PROBLEMS OF INFORMATION TRANSMISSION

A translation of *Problemy Peredachi Informatsii*

April, 1991

Volume 26, Number 4 October-December, 1990

CONTENTS

Engl./Russ.

INFORMATION THEORY AND CODING THEORY

SIGNAL PROCESSING METHODS

COMMUNICATION NETWORK THEORY

BRIEF COMMUNICATIONS

INDEX

The Russian press date (podpisano k pechati) of this issue was 11/16/1990. Publication therefore did not occur prior to this date, but must be assumed to have taken place reasonably soon thereafter.

13. R. G. Gallager, "Variations on a theme by Huffman," IEEE Trans. Inform. Theory, **24**, 668-674 (1978).

14. Yu. M. Shtar'kov, "General-purpose sequence coding of individual messages," Prob. Peredachi Inform., **23**, No. 3, 3-17 (1987).

15. A. V. Aho, J. E. Hopcroft, and J. D. Ullman, The Design and Analysis of Computer Algorithms, Addison-Wesley, Reading, Mass. (1974).

16. J. S. Vitter, Two Papers on Dynamic Huffman Coding, Tech. Rep. CS85-13, Brown Univ. Comput. Sci., Providence, RI (Dec. 1986).

17. D. W. Jones, "Application of splay trees to data compression," Commun. ACM, **31**, No. 8, 996-1007 (1989).

18. B. Ya. Ryabko, "Comments to 'A locally adaptive data compression scheme'," Commun. ACM, **30**, No. 9, 792 (1987).

19. J. Rissanen and G. G. Langdon, "Arithmetic coding," IBM J. Res. Develop., **23**, No. 2, 149-162 (1979).

20. F. Rubin, "Arithmetic stream coding using fixed precision registers," IEEE Trans. Inform. Theory, **26**, No. 6, 672-675 (1979).

21. Yu. M. Shtar'kov, "Generalized Shannon codes," Prob. Peredachi Inform., **20**, No. 3, 3-16 (1984).

22. E. N. Gilbert and E. F. Moore, "Variable-length binary encodings," Bell. Sys. Techn. J., **38**, 933-967 (1959).

23. J. Ziv and A. Lempel, "Compression of individual sequences via variable rate coding," IEEE Trans. Inform. Theory, **24**, No. 5, 530-536 (1978).

CONSTRUCTION OF LINEAR COVERING CODES

A. A. Davydov

UDC 621.391.15

A linear covering code construction is proposed, which given any binary code with covering radius R constructs an infinite family of binary codes with the same covering radius. Infinite families of R ≥ 2 linear binary covering codes are constructed with better parameters than known codes.

1. INTRODUCTION

Covering codes and other issues connected with covering of spaces over a finite alphabet have recently stimulated considerable interest among researchers (see, e.g., [1-19] and the references therein). In this paper, we consider binary linear covering codes. Some ideas of this study may be viewed as a development and generalization of the results of [18].

We start with some notation: [n, k]R is a linear code of length n, dimension k, and covering radius R; t[n, k] is the minimum possible covering radius of a linear code of length n and dimension k; [n, n − r]R is a linear code of length n, redundancy r, and covering radius R; $\lfloor x \rfloor$ is the whole part of x; $\lceil x \rceil$ is the integer nearest to x which is not smaller than x; *l*(r, R) is the minimum length of a linear code of redundancy r and covering radius R [16]; μ[n, R, C] is the density of covering of the n-dimensional space by radius-R spheres centered at code words of length n and covering radius R in code C (density of covering is computed as the ratio of the total volume of all spheres to the volume of the space, see [4, p. 692] and [14]).

For the infinite family U of codes with covering radius R, we define

$$\bar{\mu}[R, U] \overset{\Delta}{=} \liminf_{n\to\infty,\, U(n)\in U} \mu[n, R, U(n)], \tag{1.1}$$

where U(n) is a code of length n from the family U.

Translated from Problemy Peredachi Informatsii, Vol. 26, No. 4, pp. 38-55, October-December, 1990. Original article submitted June 21, 1989; revision submitted June 25, 1990.

0032-9460/90/2604-0317\$12.50 ©1991 Plenum Publishing Corporation

A code with redundancy r is of covering radius R if any column of length r is representable as the sum of R or fewer columns of the check matrix [2, 3]. Adjoining an arbitrary column to the check matrix of an [n, n − r]R-code, we obtain a [n + 1, n + 1 − r]R-code, $R_1 \le R$. Therefore, the infinite family of covering codes with a fixed R is often described by specifying, for a given r, the least length n of the code from the given family, expressing n as a function of r.

In this paper, we consider the construction of infinite families of covering [n, n − r]R-codes. These families are constructed so as to reduce n for given r and R [1, 16].

The best codes with R = 1 are the Hamming $[n = 2^r - 1, n - r]1$-codes [1].

For R = 2, a family S of codes with the parameters

$$R=2, n=\begin{cases} 5\times 2^{c-2}-1 \text{ for } r=2c-1, \\ 7\times 2^{c-2}-2 \text{ for } r=2c, \end{cases} \quad c\geqslant 4, \bar{\mu}[2,S]=49/32 \tag{1.2}$$

was constructed in [18].

For R ≥ 3, infinite families of covering codes are constructed (see, e.g., [1, 5, 11, 16, 18]) from the codes with R = 1, 2 by various constructions proposed by Graham and Sloane [1], such as DS (direct sum), ADS (amalgamated DS), EDS (extended DS), BEDS (bordered EDS).

In this paper, we propose a construction which, for any given R, produces the check matrix of a linear binary code V with covering radius R from the check matrix of an arbitrary binary code V_0 with covering radius R_0, where $R_0 \le R$. (In the proposed construction, we usually take $R_0 = R$.)

If the initial code V_0 is of length Q and redundancy s, then the constructed code V is of length n and redundancy r:

$$n=2^m Q+N(m),\ r=s+mR, \tag{1.3}$$

where m is an integer parameter, N(m) is the number of columns of the auxiliary matrix used in the construction.

The parameter m is lower bounded, but it may be increased without bound, i.e., an *infinite family* of codes V may be constructed.

To reduce N(m), the initial code V_0 in the proposed construction is interpreted as the R_0^*, *l*-subset of the Q-dimensional space (for definition see Sec. 2). For $l \ge 1$ any column of length s, including the zero column, may be generated as the sum of not fewer than *l* and not more than R_0^* columns of the check matrix of the code V_0. The relationship between the parameter R_0^* and the covering radii of the codes V and V_0 has the form $R \ge R_0^* \ge R_0$. (Often, $R = R_0^* = R_0$.)

The constructed codes V are normal [1] and may be used in the ADS scheme. The proposed construction is sufficiently flexible and admits various implementations.

As an example of using the proposed construction and its various implementations, we have constructed infinite families of codes with covering radii R ≥ 2 with better parameters than the known codes. In particular, we have constructed code families V^1-V^3 with the parameters

$$R=2,\ n=55\times 2^{c-5}-2,\ r=2c,\ c\geqslant 5,\ \bar{\mu}[2, V^1]\approx 1{,}477, \tag{1.4}$$

$$R=3, n=\begin{cases} 311\times 2^{c-7}-3 & \text{for } r=3c, c\geqslant 7, \\ 823\times 2^{c-9}-3 & \text{for } r=3c-1, c\geqslant 9,\ \bar{\mu}[3, V^2]\approx 1{,}384, \\ 2^{c+1}-1 & \text{for } r=3c-1,\ c=\overline{5,8}, \end{cases} \tag{1.5}$$

$$R=4,\ n=2^{c+1}-2,\ r=4c-3,\ c\geqslant 5, \tag{1.6}$$

$$\begin{gathered} R\geqslant 16,\ r=Rc,\ 2^c\geqslant 8R+5{,}2\sqrt{R}+16, \\ n<0{,}5R\times 2^{r/R}(1+1{,}5/\sqrt{R})+0{,}15\times 2^{r/R}-\sqrt{R}. \end{gathered} \tag{1.7}$$

From (1.4)-(1.6) we obtain

$$t[53,43]=2,\ t[63,49]=t[64,50]=3,\ t[62,45]=t[63,46]=4. \tag{1.8}$$

Relationships (1.4)-(1.7) are upper bounds on *l*(r, R). Thus, from (1.4) we get

$$l(10,2)\leqslant 53,\ l(12,2)\leqslant 108,\ l(14,2)\leqslant 218,\ l(16,2)\leqslant 438. \tag{1.9}$$

The proposed construction is naturally extended to nonbinary linear covering codes over the field GF(q), q > 2. As an illustration, Sec. 3 constructs the code family V^5 with the parameters q = 3, R = 2, $\overline{\mu}[2, V^5] \approx 1.185$.

The paper is organized as follows. Section 2 introduces the notation and definitions. Section 3 describes the general covering code construction and its alternative implementations. Sections 4 and 5 present examples that apply the construction to obtain code families with $R = 2$ and $R \geq 3$.

2. NOTATION AND DEFINITIONS

We consider binary columns and matrices. The superscript attached to the matrix (column) gives the number of rows (entries) in the matrix (the column); the only exception is the superscript tr, which denotes the transpose.

Depending on context, the matrices may be treated as sets whose elements are columns. The signs +, ∪, ∈, ... are then interpreted accordingly. Thus the expression $\{T_1 + \dots + T_v\}$, where T_i is a matrix, is understood in the following sense:

$$\{T_1 + \dots + T_v\} = \{x : x = t_1 + \dots + t_v,\ t_i \in T_i,\ i = \overline{1, v}\}.$$

The representation of the element h of the field $GF(2^m)$ as a matrix or column element corresponds to the binary representation of the element h as an m-bit column vector. For definiteness, we take

$$h = h_m\alpha^{m-1} + \dots + h_2\alpha + h_1 = (h_m \dots h_2 h_1)^{tr}, \tag{2.1}$$

where $h \in GF(2^m)$, α is the primitive element of $GF(2^m)$, $h_i \in \{0, 1\}$, $i = 1, \dots, m$.

We introduce the matrices $P^s(\varphi_i)$, 0^m, E^m, $E_0{}^m$, W^{mR}, and $B_\xi{}^{mR}(b)$.

