Designs, Codes and Cryptography, 22, 305–316, 2001.

New Constructions of Covering Codes

ALEXANDER A. DAVYDOV adav@iitp.ru
Institute for Information Transmission Problems, Russian Academy of Sciences, Moscow, 101447, Russia

Communicated by: A. Tietäväinen

Received November 10, 1998; Revised July 21, 1999; Accepted October 22, 1999

Abstract. Covering code constructions obtaining new codes from starting ones were developed during last years. In this work we propose new constructions of such kind. New linear and nonlinear covering codes and an infinite families of those are obtained with the help of constructions proposed. A table of new upper bounds on the length function is given.

Keywords: Constructions, covering codes, covering radius, length functions

1. Introduction

Covering codes and their constructions and a general survey of covering problems are considered in [2]. A useful approach to designing covering code constructions is described in [2, Chapter 5], see also [3]–[5]. Using a starting code of covering radius $R \geq 2$ these constructions form a new code or a code family with the same covering radius. Linear and nonlinear starting codes are represented with using some matrix. To obtain a new code this matrix is repeated q^m times where q is the code basis. Therefore constructions of such kind can be called "q^m—concatenating constructions." In [9, Supplement] modified q^m—concatenating constructions using arcs of a projective geometry are proposed.

In Section 2, we propose new q^m—concatenating constructions for linear and nonlinear codes and give one known construction. In Section 3, new covering codes and infinite code families are obtained using the constructions described. The parameters obtained are better than those of known codes. The new linear codes imply new upper bounds on the length function. A table of these bounds is given.

Denote by $\mathbb{F}_q$ the Galois field of q elements. Let $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. 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 $\mathcal{S}_q^r$ be the space of r–dimensional q–ary column vectors. The length function $l(r, R; q)$ is the smallest length of a q–ary linear code with codimension r and covering radius R.

Below all matrices (columns) are q–ary. In a q–ary matrix (column) an element of $\mathbb{F}_{q^m}$ denotes a column vector of $\mathcal{S}_q^m$ that is a q–ary representation of this element, and vice versa we can treat a column vector of $\mathcal{S}_q^m$ as an element of $\mathbb{F}_{q^m}$.

We always specify the number of *q–ary* rows in a matrix or positions in a column. Let $\mathbf{0}^k$ be a zero matrix with k rows. Denote by $\mathbf{0}$ a zero column. Usually the number of columns in a matrix $\mathbf{0}^k$ or positions in a column $\mathbf{0}$ is defined by context.

We consider linear combinations of q–ary columns only with *nonzero* q–ary coefficients.

Let $\mathcal{C}$ be a linear code and let $\mathcal{C}(\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p)$ be the union of its cosets with syndromes $\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p$. If $\mathcal{C}$ is an $[n, n-r]_q$ code with a parity-check matrix $\mathbf{H}$ then

$$\mathcal{C}(\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p) = \{\mathbf{x}\colon\ \mathbf{x} \in \mathcal{E}_q^n, \quad \mathbf{H}\mathbf{x}^T \in \{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p\} \subseteq \mathcal{S}_q^r\} \tag{1}$$

where $\mathcal{E}_q^n$ is the space of n–dimensional row vectors over $\mathbb{F}_q$. Clearly, $\mathcal{C}(\mathbf{0}) = \mathcal{C}$. If all syndromes $\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p$ are distinct, $\mathcal{C}(\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p)$ is an $(n, pq^{n-r})_q$ code. We consider only such situations.

Note that any $(n, M)_q R$ code can be considered in the form $\mathcal{C}(\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p)$. Let $\mathcal{Z}_n$ be the code consisting of the only zero word of length n. We treat $\mathcal{Z}_n$ as the linear $[n, n-n]_q$ code with the identity parity-check matrix. For any $(n, M)_q$ code $\mathcal{V}$ there exist a linear code $\mathcal{C}$ and a syndrome set $\{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p\}$ with $\mathcal{V} = \mathcal{C}(\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p)$. In any case one may put $\mathcal{C} = \mathcal{Z}_n$, $p = M$, and take all transposed words of the code $\mathcal{V}$ as the syndrome set. A similar approach was noted, e.g, in [1] and [8].

FACT 1 *Let $\mathcal{C}$ be an $[n, n-r]_q$ code and let $\{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p\} \subseteq \mathcal{S}_q^r$ be a syndrome set. The covering radius of the code $\mathcal{C}(\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p)$ is the least integer R such that every column of $\mathcal{S}_q^r$ is a sum of a syndrome from $\{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p\}$ with a linear combination of at most R columns of a parity-check matrix of the code $\mathcal{C}$.*

This fact is based on the matrix construction, see [1], [2, Sections 3.5, 3.9], and [8].

2. Constructions of Covering Codes

We describe constructions obtaining new codes from starting ones.

As a *starting code* $\mathcal{V}_0$ we take an $(n_0, pq^{n_0-r_0})_q R$ code with $\mathcal{V}_0 = \mathcal{C}_0(\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p)$ where $\mathcal{C}_0$ is an $[n_0, n_0-r_0]_q$ code and $\{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p\} \subset \mathcal{S}_q^{r_0}$ is a syndrome set. Let $m \geq 2$ be the least integer such that $q^m \geq n_0$. We put $r = r_0 + mR$. A *new code* $\mathcal{V}$ of covering radius $R_\mathcal{V}$ is an $(n, pq^{n-r})_q R_\mathcal{V}$ code with $\mathcal{V} = \mathcal{C}_\mathcal{V}(\mathbf{s}'_1, \mathbf{s}'_2, \ldots, \mathbf{s}'_p)$ where $\mathcal{C}_\mathcal{V}$ is an $[n, n-r]_q$ code, $\{\mathbf{s}'_1, \mathbf{s}'_2, \ldots, \mathbf{s}'_p\} \subset \mathcal{S}_q^r$ is a syndrome set, and

$$\mathbf{s}'_i = \begin{bmatrix} \mathbf{s}_i \\ \mathbf{0} \end{bmatrix} \in \mathcal{S}_q^r,\ i = 1, 2, \ldots, p,\ \mathbf{0} \in \mathcal{S}_q^{mR}. \tag{2}$$

The value of n will be considered later.

If the starting code is linear then the new code is linear as well and we have $p = 1$, $\{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p\} = \{\mathbf{0}\}$, $\mathcal{C}_0$ is an $[n_0, n_0 - r_0]_q R$ code, $\mathcal{V}_0 = \mathcal{C}_0$, $\mathcal{C}_\mathcal{V}$ is an $[n, n-r]_q R_\mathcal{V}$ code, $\{\mathbf{s}'_1, \mathbf{s}'_2, \ldots, \mathbf{s}'_p\} = \{\mathbf{0}\}$, $\mathcal{V} = \mathcal{C}_\mathcal{V}$.

To design a parity-check matrix of the code $\mathcal{C}_\mathcal{V}$ we use matrices $\mathbf{G}_k$, $\mathbf{H}_1$, and $\mathbf{H}_2$.

Let $k \geq 0$ be an integer. Define an $r \times (R-k)(q^m-1)/(q-1)$ matrix

$$\mathbf{G}_k = \begin{bmatrix} \mathbf{0}^{r_0+km} & \mathbf{0}^{r_0+km} & \ldots & \mathbf{0}^{r_0+km} \\ \mathbf{W}_m & \mathbf{0}^m & \ldots & \mathbf{0}^m \\ \mathbf{0}^m & \mathbf{W}_m & \ldots & \mathbf{0}^m \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0}^m & \mathbf{0}^m & \ldots & \mathbf{W}_m \end{bmatrix} \tag{3}$$

where $\mathbf{W}_m$ is a parity-check matrix of the $[n' = (q^m - 1)/(q - 1), n' - m]_q 1$ Hamming code. In the matrix $\mathbf{G}_k$ the submatrix $\mathbf{W}_m$ is repeated $R - k$ times.

