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 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 \( q^m \)-concatenating constructions of \([6], [7], \) and \([12]\). This generalization is close to Construction B of this work, see Remark 2.

Let \( E^n_q \) 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 \( t \in E^n_q \). So \( t + V = \{t + v : v \in V\} \). Let \( wt(g) \) be the weight of a vector \( g \). Denote by \( F^r_q \) the space of \( r \)-dimensional \( q \)-ary column vectors. Denote by

\[
C_1 \times C_2 \times \cdots \times C_t = \{(u_1, u_2, \cdots, u_t) : u_i \in C_i, \ i = 1, T\}
\]

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

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

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

\[
\overline{\mu}_q(R, U) = \lim_{n \to \infty} \mu_q(n, R, U_n), \quad U_n \in U.
\]

Let \( \mu_q(n, R) \) be the least known density of the covering of a \( q \)-ary code of length \( n \), covering radius \( R \). Denote by \( M_q^* (n, R) \) 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. The following facts are used.

**Fact 1:** If an \((n, M)_q R \) code exists then an \((n + 1, q M)_q R \) code exists.

We give parameters of the best known infinite families \( A_i \) of \((n_i, M)_32 \) codes with \( R = 3, q = 2 \).

**Fact 2:**

\[
A_1: r = 3t - 2, \quad n_1 = 48 \times 2^{t-5} - 1, \quad M = 2^{n_1-3t+1},
\]

\[
t \geq 8, \quad \overline{\mu}_2(3, A_1) \approx 2.25 \quad [12, \text{form. (4.12)}]
\]

\[
A_2: r = 3t - 1, \quad n_2 = 51 \times 2^{t-5} - 2, \quad M = 2^{n_2-2t+1},
\]

\[
t \geq 14, \quad \overline{\mu}_2(3, A_2) \approx 1.3744 \quad [12, \text{form. (1.4)}]
\]

**Fact 3:**

\[
A_3: r = 3t, \quad n_3 = 64 \times 2^{t-5} - 1, \quad M = 2^{n_3-3t},
\]

\[
t \geq 9 \text{ is even}, \quad \overline{\mu}_2(3, A_3) \approx 4/3 \quad [13, \text{Theorem 8}]
\]

**Fact 4:**

\[
A_4: r = 3t, \quad n_4 = 76 \times 2^{t-5} - 1, \quad M = 2^{n_4-3t},
\]

\[
t \geq 9 \text{ is odd}, \quad \overline{\mu}_2(3, A_4) \approx 2.23 \quad [12, \text{form. (4.16)}].
\]

We can obtain a code of arbitrary length \( n \) using a family \( A_i \) and Fact 1. But this new code has the density \( \mu_q(n, 3) \) greater than codes of the used family \( A_i \), e.g., if the length \( n \) increases from \( 64 \times 2^{t-5} - 1 \) to \( 48 \times 2^{t-5} - 2 \), where \( t \) is large even, then the density \( \mu_q(n, 3) \) increases from \( 4/3 \) to \( 9/2 \), see (1). In general, \( \mu_q^*(n_i - 1, 3) \approx 2 \mu_q^*(n_i, 3) \) for large \( n_i \). Note also that asymptotic optimal \((n', M')_3 \) codes with arbitrary length \( n' \) and
are obtained in [21]. DS of these codes gives codes $D$ with $\mu_q(n, D)$ $\approx 4.5$ for arbitrary $q$ and arbitrary large $n$.

To illustrate the new constructions, in Section IV we obtain new infinite families $F_i$ of $(n, M)_3$ codes $C$, with the following parameters:

$$F_1: R = 3, \quad q = 2, \quad r = 3 t - \log_2 q, \quad n = 40 \frac{1}{2} \times 2^{t-5} - 2,$$

$$M = 7 \times 2^{n-3t} = \frac{7}{8} M^*_3(n, 3), \quad t \geq 13,$$

$$\mu_2(n, 3, C_1) = \frac{7}{8} \mu_2^*(n, 3), \quad \mu_2(3, F_1) \approx 2.7. \quad (2)$$

$$F_2: R = 3, \quad q = 2, \quad r = 3 t - 2 - \log_q \Delta,$$

$$n = \left[46 + \frac{2}{\Delta} 2^{t-5} - 1, \quad 2 > \Delta > 1, \quad n \text{ is large},

M = \Delta \times 2^{n-3t+2} \approx \frac{\Delta}{2} M^*_3(n, 3), \quad t > 8,$$

$$4.27 > \mu_2(n, 3, C_2) > \frac{\Delta}{2} \mu_2^*(n, 3) > 2.25. \quad (3)$$

$$F_3: R = 3, \quad q = 2, \quad r = 3 t - 1,$$

$$n = 50 \frac{31}{32} \times 2^{t-5} - 1, \quad \text{if } t = 17, 20 \text{ and } t \geq 35,$$

$$M = 2^{n-3t+1} = \frac{1}{2} M^*_3(n, 3), \quad \mu_2(n, 3, C_3) = \frac{1}{2} \mu_2^*(n, 3), \quad \mu_2(3, F_3) \approx 1.3469. \quad (4)$$