The matrix $P^s(\varphi_i) = \|\varphi_i\varphi_i \dots \varphi_i\|$ consists of identical columns, where each column is the binary representation of the element φ_i of the field $GF(2^s)$; 0^m is the m-row matrix of zeros. The number of columns in the matrices $P^s(\varphi_i)$ and 0^m is determined from the context.

In the matrix E^m all columns are of length m: $E^m = \|e_0 e_1 \dots e_M\|$, $M = 2^m - 1$, $e_i \in GF(2^m)$, $i = 0, \dots, M$, $e_i \neq e_j$ for $i \neq j$. The matrix $E_0{}^m$ is the matrix E^m without the zero column. $E_0{}^m$ coincides with the check matrix of the Hamming $[2^m - 1, 2^m - 1 - m]1$-code.

The other matrices are defined as

$$W^{mR} = \left\| \begin{matrix} 0^{m(R-1)} \\ E^m \end{matrix} \right\|. \tag{2.2}$$

$$B_\xi^{mR}(b) = \left\| \begin{array}{cccc} e_0 & e_1 & \dots & e_M \\ e_0 b & e_1 b & \dots & e_M b \\ e_0 b^2 & e_1 b^2 & \dots & e_M b^2 \\ & \dots & & \\ e_0 b^{R-\xi-1} & e_1 b^{R-\xi-1} & \dots & e_M b^{R-\xi-1} \\ \hline e_0 (a_1 + b)^{-1} & e_1 (a_1 + b)^{-1} & \dots & e_M (a_1 + b)^{-1} \\ e_0 (a_2 + b)^{-1} & e_1 (a_2 + b)^{-1} & \dots & e_M (a_2 + b)^{-1} \\ & \dots & & \\ e_0 (a_\xi + b)^{-1} & e_1 (a_\xi + b)^{-1} & \dots & e_M (a_\xi + b)^{-1} \end{array} \right\|, \tag{2.3}$$

where $M = 2^m - 1$; $b,\ e_i,\ e_i b^u,\ a_j,\ e_i(a_j + b)^{-1} \in GF(2^m)$, $i = \overline{0, M}$, $u = \overline{1, R-\xi-1}$, $j = \overline{1, \xi}$; $\xi \in \{\overline{0, R-1}\}$; ξ is the number of rows with elements of the form $e_i(a_j + b)^{-1}$ (when $\xi = 0$, no such rows exist); $e_i \neq e_j$ for $i \neq j$; $b \neq a_j$, $j = 1, \dots, \xi$; $a_v \neq a_j$ for $v \neq j$.

We introduce the class $G(\rho)$ of vectors with positive integer components. The vector $g \in G(\rho)$ if

$$g = (R_1, R_2, \dots, R_\gamma);\ R_\lambda \in \{\overline{1, \rho}\},\ \lambda = \overline{1, \gamma}; \tag{2.4}$$
$$\sum_{\lambda=1}^{\gamma} R_\lambda = \rho;\ \ \gamma \geqslant \lceil \log_2(\rho + 1) \rceil;$$

any integer t, $t \in \{1, \dots, \rho\}$, is representable as the sum of components of the vector g, i.e., there exists a set $\theta(t)$ (not necessarily unique) of the vector components that sum to t, $\sum\limits_{R_\lambda \in \theta(t)} R_\lambda = t$.

In the class $G(\rho)$ we identify the subclasses $G_1(\rho, \nu, a)$, $G_2(\rho)$, and $G_3(\rho)$:

$$G_1(\rho, \nu, a) = \{g : g \in G(\rho);\ R_\lambda = 1,\ \lambda = \overline{1, \nu};\ R_t \leqslant \nu + a,\quad t = \overline{\nu + 1, \gamma}\},\ a \in \{0, 1\},\ \nu \in \{\overline{1, \rho}\}, \tag{2.5}$$

$$G_2(\rho)=\{g : g\in G(\rho);\ \gamma=\lceil\log_2(\rho+1)\rceil;\ R_1=\lceil\rho/2\rceil,\ \ R_\lambda=\left\lceil\frac{1}{2}\left(\rho-\sum_{i=1}^{\lambda-1}R_i\right)\right\rceil,\ \ \lambda=\overline{2,\gamma}\},\tag{2.6}$$

$$G_3(\rho)=\{g : g\in G(\rho);\ \gamma=\lceil\log_2(\rho+1)\rceil;\ R_1=\rho-2^{\gamma-1}+1,\ R_i=2^{\gamma-i},\ i=\overline{2,\gamma}\}.\tag{2.7}$$

In the subclass $G_1(\rho, \nu, a)$ for fixed ρ, ν, a the vector g is defined nonuniquely, except the cases $\nu = \rho$ and $\nu = 1$, $a = 0$, when $g = (1, 1, \dots, 1)$. The subclasses $G_2(\rho)$ and $G_3(\rho)$ contain one element each.

The construction of the set $\theta(t)$ follows from the construction of the vector g. Thus, for $g \in G_2(\rho)$, we may take $R_\lambda \in \theta(t)$ if and only if $t - \sigma_\lambda \geq R_\lambda$, $\lambda = 1, \dots, \gamma$, where $\sigma_1 = 0$, $\sigma_\lambda = \sum\limits_{R_i\in\theta(t), i<\lambda} R_i$, $\lambda = 2, \dots, \gamma$. For the vector $g \in G_1(\rho, \nu, a)$ we denote by K(t) the set $\theta(t)$ of the vector components with consecutive indices, such that at least one of two components R_ν, $R_{\nu+1}$ is in K(t):

$$K(t)\overset{\blacktriangle}{=}\{R_{X(t)}, R_{X(t)+1}, R_{X(t)+2}, \dots, R_{\nu+y(t)}\},\tag{2.8}$$

where

$$X(t)=\nu+1-(t-Y(t)),\ Y(t)=\sum_{i=1}^{y(t)}R_{\nu+i}\leq t<\sum_{i=1}^{y(t)+1}R_{\nu+i};$$

if $t < R_{\nu+1}$ or $\nu = \rho$, then $Y(t) = y(t) = 0$.

Example 1.1. $(1.\ 1.\ 1.\ 3,\ 3)\in G_1(9.\ 3.\ 0)$, $K(5)=\{R_2, R_3, R_4)$. $(1, 1, 1, 2, 3, 1)\in G_1(9, 3, 0)$, $K(5)=\{R_4, R_5\}$, $K(6)=\{R_3, R_4, R_5\}$, $(1, 1, 1, 1, 4, 5, 5)\in G_1(18, 4, 1)$, $K(4)=\{R_5\}$, $K(10)=\{R_4, R_5, R_6\}$.

We define the function f as follows: $f(g) = i$ if for any t we can construct a set $\theta(t)$ so that $R_u \in \theta(t)$, $u \leq i$, implies $R_p \in \theta(t)$, $p = 1, \dots, u - 1$, but this is not true for $u \geq i + 1$.

Example 1.2. $g = (12, 6, 3, 2, 1) \in G_2(24)$, $\theta(17) = \{R_1,R_3,R_4\}$, $f(g) = 1$.

Example 1.3. $g = (7, 8, 4, 2, 1) \in G_3(22)$, $\theta(17) = \{R_1,R_2,R_4\}$, $f(g) = 2$.

The vector g may be generated iteratively. If $\rho \leq 2u + 1$ and $(R_2, R_3, \dots, R_\gamma) \in G(u)$, then $g = (R_1 = \rho - u, R_2, R_3, \dots, R_\gamma) \in G(\rho)$.

Example 1.4. $(12, 6, 3, 2, 1) \in G(24)$, $g = (10, 12, 6, 3, 2, 1) \in G(34)$, $f(g) = 2$.

We introduce the matrix $D_\varkappa{}^{mR}(g, \rho)$ whose structure depends on the parameters m, R, $\varkappa$, ρ and on the components of the vector g, $g \in G(\rho)$:

$$D_{\varkappa}^{mR}(g,\rho)=\left\|\begin{array}{c|c}
\begin{array}{ccc} A^{mR_1} & 0^{mR_1}\dots & 0^{mR_1}\\ 0^{mR_2} & A^{mR_2}\dots & 0^{mR_2}\\ & \dots & \\ 0^{mR_\varkappa} & 0^{mR_\varkappa}\dots & A^{mR_\varkappa}\end{array} & 0^{m(R_1+R_2+\dots+R_\varkappa)}\\
\hline
0^{m\Lambda}\quad 0^{m\Lambda}\dots 0^{m\Lambda} & 0^{m\Lambda}\quad 0^{m\Lambda}\dots 0^{m\Lambda}\\
\hline
0^{m(R_{\varkappa+1}+\dots+R_\gamma)} & \begin{array}{ccc} A^{mR_{\varkappa+1}} & 0^{mR_{\varkappa+1}} & \dots 0^{mR_{\varkappa+1}}\\ 0^{mR_{\varkappa+2}} & A^{mR_{\varkappa+2}} & \dots 0^{mR_{\varkappa+2}}\\ & \dots & \\ 0^{mR_\gamma} & 0^{mR_\gamma} & \dots A^{mR_\gamma}\end{array}
\end{array}\right\|,\tag{2.9}$$

where $g = (R_1, R_2, \dots, R_\gamma) \in G(\rho)$, $R_1 + \dots + R_\gamma = \rho$; A^{mR_λ} is the check matrix of the $[N_\lambda, N_\lambda - mR_\lambda]R_\lambda$-code with covering radius R_λ, $\lambda = 1, \dots, \gamma$; $A^{m\times1} = E_0{}^m$, $N_\lambda = 2^{m-1} - 1$ for $R_\lambda = 1$, $\Lambda = R - \rho$, $R \geq \rho$; for $R = \rho$, the submatrices $0^{m\Lambda}$ are missing, $\varkappa \in \{0, \dots, \gamma\}$; for $\varkappa = 0$ ($\varkappa = \gamma$) the upper (lower) part of the matrix with A^{mR_λ} is missing, $\lambda \leq \varkappa$ ($\lambda > \varkappa$).