Denote by $\mathbf{H}_0 = [\mathbf{f}_1 \mathbf{f}_2 \ldots \mathbf{f}_{n_0}]$ a parity-check matrix of the code $\mathcal{C}_0$. Here $\mathbf{f}_i \in \mathcal{S}_q^{r_0}$, $i = 1, 2, \ldots, n_0$. Introduce an $r \times n_0 q^m$ matrix

$$\mathbf{H}_1 = \begin{bmatrix} \mathbf{f}_1 & \mathbf{f}_1 & \ldots & \mathbf{f}_1 & |\ldots| & \mathbf{f}_{n_0} & \mathbf{f}_{n_0} & \ldots & \mathbf{f}_{n_0} \\ \xi_1 & \xi_2 & \ldots & \xi_{q^m} & |\ldots| & \xi_1 & \xi_2 & \ldots & \xi_{q^m} \\ \beta_1\xi_1 & \beta_1\xi_2 & \ldots & \beta_1\xi_{q^m} & |\ldots| & \beta_{n_0}\xi_1 & \beta_{n_0}\xi_2 & \ldots & \beta_{n_0}\xi_{q^m} \\ \beta_1^2\xi_1 & \beta_1^2\xi_2 & \ldots & \beta_1^2\xi_{q^m} & |\ldots| & \beta_{n_0}^2\xi_1 & \beta_{n_0}^2\xi_2 & \ldots & \beta_{n_0}^2\xi_{q^m} \\ \vdots & \vdots & \ddots & \vdots & |\ldots| & \vdots & \vdots & \ddots & \vdots \\ \beta_1^{R-1}\xi_1 & \beta_1^{R-1}\xi_2 & \ldots & \beta_1^{R-1}\xi_{q^m} & |\ldots| & \beta_{n_0}^{R-1}\xi_1 & \beta_{n_0}^{R-1}\xi_2 & \ldots & \beta_{n_0}^{R-1}\xi_{q^m} \end{bmatrix} \tag{4}$$

where $\{\xi_1, \xi_2, \ldots, \xi_{q^m}\} = \mathbb{F}_{q^m}$, $\{\beta_1, \beta_2, \ldots, \beta_{n_0}\} \subseteq \mathbb{F}_{q^m}$, $\beta_i \neq \beta_j$ if $i \neq j$.

To design $\mathbf{H}_2$ we need an auxiliary linear code of covering radius 2 and codimension m. Assume that there exists an $[n_m, n_m - m]_q 2$ code $\mathcal{Q}_m$ with a parity-check matrix $\mathbf{A}_m = [\mathbf{a}_1\ \mathbf{a}_2\ \ldots\ \mathbf{a}_{n_m}]$, $\mathbf{a}_i \in \mathcal{S}_q^m$, $i = 1, 2, \ldots, n_m$. Let $\Delta = q^m - n_0$. For $\Delta > 0$ we define an $r \times \Delta n_m$ matrix

$$\mathbf{H}_2 = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} & |\ldots| & \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} \\ \mathbf{a}_1 & \mathbf{a}_2 & \ldots & \mathbf{a}_{n_m} & |\ldots| & \mathbf{a}_1 & \mathbf{a}_2 & \ldots & \mathbf{a}_{n_m} \\ \beta_{n_0+1}\mathbf{a}_1 & \beta_{n_0+1}\mathbf{a}_2 & \ldots & \beta_{n_0+1}\mathbf{a}_{n_m} & |\ldots| & \beta_{n_0+\Delta}\mathbf{a}_1 & \beta_{n_0+\Delta}\mathbf{a}_2 & \ldots & \beta_{n_0+\Delta}\mathbf{a}_{n_m} \\ \beta_{n_0+1}^2\mathbf{a}_1 & \beta_{n_0+1}^2\mathbf{a}_2 & \ldots & \beta_{n_0+1}^2\mathbf{a}_{n_m} & |\ldots| & \beta_{n_0+\Delta}^2\mathbf{a}_1 & \beta_{n_0+\Delta}^2\mathbf{a}_2 & \ldots & \beta_{n_0+\Delta}^2\mathbf{a}_{n_m} \\ \vdots & \vdots & \ddots & \vdots & |\ldots| & \vdots & \vdots & \ddots & \vdots \\ \beta_{n_0+1}^{R-1}\mathbf{a}_1 & \beta_{n_0+1}^{R-1}\mathbf{a}_2 & \ldots & \beta_{n_0+1}^{R-1}\mathbf{a}_{n_m} & |\ldots| & \beta_{n_0+\Delta}^{R-1}\mathbf{a}_1 & \beta_{n_0+\Delta}^{R-1}\mathbf{a}_2 & \ldots & \beta_{n_0+\Delta}^{R-1}\mathbf{a}_{n_m} \end{bmatrix} \tag{5}$$

where $\mathbf{0} \in \mathcal{S}_q^{r_0}$, $\{\beta_{n_0+1}, \beta_{n_0+2}, \ldots, \beta_{n_0+\Delta}\} \subset \mathbb{F}_{q^m}$, $\beta_i \neq \beta_j$ if $i \neq j$. We put

$$\{\beta_1, \beta_2, \ldots, \beta_{n_0+\Delta}\} = \mathbb{F}_{q^m}. \tag{6}$$

Remark 1. We call an element β_i an *indicator* of the corresponding submatrix of the matrix $\mathbf{H}_1$ or $\mathbf{H}_2$. The condition (6) gives a *complete set of indicators* (CSI). CSI is important for constructions of this work, see below proofs of Theorems 1–3. In [3]–[5] and [9, Supplement, Statement 6] CSI is used for $n_0 \geq q^m$ or $n_0 \geq q^m + 1$. Theorems 1 and 2 of this work develop CSI approach for $n_0 \leq q^m$. Theorem 3 gives a new construction with CSI for $n_0 \geq q^m + 1$. An important new element of constructions proposed in Theorems 1–3 is matrices $\mathbf{H}_2$ and $\mathbf{H}_3$, see below, based on a parity-check matrix of an $[n_m, n_m - m]_q 2$ code.

THEOREM 1 *Let $q \geq 2$, $R \geq 2$, and let the parity-check matrix $\mathbf{H}_\mathcal{V}$ of the code $\mathcal{C}_\mathcal{V}$ have the form*

$$\mathbf{H}_\mathcal{V} = [\mathbf{G}_1\, \mathbf{H}_1\, \mathbf{H}_2] \text{ for } \Delta > 0, \quad \mathbf{H}_\mathcal{V} = [\mathbf{G}_1\, \mathbf{H}_1] \text{ for } \Delta = 0. \tag{7}$$

Then the new code has the same covering radius as the starting code and length $n = n_0 q^m + \Delta n_m + (R - 1)(q^m - 1)/(q - 1)$.

Proof. The value of n follows directly from (3)–(5) and (7).

Let $z < R$. By Fact 1, there is a column $\mathbf{b} \in \mathcal{S}_q^{r_0}$ that cannot be represented by a sum of a syndrome from $\{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p\}$ and a linear combination of z columns of $\mathbf{H}_0$. Hence the column $(\mathbf{b}, \mathbf{u})^T \in \mathcal{S}_q^r$, where T is the symbol of transposition and $\mathbf{u} \in \mathcal{S}_q^{mR}$, cannot be written as a sum of a syndrome from $\{\mathbf{s}'_1, \mathbf{s}'_2, \ldots, \mathbf{s}'_p\}$ and a linear combination of z columns of $\mathbf{H}_\mathcal{V}$, see (2) and (7). So, $R_\mathcal{V} \geq R$.

Using Fact 1 we will show that $R_\mathcal{V} = R$.