In (2)–(5) codes with $M^*_3(n, 3), \mu_2^*(n, 3)$ 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 $A_1, A_2, A_3$. Codes of the family $A_3$ from [13] have asymptotic density $4/3$ for code length $2^n - 1$ where $u$ is odd. The obtained family $F_1$ has the same asymptotic density $4/3$ for code length $2^n + \varepsilon$ where $u$ is even and $\varepsilon$ is small compared to $2^n$. 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 $\Delta$). 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 $F_i, F_0$ of $(n, M)_3$ codes $C_5, C_6$ with $R = 3, q = 3$, and the following parameters for $t > 9$:

$$F_5: \quad n = 414 \times 3^{t-5} - 1, \quad M = 3^{n-3t-1} \leq \frac{1}{2} M^*_3(n, 3),$$

$$\mu_3(n, 3, C_5) \leq \frac{1}{2} \mu_3^*(n, 3), \quad \mu_3(3, F_5) \approx 2.2. \quad (6)$$

$$F_6: \quad n = 387 \times 3^{t-5} - 1, \quad M = 5 \times 3^{n-3t-2} \leq \frac{2}{3} M^*_3(n, 3),$$

$$\mu_3(n, 3, C_6) \leq \frac{2}{3} \mu_3^*(n, 3), \quad \mu_3(3, F_6) \approx 3.0. \quad (7)$$

Here $\mu_3^*(n, 3) \approx 4.5$. Codes with $M^*_3(n, 3), \mu_3^*(n, 3)$ 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

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

and

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

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 $(n, M)_3$ code $C$, we have

$$M = \delta_i M^*_i(n, 3), \quad \mu_i(n, 3, C_i) = \delta_i \mu_i^*(n, 3)$$

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

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 $0^b$ be a zero matrix (column) with $S$ rows. If $S = 0$ then the matrix (column) $0^b$ is treated as absent. Let $GF^q\{\} = GF(q)\{\{0\}\}$. 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 $\sigma$ of $F_q^r$, i.e.,

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

Let $\Sigma_p$ be a set of $p$ syndromes such that

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

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

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

Clearly, $C(\Sigma_p)$ is an $(n, pq^{m-1})_q$ 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 $(0 \ldots 0)$ of length $n$. We treat $Z_n$ as the linear $[n, n-n]_q$ code with the parity-check matrix $I_n$. For any $(n \times 1)_q$ code $V$ there exist a linear code $C_V$ and a set of syndromes $\Sigma_p$ such that $V = C_V(\Sigma_p)$. In any case, one may take $C_V = Z_n(\nu), p = M(\nu), \Sigma_p = \{v_1^T, \ldots, v_M^T\}$ where $\{v_1, \ldots, v_M^T\} = V$, $v_i$ is a codeword of $V$, $i = 1, M, \overline{M}$, i.e., the set $\Sigma_p$ 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 $(n, pq^{m-1})_q$ code and let $V = C_V(\Sigma_p)$ where

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

$C_V$ 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 $\sigma_{\pi}(x) \in \Sigma_p$ with a linear combination of at most $R$ columns of the matrix $H$. 
ii) Let \( x \) be a vector of \( E_n^w \) with \( xHT = \pi \in F_q^r \). If and only if the column \( \pi \) is a sum of some syndrome \( \sigma_{i(x)} \) of \( \Sigma_r \) with a linear combination of \( t \) distinct columns of \( H \) then there exists a codeword \( w \) of \( V \) with \( d(x, w) = t \). Otherwise, we define
\[
w \in \mathbb{C} \{ v \in V : vHT = \sigma_{i(x)} \}
\]
and
\[d(x, V) \leq d(x, G) \leq t.
\]

Definition 1 [8], [12]: Let \( V \) be an \((n, M)_R \) code of length \( n \), cardinality \( M \), and covering radius \( R \). Let \( I \) be an integer, \( R \leq I \geq 0 \).

The code \( V \) is called an \( R, l \)-object of the space \( E_n^w \) and is denoted by \((n, M)_R l \) code if \( x \) exists a word \( w(x) \) of \( V \) such that \( R \geq d(x, w(x)) \geq I \). If \( I \geq 1 \) then \( V \) is also a \((n, l-l) \) object with \( l = 0, 1, \ldots, l-1 \).

Remark 1: \((n, M)_R \) objects are a subclass of \((n, M)_l \) subsets of \([0, w(x) \in E_n^w, R \geq d(x, w(x)) \geq I] \), where \((n, l) \) objects are useful for.

Example 1: The set \([000000, 111000, 000111] \) is a \((6, 3) \) - 2, 1 code.

The set \([00000, 11111, 11111, 000111, 1010101, 1010101, 1101101] \) is a \((6, 4) \) - 2, 1 code. See also Section IV.

Definition 2 [8], [12]: Let \( D = \{1, \ldots, n\} \) be the set of codeword positions of an \((n, M)_R l \) code 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 \( E_n^w \) there exist a codeword \( g(x) \) of \( C \) and a vector \( e(x) \) of \( E_n^w \) such that \( x = g(x) + e(x) \), \( R \geq wt(e(x)) \geq I \), 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 \( C \). Define \( h(C, l-k) \) as the value of \( \mathbb{E} \) for defined \( l \) and \( K \). Let \( h(C, l-k) \) be a code of covering radius \( l \) and \( k \).

For linear codes \( R, l \)-partitions and \( l \)-length were introduced in \([8] \) and \([12] \). For nonlinear codes an “effective length” corresponding to \( R, l \)-length was considered in \([28, supp., statement 6] \).

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

Definition 3: Let \( V = C_{\Sigma_r} \) be an \((n, p q^{-m} \rangle) \) code of covering radius \( R \) where \( C_{\Sigma_r} \) is an \([n, n-r] \) code with a parity-check matrix \( H \) and \( \Sigma_r = \{\sigma_1, \ldots, \sigma_r\} \) \( F_q^r \).