The number of columns N(m) of the matrix $D_\varkappa{}^{mR}(g, \rho)$ is $N(m) = N_1 + \dots + N_\gamma$. The matrix obtained from $D_\varkappa{}^{mR}(g, \rho)$ be eliminating the zero rows (formed by the submatrices $0^{m\Lambda}$) is the direct sum [1, p. 391] of the matrices A^{mR_λ}, $\lambda = 1, \dots, \gamma$ and constitutes the check matrix of the $[N(m), N(m) - m\rho]\rho$-code.

Define the column

$$(u_1,\ldots,u_R)^{mR}=\left\|\begin{matrix}u_1\\ \cdots\\ u_R\end{matrix}\right\|,\quad u_i\in GF(2^m),\quad i=\overline{1, R}. \tag{2.10}$$

We use the following notation: $[B^m]A, l$ is the set whose elements are all possible sums of the columns of the matrix B^m with no fewer than l and no more than A addends, with each column entering the sum at most once and $l \geq 1$; $[B^m]0, l = \varnothing$; $[B^m]_2A, l$ is the subset of the set $[B^m]A, l$ that consists of sums with an even number of addends.

Definition 1. A linear binary code of length Q and redundancy s with check matrix Φ^s is called the R^*, l-subset of the Q-dimensional space and is denoted by $[Q, Q - s]R^*, l$ if the following holds. For $l \geq 1$, any column from E^s, including the zero column, is representable as the sum of not fewer than l and not more than R^* columns of the matrix Φ^s. For $l = 0$, any nonzero column from E^s is representable as the sum of no more than R^* columns of the matrix Φ^s. In all cases, R^* is the least integer with this property† for the given l. In other words:

$$[\Phi^s]R^*.\ l=E^s \text{and} [\Phi^s]A.\ l\subset E^s \text{ for } A<R^*,\ l\geqslant 1. \tag{2.11}$$

$$[\Phi^s]R^*.\ 1=E_0^s \text{and} [\Phi^s]A,\ 1\subset E_0^s \text{ for } A<R^*,\ l=0. \tag{2.12}$$

It is easy to verify that a point that belongs to the R^*, l-subset exists at a distance not smaller than l and not greater than R^* from any point in the Q-dimensional space (this property may be used as the definition of the R^*, l-subset in both the linear and the nonlinear case). The R^*, 0-subset corresponds to the ordinary sphere covering.

The [Q, Q − s]-code with the check matrix Φ^s has the covering radius R [2, 3] if and only if any column from E_0^s is representable as the sum of not more than R columns of the matrix Φ_s while this is not true for A < R:

$$[\Phi^s]R,1=E_0^s,\ [\Phi^s]A,\ 1\subset E_0^s \text{ for } A<R. \tag{2.13}$$

The code notations [Q, Q − s]R, 0 and [Q, Q − s]R have the same meaning, i.e., $R^*(0) = R$, where R is the covering radius. If $R \geq l > 0$, then $R^*(l) \geq R$.

Definition 2. For R < Q, the collection of matrices $(T_1^w, \ldots, T_Q^w)$ is called R-closed if for any combination of distinct indices of the form $J_R = \{j_1, \ldots, j_R\}$, $j_k \in \{1, \ldots, Q\}$, $k = 1, \ldots, R$, any column from E^w, including the zero column, is representable as the sum of R columns, with one column included from each matrix $T_{j1}^w, \ldots, T_{jR}^w$, i.e.,

$$\{T_{j_1}^w+\ldots+T_{j_R}^w\}=E^w. \tag{2.14}$$

Definition 3. For $l \geq 0$, R < Q, the matrix L^w is called R, l-complementary to the R-closed collection of matrices $(T_1^w, \ldots, T_Q^w)$ if the following two conditions are satisfied.

1. For any combination of distinct indices of the form $J_z = \{j_1, \ldots, j_z\}$, $z \in \{l, \ldots, R\}$, $z \geq 1$, $j_k \in \{1, \ldots, Q\}$, $k = 1, \ldots, z$: any column from E^w, including the zero column, is representable as the sum of no fewer than z and no more than R columns, where the first z columns necessarily entering the sum are taken one from each matrix $T_{j1}^w, \ldots, T_{jz}^w$ and the remaining columns (the second group of terms) are taken from the matrices $L^w, T_1^w, \ldots, T_Q^w$. The second group of terms (if present in the sum) includes an even number of columns or no columns at all from each matrix T_i^w, i = 1, ..., Q, and any (i.e., even or odd) number of columns from the matrix L^w.

2. For $l = 0$ any nonzero column from E^w is representable as the sum of at most R columns from the matrices $L^w, T_1^w, \ldots, T_Q^w$, with an even number of columns or no columns at all taken from each matrix T_i^w, i = 1, ..., Q, and any number of columns (i.e., even or odd) taken from the matrix L^w.

In order to satisfy condition 1 in Definition 3, it is sufficient to have the following relationship for any combination of distinct indices $\{j_1, \ldots, j_z\}$:

$$\{T_{j_1}^w+\ldots+T_{j_z}^u\}+\{\nu^w\cup[L^w]R-z,\ 1\}=E^w,\ z\in\overline{\{l,\ R\}}, \tag{2.15}$$

where $z \geq 1$, $j_k \in \{1, \ldots, Q\}$, $k = 1, \ldots, z$, ν^w is the zero column in E^w. If (2.15) holds, all the columns in the second group of terms (if present in the sum) originate from the matrix L^w.

†Therefore R^* is sometimes denoted by $R^*(l)$.

To satisfy condition 2 in Definition 3, it is sufficient to ensure that the matrix L^w is the check matrix of a code with covering radius R, i.e.,

$$[L^w]R,1=E_0^w \text{ for. } l=0. \tag{2.16}$$

Another sufficient relationship for condition 2 of Definition 3 is

$$[L^w]R,1 \cup \bigcup_{j=1}^{Q} [T_j^w]_2 R,2=E_0^w \quad \text{for} \quad l=0. \tag{2.17}$$

3. LINEAR COVERING CODE CONSTRUCTIONS

THEOREM 1. Let $\varphi_i \in GF(2^s)$, i = 1, ..., Q, and let $\Phi^s = \|\varphi_1\varphi_2 ... \varphi_Q\|$ be the check matrix of the $[Q, Q - s]R_0^*$, l-code V_0 which is the R_0^*, l-subset of the Q-dimensional space. Also let T_j^w be a w × Γ matrix, j = 1, ..., Q; $(T_1^w, ..., T_Q^w)$ an R-closed collection of matrices; L^w a w × N matrix which is R, l-complementary to the collection of matrices $(T_1^w, ..., T_Q^w)$; $R \geq R_0^* \geq l \geq 0$. Then

$$H^{s+w}=\left\|\begin{array}{c|cccc} 0^s & P^s(\varphi_1) & P^s(\varphi_2) & \ldots & P^s(\varphi_Q) \\ \hline L^w & T_1^w & T_2^w & \ldots & T_Q^w \end{array}\right\| \tag{3.1}$$

(for l = R the submatrices 0^s and L^w are missing) is the check matrix of the [n, n − r]R-code V of length n = ΓQ + N, redundancy r = s + w, and covering radius R.

Proof. We will show that an arbitrary column U^{s+w} in E_0^{s+w} is the sum of at most R columns of the matrix (3.1). We represent U^{s+w} in the form

$$U^{s+w}=\left\|\begin{array}{c} v^s \\ u^w \end{array}\right\|, \tag{3.2}$$

where v^s and u^w are columns of length s and w, respectively. For simplicity, assume that we have cases (2.15) and (2.16). The general case of R, l-complementarity is proved similarly.

Let $l \geq 1$. Since the code V_0 is the R_0^*, l-subset, then by Definition 1 the column v^s is representable as the sum of z columns of Φ^s:

$$v^s=\varphi_{j_1}+\varphi_{j_2}+\ldots+\varphi_{j_z},\ z\in\{\overline{l, R_0^*}\}. \tag{3.3}$$

Now to obtain u^w we *must* take one column from each matrix $T_{j1}^w, ..., T_{jz}^w$. Moreover, we may use (in any order) at most R − z columns from L^w. In other words, we have to prove the existence of the representation

$$u^w=t_{i_1,j_1}+\ldots+t_{i_z,j_z}+l_{a_1}+\ldots+l_{a_f} \qquad z+f=F\leqslant R, \tag{3.4}$$

where t_{i_k,j_k} is the i_k-th column from T_{jk}^w, $j_k \in J_z$, k = 1, ..., z, $J_z = \{j_1, ..., j_z\}$ is the combination of distinct indices formed by the indices of the columns entering the sum (3.3); f ≥ 0; $l_{a_i} \in L^w$, i = 1, ..., f; for f = 0, the terms l_{a_i} are missing.

Let $z = R_0^* = R$. Since $(T_1^w, ..., T_Q^w)$ is an R-closed collection of matrices, then by Definition 2 the existence of the representation (3.4) with f = 0 follows from (2.14).

Let z < R. The existence of representation (3.4) with f ≥ 0 follows from (2.15).

Let l = 0. Then for $v^s \neq 0$ the representations (3.3), (3.4) are still true. For $v^s = 0$, the column U^{s+w} is obtained by condition (2.16) as the sum of at most R columns of the matrix $\left\|\begin{array}{c} 0^s \\ L^w \end{array}\right\|$ Q.E.D.

Theorem 2 for w = mR describes a natural implementation of the construction (3.1), which uses the matrix $D_\varkappa^{mR}(g, \rho)$ as L^w and the matrices $B_\xi^{mR}(b_j)$ (with distinct b_j) as the matrices T_j^w. We have examined alternatives with various relationships between the parameters Q, m, ξ, ρ and with various vectors g.

The column $u^w = u^{mR} = (u_1, ..., u_R)^{mR}$ is represented as the sum (3.4) in two stages. In the first stage, summing z columns t_{i_k,j_k} from the matrices $B_\xi^{mR}(b_{j_k})$ we form the column $(u^*)^{mR}$ which matches u^{mR} in z elements $u_{\tau_1}, ..., u_{\tau_z}$. The indices i_k are determined by solving over the field $GF(2^m)$ a system of equations with a nonsingular matrix which is a submatrix of the Vandermonde matrix, Cauchy matrix, or a combination of these matrices. The appearance of matrices of this kind is associated with the structure of $B_\xi^{mR}(b_j)$ (2.3).