Let $(\mathbf{b}, \mathbf{u})^T$ be an *arbitrary* column of $\mathcal{S}_q^r$ with $\mathbf{b} \in \mathcal{S}_q^{r_0}$, $\mathbf{u} = (\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_R)^T \in \mathcal{S}_q^{mR}$, $\mathbf{u}_i \in \mathcal{S}_q^m$, $i = 1, 2, \ldots, R$. Denote by $\mathbf{u}^*(f) = (\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_f, \mathbf{u}^*_{f+1}, \mathbf{u}^*_{f+2}, \ldots, \mathbf{u}^*_R)^T$ a column of $\mathcal{S}_q^{mR}$ such that the first f its positions coincide with those of the column $\mathbf{u}$ and $\mathbf{u}^*_i \in \mathcal{S}_q^m$, $i = f+1, f+2, \ldots, R$. Let $\mathbf{u}'(f) = (\underbrace{\mathbf{0}, \ldots, \mathbf{0}}_{f}, \mathbf{u}'_{f+1}, \mathbf{u}'_{f+2}, \ldots, \mathbf{u}'_R)^T \in \mathcal{S}_q^{mR}$ be a column with $\mathbf{0} \in \mathcal{S}_q^m$, $\mathbf{u}'_i = \mathbf{u}_i - \mathbf{u}^*_i$, $i = f+1, f+2, \ldots, R$. Obviously $(\mathbf{b}, \mathbf{u})^T = (\mathbf{b}, \mathbf{u}^*(f))^T + (\mathbf{0}, \mathbf{u}'(f))^T$ where $\mathbf{0} \in \mathcal{S}_q^{r_0}$. By (3) and (7), for $f \in \{1, 2, \ldots, R-1\}$ every column $(\mathbf{0}, \mathbf{u}'(f))^T \in \mathcal{S}_q^r$ can be represented as a linear combination of at most $R - f$ columns of the submatrix $\mathbf{G}_1$. Hence to prove the equality $R_\mathcal{V} = R$ we should write an arbitrary column $(\mathbf{b}, \mathbf{u}^*(f))^T$, $f \in \{1, 2, \ldots, R\}$, as a sum of a syndrome $\mathbf{s}'_{i(\mathbf{b})} \in \{\mathbf{s}'_1, \mathbf{s}'_2, \ldots, \mathbf{s}'_p\}$ with a linear combination of at most f columns of the matrix $\mathbf{H}_\mathcal{V}$. We find this representation in the form

$$\begin{bmatrix} \mathbf{b} \\ \mathbf{u}^*(f) \end{bmatrix} = \begin{bmatrix} \mathbf{s}_{i(\mathbf{b})} \\ \mathbf{0} \end{bmatrix} + \sum_{k=1}^{z} \gamma_k \begin{bmatrix} \mathbf{f}_{j_k} \\ \mathbf{t}_{j_k i_k} \end{bmatrix} + \sum_{l=1}^{z^\bullet} \gamma_l^\bullet \begin{bmatrix} \mathbf{0} \\ \mathbf{t}^\bullet_{h_l c_l} \end{bmatrix} \tag{8}$$

where $\mathbf{s}_i(\mathbf{b}) \in \{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p\}$, $(\mathbf{s}_{i(\mathbf{b})}, \mathbf{0})^T = \mathbf{s}'_{i(\mathbf{b})} \in \mathcal{S}_q^r$, $(\mathbf{f}_{j_k}, \mathbf{t}_{j_k i_k})^T$ is a column of $\mathbf{H}_1$, $\mathbf{t}_{j_k i_k} = (\xi_{i_k}, \beta_{j_k}\xi_{i_k}, \beta_{j_k}^2\xi_{i_k}, \ldots, \beta_{j_k}^{R-1}\xi_{i_k})^T \in \mathcal{S}_q^{mR}$, $(\mathbf{0}, \mathbf{t}^\bullet_{h_l c_l})^T$ is a column of $\mathbf{H}_2$, $\mathbf{t}^\bullet_{h_l c_l} = (\mathbf{a}_{c_l}, \beta_{h_l}\mathbf{a}_{c_l}, \beta_{h_l}^2\mathbf{a}_{c_l}, \ldots, \beta_{h_l}^{R-1}\mathbf{a}_{c_l})^T \in \mathcal{S}_q^{mR}$, $\gamma_k, \gamma_l^\bullet \in \mathbb{F}_q^*$ for all k, l.

We should show that always there is a representation with $z + z^\bullet \leq f$.

The starting code $\mathcal{V}_0$ has covering radius R. By Fact 1, we can find a syndrome $\mathbf{s}_{i(\mathbf{b})}$, columns $\mathbf{f}_{j_k}$, and coefficients $\gamma_k \in \mathbb{F}_q^*$ such that

$$\mathbf{b} = \mathbf{s}_{i(\mathbf{b})} + \sum_{k=1}^{z'} \gamma_k \mathbf{f}_{j_k}, \quad \mathbf{s}_{i(\mathbf{b})} \in \{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p\}, \quad z' \in \{0, 1 \ldots, R\}. \tag{9}$$

1) Assume $z' \in \{1, 2, \ldots, R\}$ in (9). Then in (8) we use $\mathbf{s}_{i(\mathbf{b})}$, j_k, and γ_k from (9) and put $z = z'$, $f = z'$, $z^\bullet = 0$. "Locations" ξ_{i_k} of columns $(\mathbf{f}_{j_k}, \mathbf{t}_{j_k i_k})^T$ in (8) are a solution of the linear system

$$\sum_{k=1}^{z} \gamma_k \beta_{j_k}^{v-1} \xi_{i_k} = \mathbf{u}_v, \; v = 1, 2, \ldots, z. \tag{10}$$

The determinant of the system is nonzero since we have the Vandermonde matrix with distinct elements β_{j_k}.

2) Assume $z' = 0$ in (9). Then $\mathbf{b} = \mathbf{s}_{i(\mathbf{b})}$ in (8) and (9).

Assume $\mathbf{u}_1 = 0$. In (8) we put $f = 1$, $z = z^\bullet = 0$, $(\mathbf{b}, \mathbf{u}^*(1))^T = (\mathbf{s}_{i(\mathbf{b})}, \mathbf{0})^T$.

Assume $\mathbf{u}_1 \neq 0$. We put $f = 2$ in (8). Since $\{\beta_1, \beta_2, \ldots, \beta_{n_0+\Delta}\} = \mathbb{F}_{q^m}$, for $\mathbf{u}_1 \neq \mathbf{0}$ we always can find d with $\mathbf{u}_2 = \beta_d \mathbf{u}_1$. If $d \le n_0$ we put in (8) $z = 2$, $z^\bullet = 0$, $j_1 = j_2 = d$, $\xi_{i_1} = \mathbf{u}_1$, $\xi_{i_2} = 0$, $\gamma_1 = 1$, $\gamma_2 = -1$,

$$(\mathbf{b}, \mathbf{u}^*(2))^T = (\mathbf{s}_{i(\mathbf{b})}, \mathbf{0})^T + (\mathbf{f}_d, \mathbf{u}_1, \beta_d \mathbf{u}_1, \ldots)^T - (\mathbf{f}_d, \mathbf{0}, \mathbf{0}, \ldots)^T. \tag{11}$$