Let \( l \) be an integer, \( R \geq l \geq 0 \).

i) The code \( V \) is called an \((n, M)_R l \)-object of the space \( E_n^w \) if for each column \( \pi \) of \( F_q^r \) (including the zero column) there exist a syndrome \( \sigma_{i(\pi)} \) of \( \Sigma_r \) and a linear combination \( L(\pi) \) of \( \pi \) such that the \( \pi = \sigma_{i(\pi)} + L(\pi) \).

ii) Let \( D = \{1, \ldots, n\} \) be the set of codeword positions of the code \( V \). We also consider \( D \) as the set of codeword positions in the matrix \( H \). A partition of the set \( D \) into nonempty subsets is called an \((n, M)_R l \)-partition if for each column \( \pi \) of \( F_q^r \) (including the zero column) there exist a syndrome \( \sigma_{i(\pi)} \) of \( \Sigma_r \) and a linear combination \( L(\pi) \) of \( \pi \) such that \( \pi = \sigma_{i(\pi)} + L(\pi) \).

For i) and ii) we can treat the zero column as the linear combination of 0 columns of \( H \).
Construction A: Let
\[ V_0 = C_{V_1}(\Sigma^0_v) \]
be a starting \((n_0, pq^{\rho n_0-r_0})_R, I_0\) code of length \(n_0\), cardinality \(pq^{\rho n_0-r_0}\), and covering radius \(R\), where
\[ \Sigma^0_v = \{ \sigma_1, \ldots, \sigma_v \} \subseteq F^{q^r}_v \]
and \(C_{V_1}\) is a \([n_0, n_0 - r_0]_q\) code with a parity-check matrix \(H_0 = [f_1 \cdots f_{n_0}]\), \(f_s \in F^{q^r}_v, k = 1, n_0\). Let \(K_0\) be an \(R, I_0\)-partition for the starting code \(V_0\). We define \(h_0 = h(V_0, I_0; K_0)\). Let \(m, \Lambda\) be parameters, \(\Lambda \in \{0, 1, \ldots, R\}\). 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 \((n_1, p|q|^{r_1-\gamma})_R, I_1\) code \(V_1\) of length \(n_1\), cardinality \(p|q|^{r_1-\gamma}\), and covering radius \(R_1\), where
\[ V_1 = C_{V_1}(\Sigma^1_{\bar{\gamma}}), n_1 = n_0 q^m, r_1 = r_0 + m R. \]
We have
\[ \Sigma^1_{\bar{\gamma}} = \bigcup_{j=1}^q \{ \delta^1_{j, \alpha} \} \subseteq F^{q^r}_{\bar{\gamma}}. \]

2) We form the new \((n_\gamma, M_\gamma)_R, \gamma, I_\gamma\) code \(V\) of length \(n_\gamma\), cardinality \(M_\gamma\), and covering radius \(R_\gamma\). If \(\Lambda = R\) then \(V = V_1, M_\gamma = pq^{r_1-\gamma-1}\). If \(\Lambda < R\) then the parity words of the auxiliary code \(V_1\) into \(Q\) groups \(G_u\) so that
\[ G_u = \{ v \in V_1 : \gamma^T \delta^1_{u, i} = 1, i = 1, q \} \]
and \(u = 1, q\)
\[ \bigcup_{u=1}^Q G_u = V_1. \]

We choose a vector \(g_{\rho} = (\rho_1, \ldots, \rho_v)\), \((N_j, M_j, \rho_j)\) codes \(A_j\), and translates \(A_j^v\) for \(v = 1, q, j = q^{m \rho_j}, \gamma = 1, q, j = 1, q, \gamma \). and put
\[ V = \bigcup_{u=1}^Q D_u \times G_u, \quad n_\gamma = N + n_0 q^m \]
\[ M_\gamma = \bar{M}_p q^{r_1-\gamma} = \bar{M}_p q^{n_0 q^m - r_0 - m R}. \]

where
\[ \sum_{j=1}^\gamma \rho_j = \rho, \quad N = \sum_{j=1}^\gamma N_j, \quad M_\gamma = \prod_{j=1}^\gamma M_j, \]
\[ M_\gamma = p q^{m \gamma - r_1} = p q^{N + n_0 q^m - r_0 - m R}, \quad \text{if} \quad \bar{M}_p = q^{N - m \rho}. \]

Lemma 1: In Construction A for covering radii of codes \(V, V_1\), and \(V_0\) it holds that \(R_\gamma \geq R_1 \geq R_0\).

Proof: Let \(Z < R\). By Fact 3(i), there exists a column \(\pi \in F^{q^t}_v\) which cannot be represented by a sum of a syndrome \(\sigma_i \in \Sigma^0_v\) and a linear combination of \(Z\) columns of \(H_0\). We take this \(\pi\) and an arbitrary \(\lambda \in F^{q^t}_v\). Then, by (10) and (11), the column \([\pi \lambda]^T \in F^{q^r}_v\) cannot be represented by a sum of a syndrome \(\delta^1_{j, \alpha} \in \Sigma^1_{\bar{\gamma}}\) and a linear combination of \(Z\) columns of \(\Omega\). So, \(R_{\gamma} \geq R_1\). Finally, by (12), \(R_{\gamma} \geq R_0\).

Examples of Conditions Sufficient for the Equality \(R_\gamma = R\) in Construction A (always \(\rho = \bar{M}_p - \Lambda\)):