In the second stage, f columns l_{a_i} from $D_{\varkappa}^{mR}(g, \rho)$, $0 \le f \le R - z$, are added to $(u^*)^{mR}$. The added columns do not change the elements $u_{\tau_1}, \dots, u_{\tau_z}$. To find the columns l_{a_i} in $D_{\varkappa}^{mR}(g, \rho)$, we isolate the submatrix d^{mR} with zero rows in positions $u_{\tau_1}, \dots, u_{\tau_z}$. The remaining rows of d^{mR} form the check matrix of a code with covering radius $R - z$. The existence of such d^{mR} is associated with the structure and properties of the vector g (2.4)-(2.8).

If the code V_0 is given, the parameters of the constructed code V depend on N(m) — the number of columns of the matrix $D_{\varkappa}^{mR}(g, \rho)$, which in turn depends on the form of the vector g.

THEOREM 2. Let $\varphi_i \in GF(2^s)$, $i = 1, \dots, Q$, and let $\Phi^s = \|\varphi_1\varphi_2 \cdots \varphi_Q\|$ be the check matrix of the $[Q, Q - s]R_0^*, l$-code V_0, which is the R_0^*, l-subset of the Q-dimensional space; $R \ge R_0^* \ge l \ge 0$. Assume that the check matrix of the code V has the form[†]

$$H^{s+mR} = \left\| \begin{array}{c|c} 0^s & P^s(\varphi_1) \dots P^s(\varphi_{Q-1})\, P^s(\varphi_Q) \\ \hline D_{\varkappa}^{mR}(g, \rho) & B_{\xi}^{mR}(b_1) \dots B_{\xi}^{mR}(b_{Q-1})\, B_{\xi}^{mR}(b_Q) \end{array} \right\|, \qquad (3.5)$$

where $b_i \in GF(2^m)$ for all i; $b_i \ne b_j$ for $i \ne j$; $\rho = R - \Lambda \ge 0$; for $\rho = 0$ the matrices 0^s and $D_{\varkappa}^{mR}(g, \rho)$ are missing; for $Q = 2^m + 1$ the matrix $B_{\xi}^{mR}(b_Q)$ is replaced with the matrix W^{mR}. Denote by N(m) the number of columns of the matrix $D_{\varkappa}^{mR}(g, \rho)$.

Then for the code V to be a normal $[n, n - r]R$-code with covering radius R, redundancy $r = s + mR$, and length $n = 2^mQ + N(M)$, it is sufficient that one of the following cases holds:

1) $2^m+1=Q,\ \xi=0,\ \Lambda=\max\{0, l-2\},\ g\in G_1(\rho, \nu, 0),\ \nu\geqslant 1,$
$R_\tau=1,\ \varkappa=\nu;$
2) $2^m+1=Q,\ \xi=0,\ \Lambda=\max\{0, l-1\},\ g=(1, 1, \dots, 1),\ \varkappa=0;$
3) $2^m\geqslant Q,\ \xi=0,\ \Lambda=\max\{0, l-1\},\ g\in G_1(\rho, \nu, 0),\ \nu\geqslant 1,\ \varkappa=\nu;$
4) $2^m\geqslant Q,\ \xi=0,\ \Lambda=l,\ g=(1, 1, \dots, 1),\ \varkappa=0;$
5) $2^m-1\geqslant Q,\ \xi=0,\ b_i\ne 0$ for all $i,\ \Lambda=l,\ g\in G_1(\rho, \nu, 1),$
$\nu\geqslant 1,\ \varkappa=\nu;$
6) $2^m-\xi\geqslant Q,\ \xi=\rho-\sum_{\lambda=1}^{j} R_\lambda,\ 1\leqslant j\leqslant f(g),\ \Lambda=l,\ \varkappa=0,\ \forall g\in G(\rho).$

Proof. From (2.5)-(2.7) we see that $R_i = 1$ exists. Therefore $A^{mR_i} = E_0^m$, the minimum distance in the code V is $d \le 3$, and by Theorem 24 [4] the code V is normal.

By Theorem 1, it suffices to show that the collection of matrices $(B_{\xi}^{mR}(b_1), \dots, B_{\xi}^{mR}(b_Q))$ is R-closed and the matrix $D_{\varkappa}^{mR}(g, \rho)$ is R, l-complementary to this collection. Therefore (see Definitions 2 and 3) it suffices to show that conditions (2.15) and (2.16) hold.

If $l = 0$, then $R = \rho$, $D_{\varkappa}^{mR}(g, \rho)$ is the check matrix of a code with covering radius R, and condition (2.16) holds.

Let us prove that condition (2.15) also holds. Partition (from top to bottom) the rows of the matrices $D_{\varkappa}^{mR}(g, \rho)$ and $B_{\xi}^{mR}(b_j)$ into R groups, m rows in each group, and index these groups 1 to R. If the matrix column is treated as a collection of R binary representations of elements of the field $GF(2^m)$, then each group of rows corresponds to one field element.

Let $\theta(0) = \varnothing$ and let $d^{mR}(\theta(z - \Lambda))$ be the matrix formed from the columns of the matrix $D_{\varkappa}^{mR}(g, \rho)$ that contain all the submatrices A^{mR_β} with $R_\beta \notin \theta(z - \Lambda)$. The $R - z$ groups of rows of the matrix $d^{mR}(\theta(z - \Lambda))$ containing these submatrices A^{mR_β} form the check matrix of a code with covering radius $R - z$. The remaining z groups of rows of the matrix $d^{mR}(\theta(z - \Lambda))$ are zero rows. We denote their indices by $\tau_1, \dots, \tau_z$. The groups of rows corresponding to the submatrices $O^{m\Lambda}$ are always zero rows. The indices of these groups of rows are $T + 1, T + 2, \dots, T + \Lambda$, where $T = R_1 + R_2 + \dots + R_{\varkappa}$. Clearly, $\{T + 1, \dots, T + \Lambda\} \subseteq \{\tau_1, \dots, \tau_z\}$.

Let $u^{mR} = (u_1, \dots, u_R)^{mR}$ be an arbitrary column from E^{mR}. We will show that for any combination of indices $J_z = \{j_1, \dots, j_z\}$, $z \in \{l, \dots, R\}$, we can construct a set $\theta(z - \Lambda)$ that satisfies the following condition: there is one column in each matrix $B_{\xi}^{mR}(b_{j_k})$, $k = 1, \dots, z$, such that their sum forms the column $(u^*)^{mR}$ that matches the column u^{mR} in positions $\tau_1, \dots, \tau_z$, i.e.,

(3.6)

[†] In most cases when this construction is used, $R = R_0^*$.

where in case 1 one of the matrices in parentheses may be the matrix W^{mR}.

The column u^{mR} may be obtained by adding to $(u^{*})^{mR}$ at most $R - z$ columns of the matrix $d^{mR}(\theta(z - \Lambda))$. This implies that condition (2.15) holds.

Let $e_i f_v(b)$ be the element of $B_\xi^{mR}(b)$ or W^{mR} located at the intersection of row v and column (i + 1). The column "locators" e_{i_k} ensuring that (3.6) is satisfied are solutions of the system

$$\sum_{k=1}^{z} e_{i_k} f_{\tau_c}(b_{j_k}) = u_{\tau_c}, \quad c=\overline{1, z}. \tag{3.7}$$

Denote the determinant of this system by Δ_z. We will show that $\Delta_z \neq 0$.

1) Let $j_z = Q$, $b_{j_{z-1}} = 0$, $q = z - \Lambda - 2$, $K(0) = \varnothing$. For $q > 0$ find K(q), X(q) from (2.8) and denote X = X(q). Let $\theta(z - \Lambda) = \{R_1, R_\gamma\} \cup K(q)$. Then for $q > 0$ we have $\tau_1 = 1$, $\tau_i = X + i - 2$, $i = 2, \dots, z - 1$, $\tau_z = R$; Δ_z has the form (see [20, Sec. 11.5])

$$\Delta_z = \begin{vmatrix} 1 & \dots & 1 & 1 & 0 \\ b_{j_1}^{X-1} & \dots & b_{j_{z-2}}^{X-1} & 0 & 0 \\ & & \dots & & \\ b_{j_1}^{X+z-4} & \dots & b_{j_{z-2}}^{X+z-4} & 0 & 0 \\ b_{j_1}^{R-1} & \dots & b_{j_{z-2}}^{R-1} & 0 & 1 \end{vmatrix} \neq 0.$$

(This is so because $\Lambda = l - 2$ for $l \geq 3$.) Other cases are analyzed similarly. For instance, if $j_i \neq Q$, $i = 1, \dots, z$, $b_{j_z} = 0$, then $q = z - \Lambda - 1$, $\theta(z - \Lambda) = R_1 \cup K(q)$. If $j_i \neq Q$, $b_{j_i} \neq 0$, $i = 1, \dots, z$, then $q = z - \Lambda$, $\theta(z - \Lambda) = K(q)$.

2-5) Similar to case 1.

6)) Construct $\theta(z - \Lambda)$ so that if $R_u \in \theta(z - \Lambda)$, $u \leq j$, then $R_p \in \theta(z - \Lambda)$, $p = 1, \dots, u - 1$; Δ_z has the form (see [20, Sec. 11.4], [21, Sec. 2, 5, pp. 126-127])

$$\Delta_z = \left|\begin{array}{ccc} 1 & \dots & 1 \\ b_{j_1} & \dots & b_{j_z} \\ b_{j_1}^{\delta-1} & \dots & b_{j_z}^{\delta-1} \\ \hline (a_{c_1} + b_{j_1})^{-1} & \dots & (a_{c_1} + b_{j_z})^{-1} \\ & \dots & \\ (a_{c_{z-\delta}} + b_{j_1})^{-1} & \dots & (a_{c_{z-\delta}} + b_{j_z})^{-1} \end{array}\right| \neq 0,$$

where δ and $z - \delta$ is the number of rows with elements of the form $b_{j_k}{}^{u}$ and $(a_{c_c} + b_{j_k})^{-1}$. Q.E.D.