If $d \ge n_0 + 1$ then in (8) we take $z = 0$, $z^\bullet \le 2$, $h_1 = h_2 = d$. Since $\mathcal{Q}_m$ is a code with covering radius 2, each column of $\mathcal{S}_q^m$ is equal to a linear combination of at most 2 columns of the parity-check matrix $\mathbf{A}_m$. Hence we can find columns $\mathbf{a}_{c_l}$ of $\mathbf{A}_m$ and coefficients $\gamma_l^\bullet \in \mathbb{F}_q^*$ so that $\mathbf{u}_1 = \gamma_1^\bullet \mathbf{a}_{c_1} + \gamma_2^\bullet \mathbf{a}_{c_2}$ where the second summand can be absent. Since $\mathbf{u}_2 = \beta_d \mathbf{u}_1$, we have $\mathbf{u}_2 = \gamma_1^\bullet \beta_d \mathbf{a}_{c_1} + \gamma_2^\bullet \beta_d \mathbf{a}_{c_2}$. Finally,

$$(\mathbf{b}, \mathbf{u}^*(2))^T \ = \ (\mathbf{s}_{i(\mathbf{b})}, \mathbf{0}_1)^T + \gamma_1^\bullet(\mathbf{0}, \mathbf{a}_{c_1}, \beta_d \mathbf{a}_{c_1}, \ldots)^T + \gamma_2^\bullet(\mathbf{0}, \mathbf{a}_{c_2}, \beta_d \mathbf{a}_{c_2}, \ldots)^T. \tag{12}$$

■

Remark 2. We need CSI when in (9) $z' = 0$. If $d \le n_0$ and β_d is an indicator of a submatrix of $\mathbf{H}_1$ we use (11) where a linear combination of *two* columns presents. Hence if $n_0 < q^m$ and the matrix $\mathbf{H}_1$ does not provide CSI we can take a supplementary matrix $\mathbf{H}_2$ based on a parity-check matrix of a code with covering radius 2, cf. (11) and (12).

Define an $r \times n_m$ matrix

$$\mathbf{H}_3 = \begin{bmatrix} \mathbf{0}^{r_0+m} \\ \mathbf{A}_m \\ \mathbf{0}^{(R-2)m} \end{bmatrix}. \tag{13}$$

THEOREM 2 *Let $q = 2^i$, $i \ge 1$, $R \ge 3$, and let the parity-check matrix $\mathbf{H}_\mathcal{V}$ of the code $\mathcal{C}_\mathcal{V}$ have the form*

$$\mathbf{H}_\mathcal{V} = [\mathbf{G}_2\, \mathbf{H}_1\, \mathbf{H}_2\, \mathbf{H}_3] \ \textit{for}\ \Delta > 0, \quad \mathbf{H}_\mathcal{V} = [\mathbf{G}_2\, \mathbf{H}_1\, \mathbf{H}_3] \ \textit{for}\ \Delta = 0. \tag{14}$$

Then the new code has the same covering radius as the starting code and length $n = n_0 q^m + (\Delta + 1)n_m + (R-2)(q^m - 1)/(q-1)$.

Proof. The value of n follows directly from (3)–(5), (13), and (14).

For an arbitrary column $(\mathbf{b}, \mathbf{u})^T \in \mathcal{S}_q^r$ we use the same approach as in the proof of Theorem 1 with columns $\mathbf{u}^*(f)$ and $\mathbf{u}'(f)$ and representations of (8) and (9). By (3) and (14), for $f \in \{2, 3, \ldots, R-1\}$ every column $(\mathbf{0}, \mathbf{u}'(f))^T \in \mathcal{S}_q^r$ can be written as a linear combination of at most $R - f$ columns of the submatrix $\mathbf{G}_2$. But it does not hold for a column $(\mathbf{0}, \mathbf{u}'(1))^T$ with $f = 1$. If in (9) $z' \in \{2, 3, \ldots, R\}$ or $z' = 0$ and $\mathbf{u}_1 \neq 0$ then Theorem 2 can be proved similarly to Theorem 1 since its proof does not use $f = 1$ in these cases. But situations when we put $f = 1$ in the proof of Theorem 1 should be proved in Theorem 2 by another way.

1) Assume that in (9) $z' = 0$, $\mathbf{b} = \mathbf{s}_{i(\mathbf{b})}$. Let $\mathbf{u}_1 = 0$.

We find columns $\mathbf{a}_{t_e}$ and coefficients $\mu_e \in \mathbb{F}_q^*$ so that $\mathbf{u}_2 = \mu_1 \mathbf{a}_{t_1} + \mu_2 \mathbf{a}_{t_2}$ where the second summand can be absent. We put $f = 2$, use the submatrix $\mathbf{H}_3$, and write

$$(\mathbf{b}, \mathbf{u}^*(2))^T = (\mathbf{s}_{i(\mathbf{b})}, \mathbf{0})^T + \mu_1(\mathbf{0}, \mathbf{0}, \mathbf{a}_{t_1}, \mathbf{0}, \ldots)^T + \mu_2(\mathbf{0}, \mathbf{0}, \mathbf{a}_{t_2}, \mathbf{0}, \ldots)^T.$$

2) Assume that in (9) $z' = 1$, $\mathbf{b} = \mathbf{s}_{i(\mathbf{b})} + \gamma_1 \mathbf{f}_{j_1}$.

a) Assume $\mathbf{u}_2 = \beta_{j_1}\mathbf{u}_1$.

In (8) we put $f = 2$, $z = 1$, $z^\bullet = 0$, $\xi_{i_1} = \gamma_1^{-1}\mathbf{u}_1$,

$$(\mathbf{b}, \mathbf{u}^*(2))^T = (\mathbf{s}_{i(\mathbf{b})}, \mathbf{0})^T + \gamma_1(\mathbf{f}_{j_1}, \gamma_1^{-1}\mathbf{u}_1, \beta_{j_1}\gamma_1^{-1}\mathbf{u}_1, \dots)^T. \tag{15}$$

b) Assume $\mathbf{u_2} \neq \beta_{j_1}\mathbf{u}_1$ and $\mathbf{u_3} \neq \beta_{j_1}^2\mathbf{u}_1$,

In (8) we put $f = 3$. We find ξ_{i_1}, λ, and π from the nonlinear system

$$\gamma_1\beta_{j_1}^{v-1}\xi_{i_1} + \lambda^{v-1}\pi = \mathbf{u}_v, \quad v = 1, 2, 3, \quad \xi_{i_1}, \lambda, \pi \in \mathbb{F}_{q^m}. \tag{16}$$

It can be shown that for odd q the system of (16) has no solution over $\mathbb{F}_{q^m}$ if $\mathbf{u}_3 = 2\beta_{j_1}\mathbf{u}_2 - \beta_{j_1}^2\mathbf{u}_1$. For even $q = 2^i$ we have the solution

$$\lambda = \frac{\mathbf{u}_3 + \beta_{j_1}\mathbf{u}_2}{\mathbf{u}_2 + \beta_{j_1}\mathbf{u}_1}, \quad \xi_{i_1} = \frac{\lambda\mathbf{u}_1 + \mathbf{u}_2}{\gamma_1(\beta_{j_1} + \lambda)}, \quad \pi = \frac{\beta_{j_1}\mathbf{u}_1 + \mathbf{u}_2}{\beta_{j_1} + \lambda}. \tag{17}$$

Since $\{\beta_1, \beta_2, \dots, \beta_{n_0+\Delta}\} = \mathbb{F}_{q^m}$ we can always find d with $\beta_d = \lambda$. Taking into account that $\mathbf{u}_3 \neq \beta_{j_1}^2\mathbf{u}_1$ we have $\lambda \neq \beta_{j_1}$, $d \neq j_1$. If $d \leq n_0$ then in (8) we put $z = 3$, $z^\bullet = 0$, $j_2 = j_3 = d$, $\xi_{i_2} = \pi$, $\xi_{i_3} = 0$, $\gamma_2 = \gamma_3 = 1$,

$$\begin{aligned}(\mathbf{b}, \mathbf{u}^*(3))^T &= (\mathbf{s}_{i(\mathbf{b})}, \mathbf{0})^T + \gamma_1(\mathbf{f}_{j_1}, \xi_{i_1}, \beta_{j_1}\xi_{i_1}, \beta_{j_1}^2\xi_{i_1}, \dots)^T \\ &\quad + (\mathbf{f}_d, \pi, \lambda\pi, \lambda^2\pi, \dots)^T + (\mathbf{f}_d, \mathbf{0}, \mathbf{0}, \mathbf{0}, \dots)^T.\end{aligned} \tag{18}$$