1) \(R \geq 2, I_0 = 0, \Lambda = 0, \beta \subseteq GF(q^m) \{ \# \}, q^m + 1 \geq h_0, \gamma = (1, 0, \ldots, 0, 1).
2) \(R \geq 2, I_0 = 0, \Lambda = 0, \beta \subseteq GF(q^m) \{ \# \}, q^m - 1 \geq h_0, \gamma = (1, 0, \ldots, 0, 1).
3) \(R \geq 2, I_0 \geq 1, \Lambda = 0, \beta \subseteq GF(q^m) \{ \# \}, q^m - 1 \geq h_0, \gamma = (1, 0, \ldots, 0, 1).
4) \(R \geq 2, I_0 = 0, \Lambda = \beta \subseteq GF(q^m) \{ \# \}, q^m + 1 \geq h_0, \gamma = (1, 0, \ldots, 0, 1).
5) \(R \geq 2, I_0 = 0, \Lambda = 1, \beta \subseteq GF(q^m) \{ \# \}, q^m - 1 \geq h_0, \gamma = (1, 0, \ldots, 0, 1).
6) \(R \geq 3, I_0 = 0, \Lambda = 2, \beta \subseteq GF(q^m) \{ \# \}, q^m - 1 \geq h_0, \gamma = (1, 0, \ldots, 0, 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 \(GF(q^m)\) or \(GF(q^m) \cup \{ \# \}\) 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 \(q^m - 1 \geq h_0\) in respect to restrictions for \(m\). These inequalities permit us to assign distinct indicators \(b_i \neq b_j\) if the numbers \(i, k\) belong to distinct subsets of \(K_0\). Besides, we want to decrease the density of the covering \(p_i(n, R, V)\) of the new code \(V\). For the case \(M_\gamma = p q^{r_0-\gamma}\) for fixed \(r_1\), we should reduce the length \(n+\gamma\) of \(V\), see (1), increasing \(\Lambda\) causes reduction of \(N\) and \(n\).

Examples of Constructions (1)–6) give \(\Lambda = I_0, \Lambda = I_0\), Conditions 5) and 6) give \(\Lambda = I_0 + 1, \Lambda = I_0 + 2\). If \(\Lambda = R\) then \(\Lambda = 0\). For decreasing of \(N\) and \(n\) vector \(g_0 = (1, 0, \ldots, 1, [R/2])\) is preferential to \(g_0 = (1, 0, \ldots, 1, 1)\).

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., \(R_\gamma = R\). Besides, \(I_\gamma \geq I_0\) for all Conditions 1–6).

Proof: By Lemma 1, it is sufficient to prove that \(R_\gamma \leq R\).

It means that \(d((e_0, V)) \leq R\), where \((e_0)\) is an arbitrary vector of \(E^{n_\gamma}_v, \phi \in E^{n_\gamma}_v, e = (c_1, \ldots, c_v) \in E^{N_\gamma}_v, c_j \in E^{q^r}_v, j = 1, \gamma, \gamma\). We have
\[ \phi^T = \left[ \begin{array}{c} \pi \cr \lambda \end{array} \right] \in F^{q^t}_v, \quad \pi \in F^{q^t}_v, \quad \lambda = \left[ \begin{array}{c} \lambda_1 \\
\lambda_2 
\end{array} \right] \in F^{q^R}_v, \quad \lambda_i \in F^{q^R}_v, \quad i = 1, R. \quad (13) \]

We consider Condition 1 with \(\Lambda = I_0 = 0, \gamma = \rho = R, \rho_j = 1, Q_j = q^m, j = 1, R\). By Definition 3, we can find a syndrome \(\sigma_i(\pi)\),

\[ \sigma_i(\pi) = \left[ \begin{array}{c} \rho_1 \\
\rho_2 
\end{array} \right] \in F^{q^R}_v, \quad \sigma_i = \sigma_i(\pi) \in F^{q^R}_v. \]


an index collection $J = \{j_1, \cdots, j_Z\}$, and coefficients $a_k$ such that
\[ \pi = \sigma_{i(\pi)} + \sum_{k=1}^{Z} a_k f_{j_k}, \quad \sigma_{i(\pi)} \in \Sigma_{\rho}, \quad R \geq Z \geq l_0, \]
\[ a_k \in GF^*(q), \quad k = 1, \cdots, Z \]
(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 $y \neq k$, $y \in \{1, \cdots, Z\}$, $y \neq k$, see the assignment of indicators $b_i$ in (11).

Let $c_i \in E^{n_i}_0$. Denote by $\psi_i(c_i)$ the least integer such that $c_i \in A^{\psi_i(c_i)}$, see Notation 1. We take the least integer for definiteness.

Let $t_{j_y}$ be the $\mu$th column of the submatrix $B_{s_y}(b_{j_y})$ in (11).

Let $R > Z \geq 1$. For the index collection $J$ we will find columns $t_{j_k} \epsilon_k$ and a vector $\Gamma_X$ such that
\[ \left[ \frac{\pi}{\lambda} \right] = \left[ \frac{\sigma_{i(\pi)}}{\Gamma_X} \right] + \sum_{k=1}^{Z} a_k \left[ \frac{f_{j_k}}{t_{j_k} \epsilon_k} \right] \]
(15)
where $\sigma_{i(\pi)}, a_k, j_k, k = 1, \cdots, Z$, are taken from (14), and besides the vector $\Gamma_X$ must satisfy the relations
\[ \xi_{w_{\pi(c_i)}}^{(i)} = \xi_{w_{\pi(c_i)}}^{(i)}, \quad i = 1, \cdots, Z. \]
(16)
Let $b_{j_y} \neq \pi, k = 1, \cdots, Z$. “Locations” $e_{\pi_k}$ of columns $t_{j_k} \epsilon_k$ in (15) are a solution of the system
\[ \sum_{k=1}^{Z} a_k e_{\pi_k} b_{j_k}^{i-1} = \lambda_i - \xi_{w_{\pi(c_i)}}^{(i)}, \quad i = 1, \cdots, Z, \quad b_{j_y} \neq b_{j_k}, \quad i \neq k. \]
(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 $e_{\pi_k}$ from (17), we calculate
\[ \xi_{w_{\pi(c_i)}}^{(i)} = \lambda_i - \sum_{k=1}^{Z} a_k e_{\pi_k} b_{j_k}^{i-1}, \quad i = 1, \cdots, Z. \]
(18)
Now the relations (16) and (18) together give the desired vector $\Gamma_X$.