These cases do not exhaust the possible constructions (3.1), (3.5). The proof of the theorems suggests a technique for constructing new variants. In specific cases, we should try to relax the lower bounds on m (so that the construction starts working for lower r and is more efficient for finite lengths) and to choose R_λ so as to reduce N(m). The sum of ρ values R_λ is fixed, but different combinations of R_λ are efficient in different cases, which accounts for the variety of the different vectors g considered. The vectors from subclasses $G_2(\rho)$ and $G_3(\rho)$ often reduce N(m), but at the same time they strengthen the lower constraints on m.

In the matrices $B_\xi^{mR}(b)$ the elements of the form $e_i(a_j + b)^{-1}$ may be replaced with elements of the form $e_i(1 + a_j b)^{-1}$ [22].

The covering radius R_0 of the initial code V_0 is not considered here as such. Recall that $R_0^{*}(0) = R_0$, $R \geq R_0^{*}(l > 0) \geq R_0$, and often $R = R_0^{*}(l > 0) = R_0$.

Remark 1. We see from the proof of Theorem 1 that in construction (3.1) the condition of R-closure of the matrices $(T_1{}^{w}, \dots, T_Q{}^{w})$ and R, *l*-complementarity of the matrix L^{w} may be replaced with the weaker condition of (R, *l*, Φ^{s})-complementarity.

Throughout the rest of this remark (as in Theorem 1), $\varphi_i \in GF(2^s)$, $i = 1, \dots, Q$, $\Phi^s = \|\varphi_1\varphi_2 \dots \varphi_Q\|$ is the check matrix of the $[Q, Q - s]R_0{}^{*}$, *l*-code V_0, which is the $R_0{}^{*}$, *l*-subset of the Q-dimensional space, $R \geq R_0{}^{*} \geq l \geq 0$.

Let d_p be a column from E^s, $d_0 = 0$, $d_p \neq d_j$ for $p \neq j$. For $z \in \{l, \dots, R\}$ denote by $J_z(d_p)$ the combination of distinct indices corresponding to *one of the possible* representations of the sum d_p as the sum of not fewer than *l* and not more than R columns of the matrix Φ^s:

$$\begin{gathered} J_z(d_p)=\{j_1(p),\ldots,j_z(p)\}. \\ \varphi_{j_1(p)}+\ldots+\varphi_{jz(p)}=d_p, \\ z\in\{\overline{l,R}\},\ z\geqslant 1,\ j_k(p)\in\{\overline{1,Q}\}.\ k=\overline{1.z}, \\ p\in\{\overline{0,2^s-1}\}. \end{gathered} \tag{3.8}$$

Introduce the set J(R, l, Φ^s) of index combinations:

$$J(R,l,\Phi^s)=\{J_z(d_p),\ z\in\{\overline{l,R}\},\ z\geqslant 1,\ p=\overline{0,\ 2^s-1}\ \text{ for }\ l\geqslant 1,\ \ p=\overline{1,2^s-1}\text{ for }\ l=0\}. \tag{3.9}$$

The set J(R, l, Φ^s) is defined nonuniquely by the parameters R, l and the matrix Φ^s. It contains *one possible representation* of all the columns from E^s (for $l \geq 1$) or $E_0{}^s$ (for $l = 0$). Below we consider the construction of a good (in some sense) alternative of this set, which is "compatible" with the matrices L^w, $T_i{}^w$ and makes it possible to relax the conditions on these matrices by ensuring that the conditions of Definition 2 and condition 1 of Definition 3 are satisfied not for "any combinations of distinct indices" J_R and J_z but only for some index combinations from this set.

Definition 4. For $l \geq 0$, R < Q the matrix L^w is called (R, l, Φ^s)-complementary to the collection of matrices ($T_1{}^w, \ldots, T_Q{}^w$) if there exists a set J(R, l, Φ^s) such that the following conditions are satisfied:

1. $\forall J_R(d_p)=\{j_1(p),\ldots,j_R(p)\}\in J(R.l,\Phi^s),\ \{T^w_{j_1(p)}+\ldots+T^w_{j_R(p)}\}=E^w.$

2. For any index combination $J_z(d_p) = \{j_1(p), \ldots, j_z(p)\}$ from the set J(R, l, Φ^s): any column from E^w, including the zero column, is representable as the sum of not fewer than z and not more than R columns, where the first z columns necessarily included in the sum are taken one from each matrix $T_{j1(p)}{}^w, \ldots, T_{jz(p)}{}^w$ and the remaining columns (the second group of terms) are taken from the matrices $L^w, T_1{}^w, \ldots, T_Q{}^w$. The second group of terms (if present in the sum) includes an even number of columns or no columns from each matrix $T_i{}^w$, i = 1, ..., Q, and any number of columns (even or odd) from the matrix L^w.

3. For l = 0 condition 2 of Definition 3 holds.

To satisfy condition 2 of Definition 4, it suffices to have the following relationship, which is analogous to (2.15):

$$\begin{gathered} \forall J_z(d_p)=\{j_1(p),\ldots,j_z(p)\}\in J(R,l,\Phi^s), \\ \{T^w_{j_1(p)}+\ldots+T^w_{j_z(p)}\}+\{\nu^w\cup[L^w]R-z,1\}=E^w, \end{gathered} \tag{3.10}$$

where ν^w is the zero column in E^w, z ∈ {l, ..., R}, z ≥ 1.

THEOREM 3. Theorem 1 is true if the conditions of R-closure and R, l-complementarity are replaced with the condition that the matrix L^w is (R, l, Φ^s)-complementary to the collection of matrices ($T_1{}^w, \ldots, T_Q{}^w$).

The proof of Theorem 3 is similar to the proof of Theorem 1.

An example of a construction with (R, l, Φ^s)-complementarity is provided by the codes of [18]. (In condition 2 of Definition 3, these codes realize (2.17).)

Condition 1 of Definition 4 may be called R, Φ^s-closure.

To the set of index combinations J(R, l, Φ^s) we associate the Q-vertex graph Γ(J). The vertex j corresponds to the column φ_j of the matrix Φ^s. The vertices j_k and j_t are joined by an edge if and only if j_k and j_t are both contained at least in one combination from J(R, l, Φ^s). Denote by h(J) the chromatic number [23, p. 294] of the graph Γ(J).

The check matrix constructions from Theorems 1-3 will be denoted respectively by ΦLT (see (3.1)), ΦDB (see (3.5)), and ΦLTJ.

Let us describe the ΦDBJ construction. We formally use the symbol * as the value of b in $B_\xi{}^{mR}(b)$ and take $B_\xi{}^{mR}(*) = W^{mR}$. We use the same matrix Φ^s as in Theorem 2. Construct the set J(R, l, Φ^s) and the graph Γ(J). The check matrix of the code V is (3.5), where $b_i \in$ {GF(2^m) ∪ *} for all i. If the vertices i and j in the graph are joined by an edge, then necessarily $b_j \neq b_i$. The equality $b_u = b_v$ is allowed if the vertices u and v are not joined by an edge.

THEOREM 4. The code V whose check matrix is obtained by the ΦDBJ construction is a normal [n, n − r]R-code with r = s + mR, n = 2^mQ + N(m), and covering radius R if one of the conditions 1-6 of Theorem 2 holds, with the value Q in all these conditions replaced by the chromatic number[†] h(J) and with $b_i \neq *$ for all i in conditions 3-6, as before.

The proof of Theorem 4 is similar to the proof of Theorem 2.

[†] The minimum number of colors which is sufficient to paint in different colors the vertices of the graph Γ(J) that are the end points of the same edge.

If $h(J) < Q$ (e.g., when the code V_0 is constructed by ADS or by Theorems 1-4), the ΦDBJ construction starts working for smaller m than ΦDB. In the ΦDBJ construction for $h(J) < 2^m + 1 \leq Q$ it is useful to take all the values b from the set $\{GF(2^m) \cup *\}$, which reduces ρ in the matrix $D_\varkappa{}^{mR}(g, \rho)$ (and therefore reduces N(m)) by inclusion of an even number of columns from the matrices $B_\xi{}^{mR}(b_i)$, $i \in \{1, \dots, Q\}$, in the second group of terms (see Definition 4).

Remark 2. We introduce the following notation: Ω^{mR} is the check matrix of some MDS [Q, Q − R]-code [20] over the field $GF(2^m)$; $e_i\Omega^{mR}$ is the matrix Ω^{mR} with all the elements multiplied by $e_i \in GF(2^m)$ and written in binary representation. Interchanging the columns of matrix (3.5), we can write it in the form

$$H^{s+mR} = \left\| \begin{array}{c|cccc} 0^s & \Phi^s & \Phi^s & \dots & \Phi^s \\ \hline D_\varkappa^{mR}(g, \rho) & e_0\Omega^{mR} & e_1\Omega^{mR} & \dots & e_M\Omega^{mR} \end{array} \right\|, \qquad (3.11)$$

where $M = 2^m - 1$, $e_i \in GF(2^m)$, $i = 0, \dots, M$, $e_i \neq e_j$ for $i \neq j$.

The form of Ω^{mR} determines the structure of the matrix $D_\varkappa{}^{mR}(g, \rho)$ and the constraints on m.

Remark 3. The code V constructed by (3.1), (3.5), (3.11), is the R, l'-subset of an n-dimensional space, where $l' \geq l$. The matrix $D_\varkappa{}^{mR}(g, \rho)$ always includes the Hamming code check matrix with groups of w linearly dependent columns, $w \geq 3$. Such groups are also present in other matrices A^{mR_λ}. Therefore for $R \geq 3$ the code V constructed by (3.5) and (3.11) often has $l' = R - 2$. This increases the efficiency of the iterative application of these constructions, with the constructed code V used in turn as the initial code V_0.

Remark 4. For an R-closed collection of equally dimensioned $w \times \Gamma$ matrices $(T_1{}^w, \dots, T_Q{}^w)$ we have $\Gamma^R \geq 2^w$. In (3.5), $w = mR$ and Γ has its minimum possible value 2^m.

