p^V)$, $R_V \geq R$, $n_V = n_0q^m + N^{(\varepsilon)}$, $M_V = pq^{n_V - r_1}$, $r_1 = r_0 + mR$, $\Sigma_p^V = \{\delta'_1, \cdots, \delta'_p\}$, $\delta'_i = [\sigma_i \ 0^{mR}]^T \in F_q^{r_1}$, $\sigma_i \in \Sigma_p^0$, $i = \overline{1,p}$, m is a parameter, C_V is an $[n_V, n_V - r_1]_q$ code with a parity-check matrix H_V such that

$$H_V = [\Psi \ \Omega], \quad \Psi = \begin{bmatrix} 0^{r_0} \\ D_m^{(\varepsilon)} \end{bmatrix}, \quad \Omega = [\Omega_1 \cdots \Omega_{n_0}],$$
$$\Omega_\kappa = \begin{bmatrix} P(f_\kappa) \\ B_m(b_\kappa) \end{bmatrix}, \qquad \kappa = \overline{1, n_0} \quad (25)$$

the index ε remarks a variant of a matrix, $D_m^{(\varepsilon)}$ is an $mR \times N^{(\varepsilon)}$ matrix, the value of $N^{(\varepsilon)}$ depends on a form of the matrix $D_m^{(\varepsilon)}$, the matrices Ω, Ω_κ, $P(f_\kappa)$, and $B_m(b_\kappa)$ are defined by Construction A.

Example 2: We consider Construction B with $\varepsilon = 1$. Let $\Lambda \in \{\overline{0, R}\}$ be a parameter, and let

$$D_m^{(1)} = \begin{bmatrix} 0^{m(R-\rho)} & 0^{m(R-\rho)} & \cdots & 0^{m(R-\rho)} \\ \Xi_1 & 0^{m\rho_1} & \cdots & 0^{m\rho_1} \\ 0^{m\rho_2} & \Xi_2 & \cdots & 0^{m\rho_2} \\ \vdots & \vdots & \ddots & \vdots \\ 0^{m\rho_\gamma} & 0^{m\rho_\gamma} & \cdots & \Xi_\gamma \end{bmatrix},$$
$$(\rho_1, \cdots, \rho_\gamma) = g_\rho, \quad \sum_{j=1}^{\gamma} \rho_j = \rho, \quad \rho = R - \Lambda \quad (26)$$

where a vector g_ρ is defined in Notation 1, Ξ_j is a parity-check matrix of an $[N_j, N_j - m\rho_j]_q\rho_j$ code $\mathcal{A}_j$ with covering radius ρ_j

$$N^{(1)} = \sum_{j=1}^{\gamma} N_j$$

the submatrix Ψ in (25) is absent for $\Lambda = R$.

Using Notation 1 it can be shown that Construction B with $\varepsilon = 1$ is a variant of Construction A when *each* translate $\mathcal{A}_j^v$ is a *coset* of a *linear* code $\mathcal{A}_j$, $j = \overline{1, \gamma}$. Let (αg) be a codeword of the new code V of Construction A, i.e.,

$$(\alpha g) \in \mathcal{D}_u \times G_u, \qquad u \in \{\overline{1, Q}\},$$
$$\alpha = (\alpha_1 \cdots \alpha_\gamma) \in \mathcal{D}_u, \ g \in G_u, \ \alpha_j \in \mathcal{A}_j^{w_j(u)}, \ j = \overline{1, \gamma}.$$

Then $g\Omega^T = \delta_u^{(i)} = [\sigma_i \ 0^{m\Lambda} \ \Gamma_u]^T$, $\Gamma_u = [\xi_{w_1(u)}^{(1)} \cdots \xi_{w_\gamma(u)}^{(\gamma)}]^T$, see (10) and (11). Now we number cosets of an $[N_j, N_j - m\rho_j]_q\rho_j$ code $\mathcal{A}_j$ with a parity-check matrix Ξ_j in an order connected with numbering of elements of GF(Q_j). We put

$$\mathcal{A}_j^{w_j(u)} = \{e \in E_q^{N_j} : e\Xi_j^T = -\xi_{w_j(u)}^{(j)}\}, \qquad j = \overline{1, \gamma}, \ u = \overline{1, Q}.$$