If $d \geq n_0 + 1$ we find columns $\mathbf{a}_{c_l}$ and coefficients $\gamma_l^\bullet \in \mathbb{F}_q^*$ so that $\pi = \gamma_1^\bullet\mathbf{a}_{c_1} + \gamma_2^\bullet\mathbf{a}_{c_2}$ where the second summand can be absent. In (8) we put $z = 1$, $z^\bullet \leq 2$, $h_1 = h_2 = d$,

$$\begin{aligned}(\mathbf{b}, \mathbf{u}^*(3))^T &= (\mathbf{s}_{i(\mathbf{b})}, \mathbf{0})^T + \gamma_1(\mathbf{f}_{j_1}, \xi_{i_1}, \beta_{j_1}\xi_{i_1}, \beta_{j_1}^2\xi_{i_1}, \dots)^T \\ &\quad + \gamma_1^\bullet(\mathbf{0}, \mathbf{a}_{c_1}, \lambda\mathbf{a}_{c_1}, \lambda^2\mathbf{a}_{c_1}, \dots)^T + \gamma_2^\bullet(\mathbf{0}, \mathbf{a}_{c_2}, \lambda\mathbf{a}_{c_2}, \lambda^2\mathbf{a}_{c_2}, \dots)^T.\end{aligned} \tag{19}$$

c) Assume $\mathbf{u}_2 \neq \beta_{j_1}\mathbf{u}_1$ and $\mathbf{u}_3 = \beta_{j_1}^2\mathbf{u}_1$.

We find columns $\mathbf{a}_{w_e}$ and coefficients $\delta_e \in \mathbb{F}_q^*$ so that $\beta_{j_1}\mathbf{u}_1 + \mathbf{u}_2 = \delta_1\mathbf{a}_{w_1} + \delta_2\mathbf{a}_{w_2}$ where the second summand can be absent. We put $f = 3$, use $\mathbf{H}_3$, and obtain

$$\begin{aligned}(\mathbf{b}, \mathbf{u}^*(3))^T &= (\mathbf{s}_{i(\mathbf{b})}, \mathbf{0})^T + \gamma_1(\mathbf{f}_{j_1}, \gamma_1^{-1}\mathbf{u}_1, \beta_{j_1}\gamma_1^{-1}\mathbf{u}_1, \beta_{j_1}^2\gamma_1^{-1}\mathbf{u}_1, \dots)^T \\ &\quad + \delta_1(\mathbf{0}, \mathbf{0}, \mathbf{a}_{w_1}, \mathbf{0}, \dots)^T + \delta_2(\mathbf{0}, \mathbf{0}, \mathbf{a}_{w_2}, \mathbf{0}, \dots)^T.\end{aligned} \tag{20}$$

$\blacksquare$

Remark 3. Let α, β, γ, δ, $\xi \in \mathbb{F}_{q^m}$. We can treat vectors (α, β, γ) placed on positions $r_0 + 1, \dots, r_0 + 3m$ of columns of $\mathbf{H}_\mathcal{V}$, see (14), as points of a projective plane $PG(2, q^m)$ [7]. Vectors (α, β, γ) and $\delta(\alpha, \beta, \gamma)$ correspond to the same point. For even q^m a hyperoval $\mathcal{O}$ consists of $q^m + 2$ distinct points of the form $(\mathbf{0}, \mathbf{0}, \xi)$, see $\mathbf{G}_2$, $(\mathbf{0}, \xi, \mathbf{0})$, see $\mathbf{H}_3$, and $(\xi, \xi\beta, \xi\beta^2)$, see $[\mathbf{H}_1\ \mathbf{H}_2]$ where all q^m such points present due to CSI. A hyperoval has no unisecants. Hence if we fix a point $P \in \mathcal{O}$ then every point of the plane lies on a bisecant of $\mathcal{O}$ through P. When in (9) $z' = 1$ we take $P = \gamma_1(\xi, \xi\beta_{j_1}, \xi\beta_{j_1}^2)$ and find the second point $P' \in \mathcal{O}$ to pass a bisecant on which the point $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ lies. For even q^m with CSI we always can find P' since we have a whole hyperoval. The situations of (15), (16), and (20) correspond to distinct forms of P'. For odd q^m we have an oval consisting of $q^m + 1$ points. Every point of the oval has one unisecant. If a point $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3)$ lies on the unisecant through P then the system of (16) has no solution.

Now we develop the approach of Theorem 2 for $n_0 \geq q^m + 1$ and give one more new construction with CSI. Assume that there is a partition $\mathcal{K}$ of the column set of the parity-check matrix $\mathbf{H}_0$ into h nonempty subsets such that every column of $\mathcal{S}_q^{r_0}$ is a sum of a syndrome from $\{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_p\}$ with a linear combination of at most R columns of $\mathbf{H}_0$ from *distinct subsets*. We call $\mathcal{K}$ an R–parition. Assume also that there is an integer m with $n_0 \geq q^m + 1 \geq h$ and take this m to design the new code $\mathcal{V}$ instead of m with $q^m \geq n_0$ as in Theorems 1 and 2.

Let $g < n_0$ be an integer and let columns $\mathbf{f}_{g+1}, \mathbf{f}_{g+2}, \ldots, \mathbf{f}_{n_0}$ are a subset of $\mathcal{K}$. We define an $r \times gq^m$ matrix $\mathbf{H}'_g$ as the first g sections of the matrix $\mathbf{H}_1$ with columns $\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_g$. In the matrix $\mathbf{H}'_g$ we put $\beta_i \neq \beta_j$ if columns $\mathbf{f}_i$ and $\mathbf{f}_j$ belong to distinct subsets of $\mathcal{K}$ but it is possible that $\beta_i = \beta_j$ if $\mathbf{f}_i$ and $\mathbf{f}_j$ belong to the same subset. Besides in $\mathbf{H}'_g$ we put $\{\beta_1, \beta_2, \ldots, \beta_g\} = \mathbb{F}_{q^m}$. Introduce an $r \times (n_0 - g)q^m$ matrix

$$\mathbf{H}''_g = \begin{bmatrix} \mathbf{f}_{g+1} & \mathbf{f}_{g+1} & \ldots & \mathbf{f}_{g+1} & | & \ldots & | & \mathbf{f}_{n_0} & \mathbf{f}_{n_0} & \ldots & \mathbf{f}_{n_0} \\ \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} & | & \ldots & | & \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots & | & \ldots & | & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} & | & \ldots & | & \mathbf{0} & \mathbf{0} & \ldots & \mathbf{0} \\ \xi_1 & \xi_2 & \ldots & \xi_{q^m} & | & \ldots & | & \xi_1 & \xi_2 & \ldots & \xi_{q^m} \end{bmatrix} \tag{21}$$

where $\{\xi_1, \xi_2, \ldots, \xi_{q^m}\} = \mathbb{F}_{q^m}$, $\mathbf{0} \in \mathcal{S}_q^m$.

THEOREM 3 *Let $q = 2^i$, $i \geq 1$, $R \geq 4$, and let the parity-check matrix $\mathbf{H}_\mathcal{V}$ of the code $\mathcal{C}_\mathcal{V}$ have the form*

$$\mathbf{H}_\mathcal{V} = [\mathbf{G}_2 \mathbf{H}'_g \mathbf{H}''_g \mathbf{H}_3]. \tag{22}$$

Then the new code has the same covering radius as the starting code and length $n = n_0 q^m + n_m + (R-2)(q^m - 1)/(q-1)$.

Proof. The value of n follows directly from (3), (4), (13), (21), and (22).