Remark 5. For $l \geq 1$ the points of the $R_0{}^*$, l-subset can be interpreted as the centers of the "spherical capsules" covering the space. The capsules have internal radius l, external radius $R_0{}^*$, and "wall thickness" $R_0{}^* - l + 1$.

It is also useful to consider "layered spherical capsules" that consist of collections of spherical surfaces with radii $l_1 > l_2 > \dots > l_v \geq 0$. In this case, any column d from E^s (for $l_v \geq 1$) or from $E_0{}^s$ (for $l_v = 0$) is representable as the sum of z(d) columns of the matrix Φ^s, where

$$z(d) \in \{l_1 = R_0^*, l_2, l_3, \dots, l_v = l\} \triangleq \mathscr{L}(R_0^*, l).$$

For $R \geq R_0{}^*$ we can introduce the notion of R, $\mathscr{L}(R_0{}^*, l)$-complementarity, which is intermediate between R, l-complementarity and (R, l, Φ^s)-complementarity. In condition 1 of Definition 3, $z \in \mathscr{L}(R_0{}^*, l)$. This approach reduces N(m), relaxing the conditions on L^w.

The capsules are of no independent interest here: they are merely introduced as a device to reduce N(m). Capsule coverings and their density of course may be considered independently.

Remark 6. Let us generalize the previous definitions of complementarity.

Definition 5. The matrix L^w is R, Φ^s-complementary to the collection of matrices $(T_1{}^w, \dots, T_Q{}^w)$ if the matrix H^{s+w} (3.1) is the check matrix of a code with covering radius R.

Let us bring Definition 4 closer to Definition 5. Construct the set $J^*(R, l, \Phi^s)$ as the union of the subsets $J^*(d_p)$, $p = 0, \dots, 2^s - 1$ for $l \geq 1$, $p = 1, \dots, 2^s - 1$ for $l = 0$. The subset $J^*(d_p)$ consists of f(p) index combinations $J_z(d_p)$ of the form (3.8), $f(p) \geq 1$. We introduce the notion of $(R, l, \Phi^s)^*$-complementarity by replacing conditions 1 and 2 in Definition 4 with the following condition: for any column $u^w \in E^w$ every subset $J^*(d_p)$ contains an index combination $J_z(d_p)$ which produces this column u^w by the technique described in condition 2 of Definition 4.

Remark 7. The constructions (3.1), (3.5), (3.11) are naturally extended to nonbinary covering codes over the field GF(q), $q > 2$.

A [Q, Q − s]-code over GF(q) with the check matrix Φ^s has covering radius R_0 [3, 16] if and only if any nonzero q-ary column of length s is representable as a linear combination (with coefficients from GF(q)) of at most R_0 columns of the matrix Φ^s.

Therefore, when extending the construction to q-ary codes, instead of the sum of columns we consider linear combinations of columns (in the expressions $\{T_1 + \dots + T_v\}$ and $[B^m]A$, l in (2.11)-(2.17), in Definitions 1-5, in the proof of Theorems 1-4, etc.). In the matrices $P^s(\varphi_i)$, E^m, (2.2), (2.3), (2.9), (3.1), (3.5), in the column (2.10), and in the determinant Δ_z, the elements of the field $GF(2^m)$ are now replaced with the elements of the field $GF(q^m)$, which are written in q-ary representation in the form of m-digit column vectors. In (3.11) we consider an MDS code over the field $GF(q^m)$. In Theorem 2, 2^m is replaced with q^m in the lower constraints on m in cases 1-6. The length of the constructed code V is $n = q^mQ + N(m)$.

Example 2. $q = 3$, $R = 2$, V_0 is the Golay [11, 6]2, 0-code over GF(3); $D_{\times}^{m\times 2}(g, \rho)$ is the direct sum of two check matrices of the Hamming $[(3^m - 1)/2, (3^m - 1)/2 - m]1$-code over GF(3). The construction (3.5) with $\xi = 0$, $3^m - 1 \geq 11$ gives a family of codes V^5 with the parameters

$$q=3,\ R=2,\ n=12\times 3^m-1,\ r=5+2m,\ m\geqslant 3,\ \bar{\mu}[2, V^5]\approx 1.185. \tag{3.12}$$

4. CODES OF COVERING RADIUS 2

Contrary to (3.5), we construct L^w without using the direct sum of matrices. In this section we assume in (3.1) that V_0 is a [5, 1]2, 0-code,

$$\Phi^s = F^4 = \begin{Vmatrix} 10001 \\ 01001 \\ 00101 \\ 00011 \end{Vmatrix} = \| f_1 f_2 f_3 f_4 f_5 \|,\ f_i \in GF(2^4). \tag{4.1}$$

For $\Phi^s = F^4$ the construction (3.5) (case 1) produces codes whose structure is different from that of the codes in [18] but they have the parameters (1.2). In this section, we construct codes with parameters (1.4) that are better than (1.2).

Improvement of the parameters of codes with $R = 2$ is of interest not only as an independent problem but also because codes with $R = 2$ are used to construct the matrices A^{mR_λ} for codes with $R > 2$.

Using the methods of [1, pp. 391, 393], we construct the check matrices of [13, 7]2- and [28, 20]2-codes:

$$\Pi_3{}^6 = \begin{Vmatrix} 0011110000000 \\ 1100110000000 \\ 0101011000000 \\ 0000000001111 \\ 0000000110011 \\ 0000001010101 \end{Vmatrix},$$

$$\Pi_4{}^8 = \begin{Vmatrix} 000000111111 & 10 & 00000000000 & 111 \\ 000111000111 & 01 & 00000000000 & 111 \\ 011001011001 & 01 & 00000000000 & 111 \\ 101010101010 & 01 & 00000000000 & 111 \\ 000000000000 & 11 & 00000111111 & 100 \\ 000000000000 & 11 & 00111000111 & 010 \\ 000000000000 & 11 & 11001011001 & 010 \\ 000000000000 & 11 & 01010101010 & 011 \end{Vmatrix}.$$

For $m \geq 5$, the check matrix of the $[n = 7 \times 2^{m-3} - 2, n - 2(m - 1)]2$-code from [18] is representable in the form

$$K^{2m-2} = \left\| \begin{array}{c|c|c|c|c|c|c} 0\ldots 0 & 0\ \ldots\ 0 & 0\ \ldots\ 0 & 0\ \ldots\ 0 & 0\ \ldots\ 0 & 1\ \ldots\ 1 & 1\ \ldots\ 1 \\ 0\ldots 0 & 1\ \ldots\ 1 & 1\ \ldots\ 1 & 1\ \ldots\ 1 & 1\ \ldots\ 1 & 0\ \ldots\ 0 & 1\ \ldots\ 1 \\ \hline E_0^{m-3} & & & & 0^{m-3} & E^{m-3} & E^{m-3} \\ \cline{1-1}\cline{5-7} 0^{m-3} & \smash{F_0^{2m-6}(a)} & \smash{F^{2m-6}(b)} & \smash{F^{2m-6}(c)} & E^{m-3} & 0^{m-3} & 0^{m-3} \\ \hline 0\ldots 0 & 0\ \ldots\ 0 & 0\ \ldots\ 0 & 1\ \ldots\ 1 & 1\ \ldots\ 1 & 0\ \ldots\ 0 & 0\ \ldots\ 0 \\ 0\ldots 0 & 0\ \ldots\ 0 & 1\ \ldots\ 1 & 0\ \ldots\ 0 & 1\ \ldots\ 1 & 0\ \ldots\ 0 & 0\ \ldots\ 0 \end{array} \right\|, \tag{4.2}$$

where $a, b, c \in GF(2^{m-3})$, $a + b = c$, $a \neq b$, $a, b \neq 0$;

$$F^{2m-6}(d) = \begin{Vmatrix} e_0=0 & e_1 & e_2 & \ldots & e_\Psi \\ e_0=0 & e_1{}^{-1}d & e_2{}^{-1}d & \ldots & e_\Psi{}^{-1}d \end{Vmatrix}, \quad \Psi=2^{m-3}-1,$$

$d, e_i \in GF(2^{m-3})$, $i = 0, \ldots, \Psi$, $e_i \neq e_j$ for $i \neq j$; $F_0{}^{2m-6}(a)$ is the matrix $F^{2m-6}(a)$ without the zero column.

Both the upper and lower $m - 1$ rows of the matrix K^{2m-2} contain all the columns from $E_0{}^{m-1}$. Hence, using the construction from the proof of Theorem 3.3 [16, p. 104], we obtain the following lemma.

LEMMA 1. The check matrix

$$\Pi_5^{2m} = \left\| \begin{array}{c|c|c} 0 \ldots 0 & 1 \ldots 1 & 0 \ldots 0 \\ \hline & E^{m-1} & 0^{m-1} \\ K^{2m-2} & & \\ \cline{2-3} & 0^{m-1} & E^{m-1} \\ \hline 0 \ldots 0 & 0 \ldots 0 & 1 \ldots 1 \end{array} \right\|, \quad m \geqslant 5, \tag{4.3}$$

defines a $[n = 15 \times 2^{m-3} - 2, n - 2m]2$-code of covering radius 2.

THEOREM 5. Let $m \geq 3$. The check matrix of the code V is

$$H^{4+2m} = \left\| \begin{array}{c|c} 0^4 & P^4(f_1) \quad P^4(f_2) \ \ldots P^4(f_5) \\ \hline \Pi_\sigma^{2m} & B_0^{2m}(b_1) \quad B_0^{2m}(b_2) \ldots B_0^{2m}(b_5) \end{array} \right\|, \tag{4.4}$$

where $B_0^{2m}(b)$ is the matrix $B_0^{mR}(b)$ with $R = 2$; $b_i \in GF(2^m)$, $i = 1, \ldots, 5$, $b_i \neq b_j$ for $i \neq j$; α is the primitive element of $GF(2^m)$; relationship (2.1) holds; $b_5 = 0$;

for $m = 3$, $\Pi_\sigma^{2m} = \Pi_3^6$, $b_1 = \alpha$, $b_2 = \alpha + 1$, $b_3 = \alpha^2 + 1$, $b_4 = \alpha^2 + \alpha$;

for $m = 4$, $\Pi_\sigma^{2m} = \Pi_4^8$, $\alpha^4 = \alpha + 1$, $b_1 = \alpha$, $b_2 = \alpha^4$, $b_3 = \alpha^{10}$, $b_4 = \alpha^{11}$;

for $m \geq 5$, $\Pi_\sigma^{2m} = \Pi_5^{2m}$, $b_1 = \alpha^3$, $b_2 = \alpha^3 + \alpha$, $b_3 = \alpha^3 + \alpha^2$, $b_4 = \alpha^3 + \alpha^2 + \bar{\alpha}$.