Then

$$\alpha\Psi^T = [0^{r_0 + m\Lambda}, -\xi_{w_1(u)}^{(1)}, \cdots, -\xi_{w_\gamma(u)}^{(\gamma)}]^T.$$

Hence

$$(\alpha g)H_V^T = \alpha\Psi^T + g\Omega^T = [\sigma_i \ 0^{mR}]^T.$$

So, (αg) is also a codeword of the new code V of Construction B. Conditions 1–6 of Construction A are also sufficient for the equality $R_V = R$ in Construction B with $\varepsilon = 1$.

Construction B can be useful for estimates of l_V and $h(V, l_V)$ using Definition 3. Besides, in order to improve parameters of the new code V we can use special matrices $D_m^{(\varepsilon)}$ similar to corresponding matrices of linear constructions of [6]–[8], [11], and [12], see, e.g., [10, Example 1].

Remark 2: In [28, suppl., Statements 5–7] Struik briefly considered a nonlinear generalization of linear q^m-concatenating constructions of [6], [7], and [12]. This generalization uses n-arcs in a projective geometry. The construction of [28] is close and obtains codes with the same parameters as Construction B of this work in which a starting code is an $R, 0$-object, the vector g_ρ is $(1, \cdots, 1)$, and K_0 is an $R, 0$-partition. But the construction of [28] does not allow to improve parameters of new codes by using R, l-objects and R, l-partitions with $l \geq 1$ and by using parity check matrices of codes with $\rho_i \geq 2$ for design of matrices $D_m^{(\varepsilon)}$. Besides, in the construction of [28] one cannot use translates of nonlinear codes for design of codes $\mathcal{D}_u$, i.e., the construction of [28] is not close to Construction A of this work. Note also that in [28, suppl., Statement 6] ideas connected with a complete set of indicators are used only for $R = 2$ whereas Condition 5 allows to put $R \geq 2$ and Condition 6 is effective for $R = 3$, see Examples 3 and 5. It can be remarked that constructions of this work allow to design codes in a region of the code length, see Example 6. Therefore, new codes obtained by constructions of this work usually have better parameters than codes designed by the construction of [28].

Note that connections between matrices $B_m(b)$, H, Ψ of linear q^m-concatenating constructions and a projective geometry are considered in [6], and [12, Remark 5.1]. In [6, Remark 2, p. 326], e.g., it is noted that a parity-check matrix of a maximum-distance-separable (MDS) code can be used to design the matrix H. (Linear MDS codes and n-arcs are equivalent objects [27].)

IV. Families of Covering Codes

Remark 3: By Fact 2, we can treat an $(n_0, pq^{n_0 - r_0})_q R, l_0$ code V_0 as $V_0^* = C_{V_0^*}(\Sigma_{p^*}^0)$ code where V_0^* is an $(n_0, p^*q^{n_0 - r_0^*})_q R, l_0$ code, $p^* = pq^{n_0 - r_0}$, $r_0^* = n_0$, $C_{V_0^*} = Z_{n_0}$, $\Sigma_{p^*}^0$ is the set of transposed codewords of V_0. Then Construction A with $\overline{M} = q^{N - m\rho}$ gives $n_V = N + n_0q^m$, $M_V = p^*q^{n_V - r_1^*} = pq^{n_V - r_1}$ where $r_1^* = r_0^* + mR = n_0 + mR$, $r_1 = r_0 + mR$. That is why we often do not remark a code C_{V_0}.