For an arbitrary column $(\mathbf{b}, \mathbf{u})^T \in \mathcal{S}_q^r$ we use the same approach as in the proofs of Theorems 1 and 2 with columns $\mathbf{u}^*(f)$ and $\mathbf{u}'(f)$ and representations of (8) and (9). In (9) we take columns $\mathbf{f}_{j_k}$ from distinct subsets of $\mathcal{K}$. It means that in the correponding system (10) all elements β_{j_k} are distinct and the determinant is nonzero.

Since $\{\beta_1, \beta_2, \ldots, \beta_g\} = \mathbb{F}_{q^m}$, we always have $d \leq g$ when we find d with $\mathbf{u}_2 = \beta_d \mathbf{u}_1$ or with $\beta_d = \lambda$, see (11) and (18). So, we do not need the matrix $\mathbf{H}_2$ and can use the proofs of Theorems 1 and 2 for $\Delta = 0$.

Assume that in (9) $z' = 0$ or $z' \in \{1, 2, \ldots, R\}$, $j_k \leq g$, $k = 1, 2, \ldots, z'$. Then Theorem 3 can be proved similarly to Theorem 2.

Assume that in (9) $z' \in \{1, 2, \ldots, R\}$, $j_{z'} \in \{g+1, g+2, \ldots, n_0\}$. Then

$$(\mathbf{b}, \mathbf{u})^T = (\mathbf{b} - \gamma_{z'}\mathbf{f}_{j_{z'}}, \mathbf{u}^*(R-1))^T + \gamma_{z'}(\mathbf{f}_{j_{z'}}, \gamma_{z'}^{-1}\mathbf{u}'(R-1))^T$$

where $\gamma_{z'}$ and $j_{z'}$ are taken from (9) and $(\mathbf{f}_{j_{z'}}, \gamma_{z'}^{-1}\mathbf{u}'(R-1))^T$ is a column of $\mathbf{H}_g''$. The column $(\mathbf{b} - \gamma_{z'}\mathbf{f}_{j_{z'}}, \mathbf{u}^*(R-1))^T$ can be represented as a sum of the syndrome $\mathbf{s}'_{i(\mathbf{b})} = (\mathbf{s}_{i(\mathbf{b})}, \mathbf{0})^T$, see (9), with a linear combination of at most $R-1$ columns of the matrix $[\mathbf{G}_2\mathbf{H}'_g\mathbf{H}_3]$. For this we use the same way as for a representation of an arbitrary column of $\mathcal{S}_q^{r_0+(R-1)m}$ in Theorem 2 with covering radius $R-1$. It is possible since in Theorem 3 we have $R \geq 4$. Hence $R-1 \geq 3$ and the structure of upper $r_0 + (R-1)m$ rows of the matrix $[\mathbf{G}_2\mathbf{H}'_g\mathbf{H}_3]$ is the same as that of the matrix $[\mathbf{G}_2\mathbf{H}_1\mathbf{H}_3]$ in Theorem 2 with covering radius $R-1$. ■

Now we describe a construction based on [5, Theorems 4.1, 5.1]. Here $R \geq 3$, $q = 2$, and $\mathcal{V}_0 = \mathcal{C}_0$, i.e., the starting code is a linear $[n_0, n_0 - r_0]_2 R$ code. Let $l \in \{1, 2, \ldots, R\}$ be an integer. We assume that there is a partition $\mathcal{K}$ of the column set of the matrix $\mathbf{H}_0$ into h nonempty subsets such that every column of $\mathcal{S}_2^{r_0}$ is a sum of at least l and at most R columns from *distinct susbsets*. Denote such code $\mathcal{C}_0$ by an $[n_0, n_0 - r_0]_2 R, l$ code and the partition $\mathcal{K}$ by an R, l–partition. We take integer m with $2^m \geq h$ and as usually put $r = r_0 + mR$. The new code $\mathcal{V}$ is linear as well. We have $\mathcal{V} = \mathcal{C}_{\mathcal{V}}$. For this construction in the matrix $\mathbf{H}_1$ we put $\beta_i \neq \beta_j$ if columns $\mathbf{f}_i$ and $\mathbf{f}_j$ belong to distinct subsets of $\mathcal{K}$ but it is possible that $\beta_i = \beta_j$ if $\mathbf{f}_i$ and $\mathbf{f}_j$ belong to the same subset.

THEOREM 4 *Let $q = 2$, $R \geq 3$. and let a parity-check matrix $\mathbf{H}_{\mathcal{V}}$ of the new code $\mathcal{V} = \mathcal{C}_{\mathcal{V}}$ have the form*

$$\mathbf{H}_{\mathcal{V}} = [\mathbf{G}_l\mathbf{H}_1]. \tag{23}$$

Then the new code is an $[n, n-r]_2 R$ code with $n = 2^m(n_0 + R - l) - (R - l)$.

Proof. The value of n follows directly from (3), (4), and (23).

We use the approach of Theorem 1 with columns $(\mathbf{b}, \mathbf{u})^T$, $\mathbf{u}^*(f)$, and $\mathbf{u}'(f)$ and representations of (8) and (9) where syndromes $\mathbf{s}_{i(\mathbf{b})}$ and $\mathbf{s}'_{i(\mathbf{b})}$ and columns from $\mathbf{H}_2$ are absent. Every column $(\mathbf{0}, \mathbf{u}'(f))^T$ with $f \in \{l, l+1, \ldots, R-1\}$ is a sum of at most $R - f$ columns of $\mathbf{G}_l$. Since $\mathcal{C}_0$ is an $[n_0, n_0 - r_0]_2 R, l$ code, in (9) we can get $z' \in \{l, l+1, \ldots, R\}$ and take columns $\mathbf{f}_{j_k}$ from distinct subsets of the R, l–partition $\mathcal{K}$. Hence in the corresponding system (10) all elements β_{j_k} are distinct and the determinant is nonzero. We put in (8) $z = z'$, $f = z'$, $z^\bullet = 0$, and consider the system (10) similarly to point 1) in the proof of Theorem 1. ■

The condition $2^m \geq h$ bounds m only from below. Hence Theorem 4 gives an infinite family of new codes.

3. New Covering Codes

Denote by $\mu_q(n, R, \mathcal{C})$ the covering density of an $(n, M(\mathcal{C}))_q R$ code $\mathcal{C}$. We have

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

For an infinite family $\mathcal{A}$ consisting of $(n, M(\mathcal{A}_n))_q R$ codes $\mathcal{A}_n$ we consider the value

$$\bar{\mu}_q(R, \mathcal{A}) = \liminf_{n\to\infty} \mu_q(n, R, \mathcal{A}_n).$$

FACT 2 *If an* $(n, M)_q R$ *(respectively* $[n, n-r]_q R$*) code exists then an* $(n+1, qM)_q R$ *(respectively* $[n+1, n+1-r]_q R$*) code exists.*

Example 1. We consider $R = 3$, $q = 2$. Let $\mathcal{V}_0$ be the $(n_0, 2^{n_0-3v})_2 3$ code $D(v)$ of [6, Theorem 8] where $n_0 = 2^{v+1} - 1$, $v \geq 4$ is even. So $p = 1$, $r_0 = 3v$. We use Theorem 2 with $m = v+1$, $\Delta = 1$, and take the $[n_{v+1}, n_{v+1} - (v+1)]_2 2$ code of [2, Theorem 5.4.27] with $n_{v+1} = 5 \cdot 2^{v/2-1} - 1$ as the code $\mathcal{Q}_{v+1}$. We obtain an infinite family $\mathcal{A}_1$ of new $(n, M)_2 3$ codes with parameters

$$R = 3, q = 2, n = 2^{2v+2} + 5 \cdot 2^{v/2} - 3, M = 2^{n-3(2v+1)}, \bar{\mu}_2(3, \mathcal{A}_1) \approx 4/3.$$

Note that in [4, eq. (5)] the $(n', 2^{n'-3(2v+1)})_2 3$ codes are given with $n' = 2^{2v+2} + 27 \cdot 2^{v-3} - 2$, $v \geq 4$ is even. The best known codes of length $n = 2^{2v+2} + 5 \cdot 2^{v/2} - 3$ are $(n, 2^{n-3(2v+1)+1})_2 3$ codes obtained by Fact 2 from the codes of [5, eq. (1.4)].