Then V is a normal $[n = 55 \times 2^{c-5} - 2, n - 2c]2$-code for $c \geq 5$.

Proof. Let $m \geq 5$. From (4.2)-(4.4) we see that in the code V the minimum distance is $d \leq 3$ and by Theorem 24 [4] V is normal code. By Theorem 1 it suffices to show that the matrix Π_5^{2m} is 2, 0-complementary to the 2-closed collection of matrices $(B_0^{2m}(b_1), \ldots, B_0^{2m}(b_5))$. By Lemma 1, condition (2.16) holds.

In (2.15), consider the cases $z = 1, 2$. Let $u = (u_1, u_2)^{2m}$ be an arbitrary column from E^{2m} of the form (2.10) with $R = 2$. For $z = 2$: $u = X_1 + X_2$, $X_i = (e_{x_i}, e_{x_i} b_{j_i})^{2m} \in B_0^{2m}(b_{j_i})$, $i = 1, 2$. The "locators" c_{x_i} are determined from the system $e_{x_1} + e_{x_2} = u_1$, $e_{x_1} b_{j_1} + e_{x_2} b_{j_2} = u_2$. The solution of this system exists, because $b_{j1} \neq b_{j2}$.

Let $z = 1$, $u \notin B_0^{2m}(b_{j1})$. If $j_1 = 5$, then $u = Y + X$, $Y = (v, u_2)^{2m} \in \Pi_5^{2m}$, $X = (v + u_1, 0)^{2m} \in B_0^{2m}(b_5)$. Such columns X, Y can be found because $b_5 = 0$ and the lower m rows of the matrix Π_5^{2m} contain all the columns from E^m.

If $j_1 \neq 5$, then we first find u as the sum $u = Y + X$, $Y = (y, 0)^{2m} \in \Pi_5^{2m}$, $X = (e, eb_{j_1})^{2m} \in B_0^{2m}(b_{j_1})$. Then $y = u_1 + u_2 b_{j1}^{-1}$. From (4.2), (4.3) we see that $(y, 0)^{2m} \notin \Pi_5^{2m}$ if $y = (001a_1 \ldots a_{m-3})^{tr}$, $a_i \in \{0, 1\}$, $i = 1, \ldots, m - 3$. In this case, we obtain u as the sum $u = Y^* + X^*$, $Y^* = (0, y^*)^{2m} \in \Pi_5^{2m}$, $X^* = (e^*, e^* b_{j_1})^{2m} \in B_0^{2m}(b_{j_1})$. Then $y^* = u_2 + u_1 b_{j1} = y b_{j1}$. Since $b_1 = \alpha^3$, $b_2 = \alpha^3 + \alpha$, $b_3 = \alpha^3 + \alpha^2$, $b_4 = \alpha^3 + \alpha^2 + \alpha$, we have $y^* = (c_1 \ldots c_{m-1} 1)^{tr}$, $c_i \in \{0, 1\}$, $i = 1, \ldots, m - 1$. All the columns $(0, y^*)^{2m}$ with y^* of this form are contained in Π_5^{2m} (see (4.3)). The cases $m = 3, 4$ are proved similarly (they can be verified by computer). Q.E.D.

5. EXAMPLES OF INFINITE FAMILIES OF COVERING CODES WITH R ≥ 3

We will now use the construction (3.5) in case 5. In the matrix $D_\varkappa^{mR}(g, \rho)$ the submatrix $A^{m \times 2}$ is the check matrix of the code (1.4).

Example 3. $R = 3$. a) V_0 is Golay [23, 12]3, 0-code; $g = (1, 2)$; V is the code with parameters (1.5) for $r = 3c - 1$, $c \geq 9$; b) V_0 is [7, 1]3, 0-code, $g = (1, 2)$, V is the code with parameters (1.5) for $r = 3c$; c) V_0 is [7, 2]3, 2-code with check matrix of the form

$$\Phi^5 = \left\| \begin{array}{ccccccc} 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{array} \right\|. \tag{5.1}$$

$\Lambda = 2$, $\rho = 1$, $g = (1)$. The code V has the parameters (1.5) for $r = 3c - 1$, $c = 5, \ldots, 8$. ■

Now $D_\varkappa^{mR}(g, \rho)$ contains the submatrix $A^{m \times 3}$ - the check matrix of the code (1.5) with $r = 3c$.

Example 4. $R + 4$. V_0 is [6, 1]4, 2-code with the check matrix obtained by omitting the last column from the matrix (5.1). Then $\Lambda = 2$, $g = (1, 1)$. The code V has the parameters (1.6). ■

It is shown in [1] that $2 \leqslant t[53.\ 43] \leqslant 3.\ 3 \leqslant t[63.\ 49] \leqslant 4.\ 3 \leqslant t[64,\ 50] \leqslant 4,\ 4 \leqslant t[62,\ 45] \leqslant 5,\ 4 \leqslant t[63.\ 46] \leqslant 5$. Therefore (1.4)-(1.6) lead to (1.8).

Example 5. $R = 5$. V_0 is $[5, 1]5$, 3-code with the check matrix F^4 (4.1), $R_0 = 2$, $\Lambda = 3$, $\rho = 2$, $g = (1, 1)$. The parameters of the code V are $r = 4 + 5m$, $m \geq 3$, $n = 7 \times 2^m - 2$. For $r = 24$, we have $n = 110$; for $r = 29$, we have $n = 222$. An alternative is the code V′ constructed when V_0 is $[10, 1]5$, 0-code. But for $r = 24$ the code V′ cannot be constructed and for $r = 29$ the code V′ is of length 230. The case $R = R_0^*(l > 0) > R_0$ is thus useful. ■

Example 6. $R = 3v + 2$. V_0 is $[2R + 1, 1]R$, 0-code, $g = (1,1,3,\dots, 3)$. The parameters of the code V are $r = RC,\ c \geqslant 9,\ 2^c > 8R.\ n < 0.7R2^{r/R} + 0.35 \times 2^{r/R} - R.$ ■

To reduce N(m), we should increase l and Λ in an attempt to get $R_0^*(l > 0) = R_0$. To estimate $R_0^*(l)$ it is useful to have the coset weight enumerators of the code V_0, the code word configurations in V_0, or (equivalently) the configurations of groups of linearly dependent (l.d.) columns of the matrix Φ^s. These groups may be used to form the zero column in E^s and to alter the number of columns of the matrix Φ^s whose sum produces some column in E_0^s. The latter is achieved by including some group of l.d. columns as addends in the sum. The columns from the group that entered the sum prior to this inclusion "cancel out". If $d_0 \leq R_0$, where d_0 is the minimum distance of the code V_0, then $R_0^*(1) = R_0$. If $d_0 > R_0$, then always $R_0^*(l > 0) > R_0$.

Suppose that Φ^s is constructed as ADS or DS from the matrices Φ_j, $j = 1,2,\dots$ [1]. ADS should be constructed so that only one column in Φ^s is "mixed" and contains one column from each matrix Φ_j. In this case, Φ^s preserves all the groups of l.d. columns from Φ_j which did not include the mixed column. (Good results are obtained when Φ_j is the Golay code check matrix, producing codes with $n \approx 0.577R2^{r/R}$.)

DS preserves in the matrix Φ^s all the groups of l.d. columns contained in the matrices Φ_j.

Example 7. $R \geq 16$ (this constraint is associated with simplification of parameter bounds), $R_0 = R$, V_0 is $[2R + b, b]R$-code, $b = \lceil R/a \rceil$, $1 \leq a \leq R/3$. The matrix Φ^s is formed as the DS of $b - 1$ check matrices of $[2a + 1, 1]a$-code and the check matrix of $[2a_M + 1, 1]a_M$-code, $a_M = R - (b - 1)a$. Each matrix Φ_j, $j = 1, \dots, b - 1$, is a group of $2a + 1$ l.d. columns. We can thus show that $R_0^*(R - 2a) = R$ and V_0 is $[2R + b, b]R$, $(R - 2a)$-code. Let $\Lambda = l = R - 2a$, $\rho = 2a$, $g = (1,1,1,3,3,\dots, 3)$ for $2a = 3\mu$, $g = (1,1,2,3,3,\dots, 3)$ for $2a = 3\mu + 1$, and $g = (1,1,3,3,\dots, 3)$ for $2a = 3\mu + 2$. Using (1.5) and minimizing n in (1.3), we obtain after some calculations $a = \lfloor (192R/311)^{1/2} \rfloor \approx 0.785\sqrt{R},\ b \approx 1.27\sqrt{R},$ which gives the parameters (1.7). ■

Comparing examples 6 and 7 we see that the parameters of the initial code V_0, viewed as a covering code, are better in example 6. But the parameters of the constructed code V are better in example 7, because the parameters of the code V_0, viewed as a R_0^*, l-subset, are more efficient here.

In (1.7) the constant 1.5 in the multiplier $(1 + 1.5\sqrt{}R)$ can be reduced, say, in the following way: do not make all the matrices Φ_j identical, use $g \in G_i(\rho)$, $i = 2, 3$, use in $D_\times^{mR}(g, \rho)$ the codes of example 6 or (iteratively) the codes of example 7. A constructive technique to reduce this constant (to 0.5) is by using as Φ_j the check matrix of the 1st order Reed—Muller $[2^t, t + 1]a_t$-code, where $a_t = 2^{t-1} - 2^{t/2-1}$, t is an even number (see [1, p. 389], [20, Sec. 1.9, Chap. 14]). This matrix may be partitioned in $2^t - 1$ ways into two nonintersecting groups of l.d. columns with 2^{t-1} columns in each group.