Below, excepting Example 6, we consider and use Construction A with $M_j = q^{N_j - m\rho_j}$, $j = \overline{1, \gamma}$, $\overline{M} = q^{N - m\rho}$, see (9) and (12). If $\rho_j = 1$ then $\mathcal{A}_j$ is the $[\varphi_{m,q}, \varphi_{m,q} - m]_q1$ Hamming code where

$$\varphi_{m,q} = (q^m - 1)/(q - 1).$$

Usually, $\rho_1 = 1$ and $\mathcal{A}_1$ is the Hamming code. For each codeword $x_1 \in \mathcal{A}_1$ there exists a codeword $x_2 \in \mathcal{A}_1$ with $d(x_1, x_2) = 3$, $x_1 + a^\star = x_2$, where $a^\star \in \mathcal{A}_1$, wt$(a^\star) = 3$. Each coset of $\mathcal{A}_1$ also has this property. Hence for each codeword y_1 of the new code V there exists a codeword $y_2 \in V$ with $d(y_1, y_2) = 3$, $y_1 + \bar{a} = y_2$, $\bar{a} = (a^\star, 0, \cdots, 0) \in E_q^{n_V}$. So, $l_V \geq 1$ for $R \geq 3$.

We construct an $R, 1$-partition $K^{(1)}$ for the code V with $R \geq 3$. If nonzero positions of $a^\star$ are 1, 2, 3, we partition the positions $1, \cdots, \varphi_{m,q}$ corresponding to translates $\mathcal{A}_1^v$ into subsets $\{1\}, \{2\}, \{\overline{3, \varphi_{m,q}}\}$. Each code $\mathcal{A}_j$ has a $\rho_j, 0$-partition K_j with $h(\mathcal{A}_j, 0; K_j) = \eta_j$. K_j is also a $\rho_j, 0$-partition for each translate $\mathcal{A}_j^v$. If $\rho_j = 1$ then $\eta_j = 1$. We use $K_2, \cdots, K_\gamma$ to partition the positions $\varphi_{m,q} + 1, \cdots, N$ corresponding to translates $\mathcal{A}_2^v, \cdots, \mathcal{A}_\gamma^v$ into $\sum_{j=2}^{\gamma} \eta_j$ subsets. By Proof of Theorem 1, for Conditions 1 and 2, two columns from the same submatrix Ω_κ do not occur in a representation of the column $[\pi\lambda]^T$, see (15). Hence, taking into account Fact 3ii), we can partition the positions $N + 1, \cdots, n_V$ of the code V into $|\beta|$ subsets such that each subset consists of *all* column labels of *all* submatrices Ω_κ from (11) having the same indicator $b_\kappa \in \beta$. Here $|X|$ is the cardinality of a set X. We can put $|\beta| = h_0$. Besides, we may also treat V as an $(n_V, M_V)_q R, 0$

code, see Definition 1. Clearly, $h(V,0) \leq h(V,1)$. So

$$h(V,0) \leq h(V,1) \leq 3 + \sum_{j=2}^{\gamma} \eta_j + h_0 = \gamma + 1 + \eta_\gamma + h_0,$$
$$\text{for Conditions 1 and 2 with } R \geq 3, \quad |\beta| = h_0. \quad (27)$$

Example 3: $R = 3,\ q = 2$. We obtain codes with the help of an iterative process when a new code is a starting code on the next step. $V_0 = C_{V_0}(\Sigma_p^0)$ is the $(n_0, 2^{n_0 - r_0})_2 3$ code with $n_0 = 23$, $r_0 = 11$, $p = 1$, $\Sigma_p^0 = \{0\}$. C_{V_0} is the $[23, 12]_2 3$ Golay code. So, $V_0 = C_{V_0}$, see Fact 2. We use the trivial $3, 0$-partition K_0 with $h_0 = 23$ and Condition 2 with $g_3 = (1, 2)$, $2^m - 1 \geq 23$. We take *even* $m \geq 6$, $n_1 = 23 \times 2^m$, $r_1 = 11 + 3m$. Let $\mathcal{A}_2$ be the $(n, 2^{n-2m})_2 2$ code $P(m)$ of [13, Theorems 4, 5] with $n = 1.5 \times 2^m - 1$. Then $N = 2.5 \times 2^m - 2$, $n_V = 25.5 \times 2^m - 2$, $M_V = 2^{n_V - (11+3m)}$, see (12). For $m = 6$ we have a $(1630, 2^{1630-29})_2 3, 1$ code V' with