We have obtained columns $t_{j_k} \epsilon_k$ and the vector $\Gamma_X$ simultaneously satisfying (15) and (16). The columns $t_{j_k} \epsilon_k$ are given by locations $e_{\pi_k}$. By (15), we have the representation of the column $o_0^{i-1}$ of (13) by the sum of the syndrome $\xi_{w_{\pi(c_i)}}^{(i)}$ of $S_{i1}$, see (10), and a linear combination of $Z$ columns of the matrix $\Omega$. By Fact 3ii), $d(\phi, G_X) \leq Z$. The obtained vector $\Gamma_X$ exactly gives a code $D_X$, see Notation 1. By (14),
\[ c_i \in A^{\psi_i(c_i)} = A^{w_{\pi(c_i)}}, \quad i = 1, \cdots, Z. \]

\[ (c_1, c_2, \cdots, c_Z) \in A^{w_1(X)} \times A^{w_2(X)} \times \cdots \times A^{w_Z(X)}. \]
Since $A^{w_i}$ is a code with covering radius $\rho_j$, we have $d(c, D_X) \leq R - Z$. Finally,
\[ d((\phi), V) \leq d((\phi), D_X \times G_X) \]
\[ = d(c, D_X) + d(\phi, G_X) \leq (R - Z) + Z = R. \]

If $Z = R$ then calculations of (18) are not executed
\[ d(c, D_X) = 0 \quad d((\phi), V) \leq d(\phi, G_X) \leq R. \]
Let $Z = 0, \pi = \sigma_{i(\pi)}$, see (14). We put $\Gamma_X = \lambda$. Then $o_0^{i-1} = [\pi \lambda]^T = [\sigma_{i(\pi)} \Gamma_X]^T = \delta_{\pi(c_i)}^{(i)}, \quad \phi \in G_X, \quad d((\phi), V) \leq d(c, D_X) \leq \gamma = \rho = R.$

Let $R > Z \geq 2, b_{j_Z} = \pi$. In (16) we put $i = 1, 2, \cdots, Z - 1, R$. Hence $c_i \in A^{w_{\pi(c_i)}}, \quad i = 1, 2, \cdots, Z - 1, R$, and $d(c, D_X) \leq R - Z$. The system of (17) has the form
\[ \sum_{k=1}^{Z} a_k e_{\pi_k} b_{j_k}^{i-1} = \lambda_i - \xi_{w_{\pi(c_i)}}^{(i)} \]
\[ i = 1, 2, \cdots, Z - 1, \quad b_{j_Y} \neq b_{j_k}, \quad i \neq k. \]
(19)
The determinant of the system of (19) is not equal to zero since we add the column $(0, 0, \cdots, 0)^T$ to the Vandermonde matrix. By (19), we obtain $e_{\pi_k}$. Then, instead of (18), we calculate
\[ \xi_{w_{\pi(c_i)}}^{(i)} = \lambda_i - \sum_{k=1}^{Z} a_k e_{\pi_k} b_{j_k}^{i-1}, \quad i = 1, \cdots, Z. \]
So, we obtain $\Gamma_X$ and $t_{j_k} \epsilon_k$ for (15). By Fact 3ii), $d(\phi, G_X) \leq Z$. So $d((\phi), V) \leq (R - Z) + Z = R.$

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

Condition 2: We have $\rho_j = 1, Q_j = q^m, j = 1, \cdots, \rho, \quad \gamma = [R/2], \quad \gamma = [R/2] + 1, \quad \rho = R.$ Let $Z \geq 1$, see (14). We denote
\[ \xi_{w_{\pi(c_i)}}^{(i)} = E_{1,X} E_{2,X} \cdots E_{[R/2],X}, \quad E_{i,X} \in GF(q^m), \quad i = 1, \cdots, [R/2]. \]

If $R - Z \geq [R/2]$ then we use (15)–(17). Instead of (18) we have
\[ \xi_{w_{\pi(c_i)}}^{(i)} = \lambda_i - \sum_{k=1}^{Z} a_k e_{\pi_k} b_{j_k}^{i-1}, \quad i = Z + 1, \cdots, R. \]
By (20), we obtain $\xi_{w_{\pi(c_i)}}^{(i)}$ for $i = Z + 1, \cdots, R$. So
\[ d((\phi), G_X) \leq Z, \quad d(c, D_X) \leq R - Z, \quad d((\phi), V) \leq R. \]
If $R - Z < [R/2]$ then in (16) we put $i = R - Z + 1, \cdots, R$. Instead of (17) we solve the system
\[ \sum_{k=1}^{Z} a_k e_{\pi_k} b_{j_k}^{i-1} = \lambda_i - \Phi_i, \quad \Phi_i = E_{i+1,X}, \quad i = Z + 1, \cdots, R. \]
(21)
Then we use (18) with $i = 1, \cdots, R - Z$, and obtain values of $\xi_{w_{\pi(c_i)}}^{(i)}$ for $i = 1, \cdots, R - Z$. By Fact 3ii), $d(\phi, G_X) \leq Z$. By (16) with $i = R - Z + 1, \gamma$, we have $d(c, D_X) \leq R - Z.$ So, $d((\phi), V) \leq R.$