Example 2. We consider $R = 2$, $q = 2$. Let $\mathcal{V}_0$ be the $(7, 7)_2 2$ code of [2, Table 6.1]. We put $p = 7$, $r_0 = n_0 = 7$, $\mathcal{C}_0 = \mathcal{Z}_7$. We use Theorem 1 with $m = 3$, $\Delta = 1$, take the $[4, 1]_2 2$ repetition code as the code $\mathcal{Q}_3$, and obtain a new $(67, 7 \cdot 2^{54})_2 2$ code. The best known codes of length 67 is a $[67, 57]_2 2$ code obtained by Fact 2 from the $[53, 43]_2 2$ code of [2, Table 7,3].

Example 3. We consider $R = 2$, $q = 4$. Let $\mathcal{V}_0$ be the $(14, 3 \cdot 4^9)_4 2$ code that is the direct sum of the $(5, 4^3)_4 1$ Hamming code and the $(9, 3 \cdot 4^6)_4 1$ code of [2, Table 6.3]. We put $p = 3 \cdot 4^9$, $r_0 = n_0 = 14$, $\mathcal{C}_0 = \mathcal{Z}_{14}$. We use Theorem 1 with $m = 2$, $\Delta = 2$, take the $[2, 2-2]_4 2$ code with the identity parity-check matrix as $\mathcal{Q}_2$, and obtain a new $(233, 3 \cdot 4^{224})_4 2$ code. The best known codes of length 233 is a $[233, 225]_4 2$ code obtained by Fact 2 from the $[154, 146]_4 2$ code of [3].

Example 4. We consider $R = 4$, $q = 2$. Let $\mathcal{V}_0$ be the $(15, 2^{32})_2 4$ code of [2, Table 6.1]. We put $p = 2^{32}$, $r_0 = n_0 = 15$, $\mathcal{C}_0 = \mathcal{Z}_{15}$. We use Theorem 2 with $m = 4$, $\Delta = 1$, take the $[5, 1]_2 2$ repitition code as $\mathcal{Q}_4$, and obtain a new $(280, 2^{254})_2 4$ code. The best known codes of length 280 is a $[280, 255]_2 4$ code obtained by Fact 2 from the $[238, 213]_2 4$ code of [2, Table 7.3].

Now we consider linear codes.

Example 5. We consider $R = 3$, $q = 2$.

i) Let $\mathcal{V}_0$ be the $[14, 6]_2 3$ code of [2, Table 7.3]. Then $n_0 = 14$, $r_0 = 8$. We use Theorem 2 with $m = 4$, $\Delta = 2$, take the $[5, 1]_2 2$ code as $\mathcal{Q}_4$, and obtain a new $[254, 234]_2 3$ code.

ii) Now $\mathcal{V}_0$ is the $[7, 1]_2 3$ repetition code, $n_0 = 7$, $r_0 = 6$. We use Theorem 2 with $m = 3$, $\Delta = 1$, take the $[4, 1]_2 2$ code as $\mathcal{Q}_3$, and obtain a new $[71, 56]_2 3$ code.

Example 6. We consider $R = 4, q = 2$.

i) Let $\mathcal{V}_0$ be the $[16, 6]_2 4$ code of [2, Table 7.3]. We use Theorem 2 with $m = 4$, $\Delta = 0$, take the $[5, 1]_2 2$ code as $\mathcal{Q}_4$, and obtain a new $[291, 265]_2 4$ code.

ii) Now $\mathcal{V}_0$ is the $[8, 1]_2 4$ repetition code. We use Theorem 2 with $m = 3$, $\Delta = 0$, take the $[4, 1]_2 2$ code as $\mathcal{Q}_3$, and obtain a new $[82, 63]_2 4$ code.

iii) Let $\mathcal{V}_0$ be the $[9, 1]_2 4$ repetition code. We apply the trivial 4-partition with $h = n_0 = 9$ where every subset consists of one column, use Theorem 3 with $m = 3$ and $g = 8$, take the $[4, 1]_2 2$ code as $\mathcal{Q}_3$, and obtain a new $[90, 70]_2 4$ code.

iv) Now $\mathcal{V}_0$ is the $[13, 4]_2 4$ code of [2,Table 7.3]. In [5, Example 5.6] it is noted that this code has a 4-partition with $h = 9$. We use Theorem 3 with $m = 3$, take the $[4, 1]_2 2$ code as $\mathcal{Q}_3$, and obtain a new $[122, 101]_2 4$ code.

Example 7. We consider $R = 5$, $q = 2$. The new $[82, 63]_2 4$ and $[90, 70]_2 4$ codes of Example 6 in the ADS Construction [2, Chapter 4] together with the $[15, 11]_2 1$ and the $[31, 26]_2 1$ Hamming codes give $[96, 73]_2 5$, $[104, 80]_2 5$, and $[120, 95]_2 5$ codes.

Example 8. We consider $R = 3$, $q = 2$. The new $[71, 56]_2 3$ code $\mathcal{V}$ of Example 5ii has a parity-check matrix $\mathbf{H}_{\mathcal{V}} = [\mathbf{h}_1 \mathbf{h}_2 \ldots \mathbf{h}_{71}]$ where $\mathbf{h}_i \in \mathcal{S}_2^{15}$, $i = 1, 2, \ldots, 71$, and $[\mathbf{h}_1 \mathbf{h}_2 \ldots \mathbf{h}_7] = \mathbf{G}_2$, $[\mathbf{h}_8 \mathbf{h}_9 \ldots \mathbf{h}_{63}] = \mathbf{H}_1$, $[\mathbf{h}_{64} \mathbf{h}_{65} \mathbf{h}_{66} \mathbf{h}_{67}] = \mathbf{H}_2$, $[\mathbf{h}_{68} \mathbf{h}_{69} \mathbf{h}_{70} \mathbf{h}_{71}] = \mathbf{H}_3$. We write columns of the matrix W_3 and elements $\xi_i \in \mathbb{F}_{2^3}$ in the lexicographical order, i.e.,

$$W_3 = \begin{bmatrix} 0 & 0 & 0 & \ldots & 1 \\ 0 & 1 & 1 & \ldots & 1 \\ 1 & 0 & 1 & \ldots & 1 \end{bmatrix}, \quad [\xi_1 \ldots \xi_8] = \begin{bmatrix} 0 & 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 1 & 1 & \ldots & 1 \\ 0 & 1 & 0 & 1 & \ldots & 1 \end{bmatrix}. \tag{24}$$