$$h(V', 0) \leq h(V', 1) \leq 2 + 1 + (1.5 \times 2^6 - 1) + 23 = 121$$

see (27). We treat V' as a $(1630, 2^{1630-29})_2 3, 0$ code and use it as V_0 for Condition 6 with $1630 \geq 2^m + 1 \geq 121$, $m = \overline{7, 10}$. For $m = 7$ we have an $(n_D, 2^{n_D - 50})_2 3, l_D$ code D with $n_D = 1631 \times 2^7 - 1$. As usual, $\mathcal{A}_1$ is the Hamming code. Hence $l_D \geq 1$. It can be shown that actually $l_D \geq 2$, i.e., if $x \in E_2^{n_D}$, $w \in D$, $d(x, w) = 1$, then there exists a codeword $u \in D$ with $2 \leq d(x, u) \leq 3$. Existence of the word u follows from Fact 3ii) and the facts that for $q = 2, m \geq 2$, each column of a parity-check matrix of the Hamming code is a sum of two other columns and each column of the submatrix Ω_κ of (11) is a sum of three other columns. Now we use the trivial partition K_0 and take D as V_0 for Condition 3 with $\Lambda = 2$, $2^m \geq n_D$. We obtain the family F_3 of (4).

Example 4: $R = 3, q = 2$. V_0 is the $(n_0, 2^{n_0 - 3v})_2 3$ code $D(v)$ of the family A_3 [13, Theorem 8], where $n_0 = 2^{v+1} - 1$, $v \geq 4$ is even. We use the trivial $3, 0$-partition K_0 with $h_0 = n_0$ and Condition 2 with $\rho = 3$, $g_3 = (1, 2)$, $2^m \geq 2^{v+1}$. We take *odd* $m = v + 1,\ v + 3$ and obtain *two* new codes V from *every* code $D(v)$, see Remark 3. Let $\mathcal{A}_2$ be the $[N_2, N_2 - 2m]_2 2$ code of [12, eq. (1.3)] with $N_2 = 27 \times 2^{m-4} - 1$. We obtain the family F_4 of (5).

Example 5: $R = 3, q = 2$. V_0 is the $(9,\ 7)_2 3$ code of [5]. Using K_0 with $h_0 = 9$ and Condition 6 with $m = 3$, $n_0 = 2^m + 1 = h_0$, we obtain a $(79,\ 7 \times 2^{79-18})_2 3, 1$ code V'. Now we use V' as V_0 for Condition 3 with $\Lambda = 1$, $g_2 = (1, 1)$, $2^m \geq 79$. We obtain the family F_1 of (2).

Example 6: If $\rho_j = 1$ we can put that $\mathcal{A}_j$ is an $(N_j, M_j)_q 1$ code of [21] with $\varphi_{m-1,q} < N_j < \varphi_{m,q}$. Then we *shorten* the new codes V obtained when $\mathcal{A}_j$ is the Hamming code. We can construct codes for a *region of code length*. Let $R = 3$, $q = 2$, $V_0 = C_{V_0}$. Let C_{V_0} be the $[23,\ 13]_2 3, 2$ code of [12, Example 4.3]. Let $\mathcal{A}_1$ be an $(N_1, M_1)_2 1$ code of [21] where $1 + N_1 = 2^m/\Delta$, $2 > \Delta > 1$, N_1 is sufficiently large to get $M_1 \approx 2^{N_1}/(1 + N_1)$. We use Condition 3 with $\Lambda = 2$, $2^m \geq 23$, and obtain a family F_2 of (3).