Condition 3: We have $\lambda = \lambda_0 \geq 1, \quad \rho_j = 1, \quad Q_j = q^m, j = 1, \cdots, \gamma, \gamma = 1, \cdots, \rho.$ Let $Z = \lambda - \gamma, \quad \rho = \gamma + 1.$ In (16) we put $i = \Gamma, \Gamma$. Instead of (15), (17), and (18) we use (22)–(24), respectively.
\[ \left[ \frac{\pi}{\lambda} \right] = \left[ \frac{\sigma_{i(\pi)}}{\Gamma_X} \right] + \sum_{k=1}^{Z} a_k \left[ \frac{f_{j_k}}{t_{j_k} \epsilon_k} \right]. \]
(22)
\[ \sum_{k=1}^{Z} a_k e_{\pi_k} b_{j_k}^{i-1} = \lambda_i, \quad i = 1, \cdots, \lambda. \]
(23)
\[ \xi_{w_{\pi(c_i)}}^{(i)} = \lambda_{i+1} - \sum_{k=1}^{Z} a_k e_{\pi_k} b_{j_k}^{i-1}, \quad i = \lambda + 1, \cdots, \gamma. \]
(24)
Condition 4: We have $V = V_1$, $I_0 = \Lambda = R$, $n_V = n_1$. Instead of $(c_{\omega})$ we consider a vector $\omega$. The relation (14) always holds for $Z = R$. We use (15) with $[\sigma_{\omega}(\omega^{m-N})]^{T}$ instead of $[\sigma_{\omega}(\omega^{m})]^{T}$ (see (10)). Put that the right side of the equations of (17) is $\lambda_1$, obtained $\epsilon_{\omega_{1}(\omega)} = \frac{1}{\gamma}$. and show that $d(\omega, V_1) \leq R$.

For Conditions 5 and 6, the matrix $\Omega$ of (11) always contains a submatrix $B_{m}(\omega_1)$ with a calculated indicator $b_{\omega_1}$, since $\beta = GF(q^{m})$ or $\beta = GF(q^{m}) \cup \{\#\}$. For Conditions 5 and 6 we use the relation (22).

Condition 5: Here $\epsilon = \rho = R - 1$. Let $\sigma = \sigma_{\omega}(\omega), \lambda_1 \neq 0$. We put $\xi_{\omega_{1}(\omega)} = [i_{\omega_{1}(\omega)}]$. Now $c_1 \in A_1^{(1)}(\lambda_1)$ and

$$d(c, D_\lambda) \leq \gamma - 1 = R - 2$$

We calculate $b_\omega = (\lambda_2 - \epsilon_{\omega_{1}(\omega)})/\lambda_1$ and put

$$\epsilon_{\omega_{1}(\omega)} = \lambda_1 b_\omega - \lambda_{i+1}, \quad i = \Omega_{i,\omega}$$

So we obtain $\Lambda_{\omega}$. We have

$$[\lambda]^{T} = [\epsilon_{\omega_{1}(\omega)}]^{T}$$

By Fact 3ii), $d(\omega, G_{\chi}) \leq 2$. So

$$d((c_{\omega}), D_{\chi} \times G_{\chi}) \leq (R - 2) + 2 = R$$

Condition 6: Here $\chi = \omega_{1}(\omega_{1})$. Let $\sigma = \sigma_{\omega}(\omega) + a_{1}f_{12}$, see (14). If $b_{12} \neq \#$, $\lambda_2 \neq \lambda_1 b_{12}$, $\lambda_3 + \epsilon_{\omega_{1}(\omega)} = \lambda_2 b_{12}$. We calculate $b_\omega = (\lambda_3 + \epsilon_{\omega_{1}(\omega)})/(\lambda_3 + \lambda_2 b_{12}) \neq b_{12}$.

We put

$$a_1 = (\epsilon_{\omega_{1}(\omega)})/(\lambda_3 + \lambda_2 b_{12})$$

Then

$$[\lambda]^{T} = [\epsilon_{\omega_{1}(\omega)}] + a_1[f_{12}, t, b_{12}, b_\omega]$$

By Fact 3ii), $d(\omega, G_{\chi}) \leq 3$.

Let $b_{12} \neq \#$, $\lambda_2 \neq \lambda_1 b_{12}$, $\lambda_3 + \epsilon_{\omega_{1}(\omega)} = \lambda_2 b_{12}$. We take $b_\omega = \#$,$\lambda_1 = 0$. Then

$$[\lambda]^{T} = [\epsilon_{\omega_{1}(\omega)}] + a_1[f_{12}, W, Wb_{12}, Wb_\omega]$$

Again $d(\omega, G_{\chi}) \leq 3$.

Now we use the fact that $c = (c_{\omega}), d(c, D_\lambda) \leq 1$. If $b_{12} = \#$, $\lambda_1 = 0$. We put $\epsilon_{\omega_{1}(\omega)} = \lambda_3$. Then

$$[\lambda]^{T} = [\epsilon_{\omega_{1}(\omega)}] + a_1[f_{12}, 0, 0, 0, 0]$$

If $b_{12} \neq \#$, $\lambda_2 = \lambda_1 b_{12}$, we take $\epsilon_{\omega_{1}(\omega)} = \lambda_3 + \lambda_1 b_{12}, \lambda_1 W = \lambda_1$.

Then

$$[\lambda]^{T} = [\epsilon_{\omega_{1}(\omega)}] + a_1[f_{12}, W, Wb_{12}, Wb_\omega]$$

Now let $\sigma = \sigma_{\omega}(\omega), \lambda_1 \neq 0$. We calculate $b_\omega = \lambda_1 / \lambda_1$ and take $\epsilon_{\omega_{1}(\omega)} = \lambda_1 + \lambda_1 b_{12}$. Then

$$[\lambda]^{T} = [\epsilon_{\omega_{1}(\omega)}] + a_1[f_{12}, 0, 0, 0, 0]$$

Finally we consider values of $I_{\chi}$. Clearly, $I_{\chi} \geq I_0$ if $I_0 \geq 0$. For Conditions 3 and 4 we have $Z \geq I_0$ in (14) and (15). By Fact 3ii), there is a codeword $\nu$ of $V_1$ with $d(\nu, \omega) = Z \geq I_0$. So, $I_{\chi} \geq I_0$.