The columns of the submatrices $\mathbf{G}_2$ and $\mathbf{H}_1$ are placed in accordance to (24). For the column set of $\mathbf{H}_{\mathcal{V}}$ we form the following partition $\mathcal{K}$ into $h = 32$ subsets: $\{\mathbf{h}_1\}$, $\{\mathbf{h}_2\}$, $\{\mathbf{h}_3, \mathbf{h}_4, \ldots, \mathbf{h}_7\}$, $\{\mathbf{h}_j, \mathbf{h}_{j+1}\}$, $\{\mathbf{h}_{j+2}, \mathbf{h}_{j+3}\}$, $\{\mathbf{h}_{j+4}, \mathbf{h}_{j+5}, \mathbf{h}_{j+6}, \mathbf{h}_{j+7}\}$, $j = 8.16, 24, \ldots, 56$, $\{\mathbf{h}_{64}\}$, $\{\mathbf{h}_{65}\}, \ldots, \{\mathbf{h}_{71}\}$. By (24), every column of the submatrix $\mathbf{H}_1$ (respectively $\mathbf{G}_2$) is a sum of three (respectively two) columns belonging to distinct subsets of $\mathcal{K}$. Besides, since $\mathcal{Q}_3$ is the $[4, 1]_2 2$ code we have $\mathbf{h}_{64} + \mathbf{h}_{65} + \mathbf{h}_{66} + \mathbf{h}_{67} = \mathbf{0}$, $\mathbf{h}_{68} + \mathbf{h}_{69} + \mathbf{h}_{70} + \mathbf{h}_{71} = \mathbf{0}$. Now from the structure of the matrix $\mathbf{H}_{\mathcal{V}}$ and the proofs of Theorems 1 and 2 one can see that $\mathcal{K}$ is a 3,2–partition and $\mathcal{V}$ is a $[71, 56]_2 3, 2$ code. We verified it by computer. We use the code $\mathcal{V}$ as a starting code for Theorem 4 with $m \geq 5$ and obtain an infinite family $\mathcal{A}_2$ of new $[n, n - r]_2 3$ codes with parameters

$$R = 3, q = 2, n = 18 \cdot 2^{t-3} - 1, r = 3t, t = 5 \text{ and } t \geq 10, \bar{\mu}_2(3, \mathcal{A}_2) \approx 1.9.$$

For $r = 3t$ the best known linear code family is the family $\mathcal{U}$ with $n = 19 \cdot 2^{t-3} - 1$, $t \geq 9$, $\bar{\mu}_2(3, \mathcal{U}) \approx 2.23$ [2, Theorem 5.4.28], [5, eq. (4.16)].

Example 9. We consider $R = 4, q = 2$. The new $[90, 70]_2 3$ code $\mathcal{V}$ of Example 6iii has a parity-check matrix $\mathbf{H}_{\mathcal{V}} = [\mathbf{h}_1 \mathbf{h}_2 \ldots \mathbf{h}_{90}]$ where $\mathbf{h}_i \in \mathcal{S}_2^{20}$, $i = 1, 2, \ldots, 90$, $[\mathbf{h}_1 \mathbf{h}_2 \ldots \mathbf{h}_{14}] = \mathbf{G}_2$, $[\mathbf{h}_{15} \mathbf{h}_{16} \ldots \mathbf{h}_{78}] = \mathbf{H}'_8$, $[\mathbf{h}_{79} \mathbf{h}_{80} \ldots \mathbf{h}_{86}] = \mathbf{H}''_8$, $[\mathbf{h}_{87} \mathbf{h}_{88} \mathbf{h}_{89} \mathbf{h}_{90}] = \mathbf{H}_3$. The columns of the submatrices $\mathbf{G}_2$, $\mathbf{H}'_8$, and $\mathbf{H}''_8$ are placed in accordance to (24). For the column set of $\mathbf{H}_{\mathcal{V}}$ we form the following partition $\mathcal{K}$ into $h = 25$ subsets: $\{\mathbf{h}_1\}$, $\{\mathbf{h}_2\}$, $\{\mathbf{h}_3, \mathbf{h}_4, \ldots, \mathbf{h}_7\}$,

Table 1. Upper bounds on the length function $l(r, R; 2)$.

R	r	bound from [2, Table 7.3]	new bound	R	r	bound from [2, Table 7.3]	new bound
3	15	75	71	4	19	84	82
3	20	255	254	4	20	93	90
3	30	2431	2303	4	21	125	122
3	33	4863	4607	4	26	301	291
3	36	9727	9215	4	40	3038	2942
3	39	19455	18431	4	44	6015	5886
3	42	38911	36863	4	48	12031	11774
3	45	77823	73727	4	52	24063	23550
3	48	155647	147455	4	56	48127	47102
3	51	311295	294911	4	60	96255	94206
3	54	622591	589823	4	64	192511	188414
3	57	1245183	1179647	5	23	98	96
3	60	2490367	2359295	5	24	107	104
3	63	4980735	4718591	5	25	123	120

$\{\mathbf{h}_8, \mathbf{h}_9, \ldots, \mathbf{h}_{14}\}$, $\{\mathbf{h}_j\}$, $\{\mathbf{h}_{j+1}, \mathbf{h}_{j+2}, \ldots, \mathbf{h}_{j+7}\}$, $j = 15, 23, 31, \ldots, 71$, $\{\mathbf{h}_{79}, \mathbf{h}_{80}, \ldots, \mathbf{h}_{86}\}$, $\{\mathbf{h}_{87}\}$, $\{\mathbf{h}_{88}\}$, $\{\mathbf{h}_{89}\}$, $\{\mathbf{h}_{90}\}$. We need subsets $\{\mathbf{h}_j\}$, $\{\mathbf{h}_{j+1}, \mathbf{h}_{j+2}, \ldots, \mathbf{h}_{j+7}\}$, $j = 15, 23, \ldots, 71$, for (11) and (18). By (24), $\mathbf{h}_1+\mathbf{h}_2+\mathbf{h}_3 = \mathbf{0}$. Hence $\mathbf{h}_i = \mathbf{h}_i+\mathbf{h}_1+\mathbf{h}_2+\mathbf{h}_3$, $i = 4, 5, \ldots, 90$. Now from the structure of the matrix $\mathbf{H}_{\mathcal{V}}$ and the proofs of Theorems 1–3 one can see that $\mathcal{K}$ is a 4, 2–partition and $\mathcal{V}$ is a $[90, 70]_2 4, 2$ code. We verified it by computer. We use the code $\mathcal{V}$ as a starting code for Theorem 4 with $m \geq 5$ and obtain an infinite family $\mathcal{A}_3$ of new $[n, n-r]_2 4$ codes with parameters

$$R = 4, q = 2, n = 23 \cdot 2^{t-3} - 2, r = 4t, t = 5 \text{ and } t \geq 10, \bar{\mu}_2(3, \mathcal{A}_3) \approx 2.85.$$

For $r = 4t$ the best known linear code family is the family $\mathcal{D}$ with $n = 47 \cdot 2^{t-4} - 1$, $t = 5$ and $t \geq 11$, $\bar{\mu}_2(3, \mathcal{D}) \approx 3.1$ [2, Theorem 5.4.29], [5, eq. (5.13)].

The results of Examples 5–9 form Table 1.

Acknowledgments

The author wishes to thank 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 (1984) pp. 240–244.
2. G. D. Cohen, I. S. Honkala, S. N. Litsyn, and A. C. Lobstein, *Covering Codes*, North-Holland Math. Library, Vol. 54. Amsterdam: Elsevier (1997).
3. A. A. Davydov, Construction of codes with covering radius 2, Algebraic Coding (G. Cohen, S. Litsyn, A. Lobstein, G. Zemor, eds.), Lecture Notes in Computer Science, Springer-Verlag, New York, 573 (1992) pp. 23–31.

4. A. A. Davydov, Constructions of nonlinear covering codes, *IEEE Trans. Inform. Theory*, Vol. 43 (1997) pp. 1639–1647.
5. A. A. Davydov and A. Yu. Drozhzhina–Labinskaya, Constructions, families and tables of binary linear covering codes, *IEEE Trans. Inform. Theory*, Vol. 40 (1994) pp. 1270–1279.
6. T. Etzion and G. Greenberg, Constructions for perfect mixed codes and other covering codes, *IEEE Trans. Inform. Theory*, Vol. 39 (1993) pp. 209–214.
7. J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, second edition. Oxford, UK: Clarendon Press (1998).
8. J. H. van Lint, Jr., *Covering Radius Problems*, M.Sc. thesis, Eindhoven University of Technology, the Netherlands (1988).
9. R. Struik, *Covering Codes*, Ph.D. dissertation, Eindhoven University of Technology, the Netherlands (1994).