Example 7: $R = 3, q = 3$. $V_0 = C_{V_0}(\Sigma_p^0)$ is the $(14, p \times 3^{14 - r_0})_3 3$ code of [29] with $r_0 = 14$, $p = 2187 = 3^7$, $C_{V_0} = Z_{14}$, see Fact 2. We use the trivial partition K_0 with $h_0 = 14$ and Condition 2 with $g_3 = (1,\ 2)$, $3^m - 1 \geq 14$, $m = 3$. Let $\mathcal{A}_2$ be the $[22,\ 16]_3 2$ code of [11, table 1]. Then $N = \varphi_{3,3} + 22 = 35$ and we have a $(413,\ 3^{413-16})_3 3, 1$ code V' with $h(V', 1) \leq 39$, see (27). We take V' as V_0. We use the $3,\ 1$-partition $K^{(1)}$ as K_0 and Condition 3 with $\Lambda = 1$, $g_2 = (1, 1)$, $3^m \geq 39$. We put $m \geq 4$. Then $N = 2\varphi_{m,3}$, $n_V = 414 \times 3^m - 1$, $M_V = 3^{n_V - (16+3m)}$, see (12) and Remark 3. We obtain the family F_5 of (6). Similarly, if V_0 is the $(13,\ 1215)_3 3$ code of [19] we obtain the family F_6 of (7).

Remark 4: The described constructions can be developed and modified by using the ideas of [6]–[12]. For example, we can use Cauchy matrices for design of matrices $B_m(b)$ [6, eq. (2.3)], take vectors g_ρ with many nonidentity components [6, pp. 319–320], [8, p. 2073], give more conditions sufficient for $R_V = R$ [6, Theorem 2], [8, p. 2074], [12, Theorems 3.1, 4.1, 5.1], obtain estimates of $l_V, h(V, l_V)$ and use them for improving the iterative process of constructing codes [8, Secs. IV, VI, VII], use R^*, l-subsets with covering radius smaller than R^* [6, Definition 1, Example 5], etc.

Remark 5: The proposed constructions can be used to improve estimates of the value

$$\mu_q(R) = \limsup_{n \to \infty} \mu_q(n, R)$$

where $\mu_q(n, R)$ is the minimal density of the covering of a q-ary code of length n, covering radius R. For example, the known families A_i (see Section I) and Fact 1 give the following local maxima of $\mu_2^\bullet(n, 3)$: $\mu_2^\bullet(n_1 - 1, 3) \approx 4.5$, $\mu_2^\bullet(n_2 - 1, 3) \approx 2.75$, $\mu_2^\bullet(n_3 - 1, 3) \approx 2.67$, $\mu_2^\bullet(n_4 - 1, 3) \approx 4.46$. So, the known codes imply $\mu_2(3) \leq 4.5$. It can be shown that the obtained families F_j of (2)–(5) and Fact 1 give the following new local maxima of $\mu_2^\bullet(n, 3)$: $\mu_2^\bullet(n_{F_1} - 1, 3) \approx 3.01$, $\mu_2^\bullet(n_{F_2}, 3) \approx 3.74$, $\mu_2^\bullet(n_{F_3} - 1, 3) \approx 2.69$, $\mu_2^\bullet(n_3 - 1, 3) \approx \mu_2^\bullet(n_{F_4} - 1, 3) \approx 2.67$, where n_{F_j} is the length of codes of the family F_j, n_{F_2} is taken for $\Delta = 7/4$. For the length n_{F_2} the family F_2 gives the same density 3.74 as the family F_1 and Fact 1. For the length $n_{F_1} - 1$ the family A_3 (if t is even) or the family F_4 (if t is odd) and Fact 1 give the density 3.01. So, we obtained $\mu_2(3) \leq 3.74$ instead of $\mu_2(3) \leq 4.5$.

Acknowledgment

The author wishes to thank G. A. Kabatianskii for his suggestion to treat nonlinear code as a union of cosets of a linear code [20]. The author also wishes to thank the anonymous referees for useful remarks.

References

[1] A. Blokhuis and C. W. H. Lam, “More coverings by rook domains,” *J. Combin. Theory*, ser. A, vol. 36, pp. 240–244, 1984.

[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. D. Cohen, M. G. Karpovsky, H. F. Mattson, Jr., and J. R. Schatz, “Covering radius—Survey and recent results,” *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 328–343, May 1985.