Comment 2: From the proof one can see the following. Let $(c_{\omega}) \in E_{\omega}^{n(V)}$ where $\phi$ is an arbitrary vector of $E_{\omega}^{n(V)}$. $c = (c_{1}, \ldots, c_{i}) \in E_{\omega}^{n(V)}$, $c_{i} \in E_{\omega}^{n(V)}$, $j = \Omega_{i,\omega}$. For Conditions 1–4 there exists a value $Z$ such that $R \geq Z \geq I_0 = \Lambda$ and at least $q^{m}$ distinct groups $G_{\chi}$ have the following property: each group $G_{\chi}$ contains a word $r_{\chi}(\omega)$ with $d(\omega, r_{\chi}(\omega)) = Z$ (and $d(\omega, G_{\chi}) \leq Z$). The value $Z$ depends on $\omega$, see (13) and (14). Nonzero positions of the vector $\sigma - r_{\chi}(\omega)$ can be given by locations of $Z$ columns $t_{j_{k}\phi_{k}}$ in the matrix (11), see (15), (22), and Fact 3ii). If $Z = \Lambda$ then there is only one such group $G_{\chi}$. Condition 4 always implies $Z = \Lambda$. If $Z > \Lambda$ the groups $G_{\chi}$ can be given by vectors $\chi$ in which, e.g., the following components $\epsilon_{\omega_{1}(\omega)}$ can be chosen arbitrarily: $i = 1, Z = Z - 1$ for Condition 1 with $b_{12} \neq \#$, Condition 2 with $I_{\chi} \geq [R/2]$; and Condition 3: $i = 1, 2, \ldots, Z - 1, R$ for Condition 1 with $Z \geq 2, b_{12} = \#$; $i = R - Z + 1, \gamma$ for Condition 2 with $R - Z \geq [R/2];$ etc. It is naturally to put for these “free” components $\epsilon_{\omega_{1}(\omega)} = e_{10}(c_{\omega}), \sigma_{\omega}(\omega)$, see (16) and changes of values of $i$ in (16) for distinct Conditions. Now $c_{i} \in A_{i}^{(i,\omega)}(\lambda_1), d(c, D_{\chi}) \leq R - Z$, and

$$d((c_{\omega}), D_{\chi} \times G_{\chi}) \leq (R - Z) + Z = R$$

Locations of columns $t_{j_{k}\phi_{k}}$ providing the equality $\epsilon_{\omega_{1}(\omega)} = \sigma_{\omega_{1}(\omega)}$ are values of $e_{\phi_{k}}$ obtained from the systems in (17), (19), (21), and (23).

For Conditions 5 and 6 we have $\Lambda > I_0$ and it is possible in (14) that $\Lambda > Z \geq I_0$. Then we calculate $b_\omega$ and find a desired group $G_{\chi}$ using the equalities $\beta = GF(q^{m})$ or $\beta = GF(q^{m}) \cup \{\#\}$. Again, for some $Z' > Z$ we have $d(\omega, G_{\chi}) \leq Z'$, $d(c, D_{\chi}) \leq R - Z'$. Note that Condition 6 is connected with an oval of $q^{m} + 2$ points in a projective plane $PG(2, q^{m})$.

By structure, the construction

$$V = \bigcup_{u=1}^{Q} D_u \times G_u$$

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 $\min_u d(c, D_u) + \max_u d(c, D_u)$ and $\min u d(\omega, G_u) + \max_u d(\omega, G_u)$ 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

$$V_0 = C_{10}(10)^{0}_{\chi}$$

be a starting $(n_0, p_{\chi}^{m-\alpha-\gamma})_{\chi} R, I_0$ code of covering radius $R$ where

$$\Sigma_{\chi}^{0} = \{\sigma_{1}, \ldots, \sigma_{\gamma}\} \subseteq F_{q}^{\alpha}$$

$C_{10}$ is an $(n_0, n_0 - r_0)_{\chi}$ code with a parity-check matrix

$$H_0 = [f_{1}, \ldots, f_{n_0}]$$

Let $K_0$ be an $R, I_0$-partition for the code $V_0$. We denote $h_0 = h(V_0, I_0; K_0)$. We form a new $(n, m_V, \gamma) R, I_0$ code $V$ of covering
We consider Construction B with \( \varepsilon = 1 \). Let \( \Lambda = \{0, R\} \) be a parameter, and let

\[
D_{m,1} = \begin{bmatrix}
0^{m(R-\rho)} & 0^{M_{\rho} - \rho} & \ldots & 0^{m(R-\rho)} \\
\Xi_{1} & 0^{m\rho} & \Xi_{2} & \ldots & 0^{m\rho} \\
0^{m\rho} & \Xi_{3} & \ldots & 0^{m\rho} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0^{m\rho} & 0^{m\rho} & \ldots & \Xi_{\varepsilon}
\end{bmatrix},
\]

where a vector \( g_{\rho} \) is defined in Notation 1, \( \Xi_{\varepsilon} \) is a parity-check matrix of an \([N, \rho, N - m\rho]\) code \( A_{\rho} \) with covering radius \( \rho \).