[4] G. D. Cohen, S. N. Litsyn, A. C. Lobstein, and H. F. Mattson, Jr., “Covering radius 1985–1994,” *AAECC J.*, to be published.

[5] G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, “Further results on the covering radius of codes,” *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 680–694, Sept. 1986.

[6] A. A. Davydov, “Construction of linear covering codes,” *Probl. Pered. Inform.* (in Russian), vol. 26, no. 4, pp. 38–55, Oct.–Dec. 1990. English transl. in *Probl. Inform. Transm.*, vol. 26, no. 4, pp. 317–331, Oct.–Dec. 1990.

[7] ——, “Construction of codes with covering radius 2,” in *Lecture Notes in Computer Science, Algebraic Coding*, no. 573. New-York: Springer-Verlag, 1992, pp. 23–31.

[8] ——, “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.

[9] ——, “On nonlinear covering codes,” in *Proc. Israeli–French Workshop “Coding and Information Integrity”* (Tel-Aviv, Israel, Dec. 1994).

[10] ——, “On constructions of nonlinear covering codes,” in *Proc. VII Joint Swedish–Russian Int. Workshop on Information Theory* (St.-Petersburg, Russia, June 1995), pp. 67–71.

[11] ——, “On nonbinary linear codes with covering radius two,” in *Proc. V Int. Workshop on Algebraic and Combinatorial Coding Theory* (Sozopol, Bulgaria, June 1996), pp. 105–110.

[12] A. A. Davydov and A. Yu. Drozhzhina-Labinskaya, “Constructions, families and tables of binary linear covering codes,” *IEEE Trans. Inform. Theory*, vol. 40, pp. 1270–1279, July 1994.

[13] T. Etzion and G. Greenberg, "Constructions for perfect mixed codes and other covering codes," *IEEE Trans. Inform. Theory*, vol. 39, pp. 209–214, Jan. 1993.
[14] E. M. Gabidulin, A. A. Davydov, and L. M. Tombak, "Codes with covering radius 2 and other new covering codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 219–224, Jan. 1991.
[15] R. L. Graham and N. J. A. Sloane, "On the covering radius of codes," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 385–401, May 1985.
[16] I. S. Honkala, "On (k, t)-subnormal covering codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1203–1206, July 1991.
[17] ——, "On lengthening of covering codes," *Discr. Math.*, vol. 106–107, pp. 291–295, 1992.
[18] I. S. Honkala and H. O. Hämäläinen, "A new construction for covering codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1343–1344, Sept. 1988.
[19] H. O. Hämäläinen and S. Rankinen, "Upper bound for footbal pool problems and mixed covering codes," *J. Combin. Theory*, ser. A, vol. 56, no. 1, pp. 84–95, Jan. 1991.
[20] G. A. Kabatianskii, private communication.
[21] G. A. Kabatianskii and V. I. Panchenko, "Unit sphere packings and coverings of the Hamming space," *Probl. Pered. Inform.* (in Russian), vol. 24, no. 4, pp. 3–16, Oct.–Dec. 1988. English transl. in *Probl. Inform. Transm.*, vol. 24, no. 4, pp. 261–272, Oct.–Dec. 1988.
[22] H. J. L. Kamps and J. H. van Lint, "A covering problem," in *Proc. Colloq. Math. Soc. Janos Bolyai; Hung. Combin. Theory and Appl.* (Balantonfured, Hungary, 1969), pp. 679–685.
[23] J. H. van Lint, "Recent results on covering problems," in *Lecture Notes in Computer Science*, no. 357. New-York: Springer-Verlag, 1989, pp. 7–21.
[24] J. H. van Lint, Jr., "Covering radius problems," Master's thesis, Eindhoven University of Technology, Eindhoven, The Netherlands, 1988.
[25] A. C. Lobstein and V. S. Pless, "The length function: A revised table," in *Lecture Notes in Computer Science, Algebraic Coding*, no. 781. New-York: Springer-Verlag, 1994, pp. 51–55.
[26] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
[27] L. Storme and J. A. Thas, "Complete k-arcs in PG (n, q), q even," *Discr. Math.*, vol. 106–107, pp. 455–469, 1992.
[28] R. Struik, "Covering codes," Ph.D. dissertation, Eindhoven University of Technology, Eindhoven, The Netherlands, 1994.
[29] P. R. J. Ötergård, "New upper bounds for q-ary covering codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 660–664, May 1991.
[30] ——, "Further results on (k, t)-subnormal covering codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 206–210, Jan. 1992.

New Good Quasi-Cyclic Ternary and Quaternary Linear Codes

Rumen N. Daskalov, *Associate Member, IEEE*, and T. Aaron Gulliver, *Senior Member, IEEE*

***Abstract*—Let $[n, k, d; q]$-codes be linear codes of length n, dimension k and minimum Hamming distance d over GF (q). The following quasi-cyclic codes are constructed in this paper:**

$$[44, 11, 20; 3],\ [55, 11, 26 : 3],\ [66, 11, 32; 3],\ [48, 12, 21; 3],$$
$$[60, 12, 28; 3],\ [56, 13, 24; 3],\ [65, 13, 29; 3],\ [56, 14, 23; 3],$$
$$[60, 15, 23; 3],\ [64, 16, 25; 3],\ [36, 9, 19; 4],\ [90, 9, 55; 4],$$
$$[99, 9, 61; 4],\ [30, 10, 14; 4],\ [50, 10, 27; 4],\ [55, 10, 30; 4],$$
$$[33, 11, 15; 4],\ [44, 11, 22; 4],\ [55, 11, 29; 4],\ [36, 12, 16; 4],$$
$$[48, 12, 23; 4],\ [60, 12, 31; 4].$$

All of these codes have established or exceed the respective lower bounds on the minimum distance given by Brouwer.

***Index Terms*—Quasi-cyclic codes, ternary and quaternary linear codes.**

I. Introduction

Let GF (q) denote the Galois field of q elements. A linear code over GF (q) of length n, dimension k, and minimum Hamming distance d is called an $[n, k, d; q]$-code.

A code C is said to be quasi-cyclic (QC) if a cyclic shift of any codeword by p positions is also a codeword in C. A cyclic code is a QC code with $p = 1$. The length n of a QC code is a multiple of p, i.e., $n = mp$. With a suitable permutation of coordinates, many QC codes can be characterized in terms of $(m \times m)$ circulant matrices. In this case, a QC code can be transformed into an equivalent code with generator matrix

$$G = [R_0;\ R_1;\ R_2;\ \cdots;\ R_{p-1}] \tag{1}$$

where R_i, $i = 0, 1, \cdots, p-1$ is a circulant matrix of the form

$$R = \begin{bmatrix} r_0 & r_1 & r_2 & \cdots & r_{m-1} \\ r_{m-1} & r_0 & r_1 & \cdots & r_{m-2} \\ r_{m-2} & r_{m-1} & r_0 & \cdots & r_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ r_1 & r_2 & r_3 & \cdots & r_0 \end{bmatrix}. \tag{2}$$

The algebra of $m \times m$ circulant matrices over GF (q) is isomorphic to the algebra of polynomials in the ring GF $(q)[x]/(x^m - 1)$ if R is mapped onto the polynomial

$$r(x) = r_0 + r_1 x + r_2 x^2 + \cdots + r_{m-1} x^{m-1}$$

formed from the entries in the first row of R [8]. The $r_i(x)$ associated with this QC code are called the *defining polynomials* [4].

Manuscript received September 30, 1996; revised March 3, 1997. This work was supported in part by the Bulgarian National Science Fund under Grant I-618/96, and by the Natural Sciences and Engineering Research Council of Canada.

R. N. Daskalov is with the Department of Mathematics, Technical University, 5300 Gabrovo, Bulgaria.

T. A. Gulliver was with the Department of Systems and Computer Engineering, Carleton University, Ottawa, Ont., Canada. He is now with the Department of Electrical and Electronic Engineering, University of Canterbury, Christchurch, New Zealand.

Publisher Item Identifier S 0018-9448(97)05217-6.