The submatrix \( \Psi \) 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 translates \( A_{\rho} \) is a coset of a linear code \( A_{\rho}, j = \Gamma_{\varepsilon} \). Let \( a_{\rho} \) be the codeword of the new code \( V \) of Construction A, i.e.,

\[(a_{\rho}) \in D_{a} \times G_{a}, \quad u \in \{1, Q\}, \quad a_{\rho} = (a_{\rho,1}, \ldots, a_{\rho,\varepsilon}), \quad u = \Gamma_{\varepsilon} .\]

Then \( g_{\rho}^{T} = \xi_{\rho}^{T} = [\sigma | 0^{M_{\rho}} | \Gamma_{\varepsilon}]^{T}, \quad G_{a} = \{a_{\rho}^{(1)}, \ldots, a_{\rho}^{(\varepsilon)}\}^{T} \), see (10) and (11). Now we number cosets of an \([N, N - m\rho]_{\rho}\) code \( A_{\rho} \) with a parity-check matrix \( \Xi_{\varepsilon} \) in an order connected with numbering of elements of \( GF(Q) \). We put

\[A_{\rho}^{(j)} = \{e \in E_{\rho}^{N_{\rho}} : e\Xi_{\rho}^{T} = -\xi_{\rho}^{(j)}\}, \quad j = \Gamma_{\varepsilon}, \quad u = \Gamma_{\varepsilon} .\]

Then

\[a^{T} = [0^{m\rho} + M, -\xi_{\rho}^{(1)}, \ldots, -\xi_{\rho}^{(\varepsilon)}]^{T} .\]

Hence

\[(a_{\rho})H_{V}^{T} = a^{T} + g_{\rho}^{T}T = [\sigma, 0^{M_{\rho}}]^{T} .\]

So, \( a_{\rho} \) is also a codeword of the new code \( V \) of Construction B. Conditions 1–6 of Construction A are also sufficient for the equality \( R_{V} = \Gamma_{\varepsilon} \) in Construction B with \( \varepsilon = 1 \).

Construction B can be useful for estimates of \( l_{V} \) and \( h(V, R_{V}) \) using Definition 3. Besides, in order to improve parameters of the new code \( V \) we can use special matrices \( D_{m,1}^{(\rho)} \) 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 \( g_{\rho} \) is \((1, \ldots, 1)\), and \( K_{0} \) is an \( R, 0 \)-partition. But the construction of [28] does not allow to improve parameters of new codes by using \( R, 1 \)-objects and \( R, 1 \)-partitions with \( l \geq 1 \) and by using parity check matrices of codes with \( \rho_{i} \geq 2 \) for design of matrices \( D_{m,1}^{(\rho)} \). Besides, in the construction of [28] one cannot use translates of nonlinear codes for design of codes \( D_{m,1} \), 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 \( B_{a}(b), H, \Psi \) 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]).
Cauchy matrices for design of matrices $B_2(b)$ [6, eq. (2.3)], take vectors $g_\nu$ 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, V, VI], 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

$$
\mu_v(R) = \maxsup_{n \to \infty} \mu_v(n, R)
$$

where $\mu_v(n, R)$ is the minimal density of the covering of a $q$-ary code of length $n$, covering radius $R$. For example, the known families $A_j$ (see Section I) and Fact 1 give the following local maxima of $\mu_v^*_2(n, 3); \mu_v^*_2(n_2 - 1, 3) \approx 4.5, \mu_v^*_2(n_2, 1, 3) \approx 2.75, \mu_v^*_2(n_2, 1, 3) \approx 2.67, \mu_v^*_2(n_4, 1, 3) \approx 4.65$. So, the known codes imply $\mu_v(3) \leq 4.5$. It can be shown that the obtained families $F_j$ of (2)–(5) and Fact 1 give the following new local maxima of $\mu_v^*_2(n, 3); \mu_v^*_2(n_2 - 1, 3) \approx 3.01, \mu_v^*_2(n_2, 3) \approx 3.74, \mu_v^*_2(n_2, 1, 3) \approx 2.68, \mu_v^*_2(n_2, 1, 3) \approx 2.75, \mu_v^*_2(n_4, 1, 3) \approx 2.67$, where $n_2$ is the length of codes of the family $F_j, n_2$ is taken for $\Delta = 1/4$. For the length $n_2 = 4$ the family $F_2$ gives the same density 3.74 as the family $F_1$ and $F_1$. For the length $n_2$ it is the family $A_3$ (if it is even) or the family $F_1$ if $n_2$ is odd) and Fact 1 give the density 3.01. So, we obtained $\mu_v(3) \leq 3.74$ instead of $\mu_v(3) \leq 4.5$.

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

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:

\[
\begin{align*}
 & \{44, 11, 20; 3\}, \{55, 11, 20; 3\}, \{66, 11, 32; 3\}, \{48, 12, 21; 3\}, \\
 & \{60, 12, 28; 3\}, \{56, 13, 24; 3\}, \{65, 13, 29; 3\}, \{56, 14, 23; 3\}, \\
 & \{60, 15, 21; 3\}, \{64, 16, 25; 3\}, \{36, 9, 19; 4\}, \{90, 9, 55; 4\}, \\
 & \{89, 9, 61; 4\}, \{30, 10, 14; 4\}, \{50, 10, 27; 4\}, \{55, 10, 30; 4\}, \\
 & \{33, 11, 15; 4\}, \{44, 11, 22; 4\}, \{55, 11, 29; 4\}, \{36, 12, 16; 4\}, \\
 & \{48, 12, 23; 4\}, \{60, 12, 31; 4\}.
\end{align*}
\]

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

\[
G = [R_0; R_1; R_2; \ldots; R_{p-1}]
\]

where \(R_i, i = 0, 1, \ldots, p - 1\) is a circulant matrix of the form

\[
R = \begin{bmatrix}
  r_0 & r_1 & r_2 & \cdots & r_{m-1} \\
  r_m & r_0 & r_1 & \cdots & r_{m-2} \\
  \vdots & \vdots & \vdots & \ddots & \vdots \\
  r_{m-1} & r_{m-2} & r_{m-1} & \cdots & r_0
\end{bmatrix}.
\]

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

\[
r(x) = r_0 + r_1x + r_2x^2 + \cdots + r_{m-1}x^{m-1}
\]

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.