The matrix Φ^s may be constructed in the following way. Take (as the base for the construction of the code V_0) some auxiliary code V_0^* with check matrix Φ_*^s. Including in Φ_*^s additional columns that form l.d. groups, we obtain the matrix Φ^s.

Example 8. $R \geq 16$, $R_0 = R$, V_0^* is $[Q^*, Q^* - s]R$-code, $Q^* = w_1^*R2^{s/R} + w_2^*2^{s/R}$, w_1^*, w_2^* are constants. Let $p \leq R/3$, $f = \lceil Q^*/p \rceil$. Partition the columns of the check matrix Φ_*^s of the code V_0^* into f nonintersecting groups, $f - 1$ of which contain p columns each. To each group add a column equal to the sum of its columns. This gives the matrix Φ^s. It is easy to verify that V_0 is $[Q^* + f, Q^* + f - s]R$, $(R - p)$-code. Let $\Lambda = R - p$, $\rho = p$, $g \in G_1(p, 2, 1)$, for instance, $g = (1,1,3,3,\dots, 3)$ for $p = 3\mu + 2$. As in example 6, we use (1.5) and minimizing the length n of the code V we obtain after calculations $p = \lfloor (384Q^*/311)^{1/2} \rfloor \approx 1.1\sqrt{Q^*},\ f \approx 0.9\sqrt{Q^*}$. This produces the code V with the parameters

$$r = s + mR,\quad 2^m > Q^* + 0.9\sqrt{Q^*},\quad q = 1 + 2.2/\sqrt{Q^*},\quad n < w_1^*qR2^{r/R} + (w_2^*q + 0.6/2^{s/R})2^{r/R}. \tag{5.2}$$

The constant 2.2 can be reduced by using in $D_\times^{mR}(g, \rho)$ the codes of example 7. ■

The codes constructed in this paper have high rates. We see from examples 3-8 that for large R the parameters of the constructed codes are conveniently written in the form

$$n = wR2^{r/R} + o(R2^{r/R}) = UR^2 + o(R^2), \tag{5.3}$$

$$U = wg2^v,\ r = r_{\min} + vR,\ r_{\min} = \lceil R \log_2 gR \rceil,\ 2^{r/R} = gR2^v,$$

where $w < 1$, $g > 1$ are constants (in general, not integers) that are fixed for a specific code family; $v \geq 0$ is an integer constant which may increase without bound (this defines a *family* of codes); $r_{\min}$ is the minimum value of r for which the code V of the given family can be constructed.

The constant w determines the quality of the constructed code family; the reduction of this constant is a basic problem in the construction of asymptotically good codes with parameters of the form (5.3). The constant g sets a lower bound on r. For the codes (1.7), $16 \geq g > 8$.

Let us estimate w by the spherical packing bound: $2^r \leqslant \sum_{i=0}^{R} C_n^i$. By Stirling's formula $C_n^R < n^R e^R / (\sqrt{2\pi R} R^R)$. For sufficiently large R, we have $(2\pi R)^{1/2R} \sim 1$, $n \sim UR^2$, and $n > e^{-1} R 2^{r/R} \approx 0.367 R 2^{r/R}$.

For the codes (1.7), $w = 0.5$. For comparison note that if a code with covering radius R is constructed as ADS of Hamming codes, then $w = 1$; if we use ADS of the codes (1.2) from [18], then $w = 0.875$.

For sufficiently large R, the covering density ensured by codes with the parameters (5.3) and $w = 0.5$ is $\bar{\mu}[R, V] = \sum_{i=0}^{R} C_n^i / 2^r \sim (we)^R / \sqrt{2\pi R} \sim (e/2)^R$.

In accordance with example 8, the construction (3.5) preserves the value of the constant w used in the base code V_0^*. In this respect, it is interesting to use as V_0^* the 1st order Reed—Muller codes, which are used in the analysis of the Gale—Berlekamp switching game (light-bulb codes) [1, 5, 12, 17], and the ADS of these codes. These codes lead to $w < 0.5$. Thus [1, formula (80)], from light-bulb codes with $l = m = 81$ we obtain a code V with $w = 0.4977$.

The code V_0^* is essentially shorter than V. Therefore, if the code V_0^* with a good value of w is chosen by enumeration, the construction complexity of the code V may be acceptable (for $m \sim Q^*$, $n \sim 2^{Q^*} Q^*$, the code V is constructed in polynomial time even if the code V_0^* has exponential complexity).

Let us compare our results with those available for finite n, R.

The results (1.8) and (1.9) improve respectively Table I of [1] and Table II of [16]. Most of the results that follow from (3.1), (3.5), and (4.4) lie outside these tables.

For $R = 2$, there is a number of infinite code families [1, 16, 18]. Among these families, the codes of [18] have the best parameters (see (1.2)). The codes (1.4) constructed in this paper have shorter length and lower covering density than the codes (1.2) for even $r \geq 10$.

Pairs of values n, k for which we do not know if $t[n, k]$ equals precisely 2 or 3 are given in [1] (Theorem 30 and the following remark). Using the codes (1.4), we can reduce the number of such uncertain pairs. Thus, for $55 \times 2^{c-5} - 2 \leq n < 56 \times 2^{c-5} - 2$ we obtain from (1.4) $t[n, k = n - 2c] = 2$, whereas from [1, 18] we have $2 \leq t[n, k] \leq 3$.

Codes with $R = 3$ can be compared with (1.5) if they are constructed as ADS of Hamming codes and codes (1.2). This produces, for instance, the family $\bar{V}$ with the parameters $R=3$, $n=9\times 2^{c-2}-3$, $r=3c-1$, $c\geqslant 4$, $\bar{\mu}[3, \bar{V}]\approx 3{,}79$, which are worse than in (1.5). But note that (here and in other cases) new codes are not constructed for relatively small r. Thus, in (1.5), $r \geq 26$, $r \geq 21$, $r \geq 14$, while in the last formula for known codes $r \geq 11$.

On the whole, for finite n and R, the constructions (3.1) and (3.5) produce a *variety* of possible covering codes. For r values when these constructions are applicable, they often produce better results than standard constructions. Note the relatively low covering density in (1.4), (1.5).

I would like to acknowledge the useful comments of V. M. Blinovskii, G. A. Kabatyanskii, and A. N. Skorobogatov. This paper has benefited from constructive discussion of results at the seminar on algebraic coding theory at the Institute of Problems of Information Transmission of the Academy of Sciences of USSR.

LITERATURE CITED

1. R. L. Graham and N. J. A. Sloane, "On the covering radius of codes," IEEE Trans. Inform. Theory, **31**, No. 3, 385-401 (1985).
2. G. D. Cohen, M. G. Karpovsky, H. F. Mattson, Jr., and J. Shatz, "Covering radius: survey and recent results," IEEE Trans. Inform. Theory, **31**, No. 3, 328-343 (1985).
3. T. Helleseth, "On the covering radius of cyclic linear codes and arithmetic codes," Discr. Appl. Math., **11**, No. 2, 157-173 (1985).

4. G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, "Further results on the covering radius of codes," IEEE Trans. Inform. Theory, **32**, No. 5, 680-694 (1986).

5. H. F. Mattson, Jr., "An improved upper bound on covering radius," Lect. Notes Comput. Sci., **228**, 90-106 (1986).

6 . P. Delsart and P. Piret, "Do most binary linear codes achieve the Goblick bound on the covering radius?" IEEE Trans. Inform. Theory, **32**, No. 6, 826-828 (1986).

7. N. J. A. Sloane, "A new approach to the covering radius of codes," J. Combin. Theory, Ser. A, **42**, No. 1, 61-86 (1986).

8. V. M. Blinovskii, "Asymptotic lower bound for the number of words of a linear code in an arbitrary sphere of a given radius in F_q^n," Prob. Peredachi Inform., **23**, No. 2, 50-53 (1987).

9. K. E. Kilby and N. J. A. Sloane, "On the covering radius problem for codes. I. Bounds on the normalized covering radius," SIAM J. Algebra Discr. Math., **8**, No. 4, 604-618 (1987).

10. K. E. Kilby and N. J. A. Sloane, "On the covering radius problem for codes. I. Of low dimension; normal and abnormal codes," SIAM J. Algebra Discr. Math., **8**, No. 4, 619-627 (1987).

11. A. R. Calderbank and N. J. A. Sloane, "Inequalities for covering codes," IEEE Trans. Inform. Theory, **34**, No. 5, Part 2, 1276-1280 (1988).

12. J. Pach and J. Spencer, "Explicit codes with low covering radius," IEEE Trans. Inform. Theory, **34**, No. 5, Part 2, 1281-1285 (1988).

13. I. S. Honkala and H. O. Hämäläinen, "A new construction for covering codes," IEEE Trans. Inform. Theory, **34**, No. 5, Part 2, 1343-1344 (1988).

14. G. A. Kabatyanskii and V. I. Panchenko, "Unit sphere packings and coverings of the Hamming space," Prob. Peredachi Inform., **24**, No. 4, 3-16 (1988).

15. S. G. Vlĕduts and A. N. Skorobogatov, "Covering radius for long BCH codes," Prob. Peredachi Inform., **25**, No. 1, 38-45 (1989).

16. R. A. Brualdi, V. S. Pless, and R. M. Wilson, "Short codes with a given covering radius," IEEE Trans. Inform. Theory, **35**, No. 1, 99-109 (1989).

17. P. C. Fishburn and N. J. A. Sloane, "The solution to Berlekamp's switching game," Discr. Math., **74**, No. 3, 263-290 (1989).

18. E. M. Gabidulin, A. A. Davydov, and L. M. Tombak, "Codes of covering radius 2 and other new covering codes," Proc. 10th All-Union Symp. on Redundancy Problem in Information Systems, abstracts of papers [in Russian], part 1, Leningrad (1989), pp. 14-17.

19. V. M. Blinovskii, "Asymptotically exact uniform bounds for spectra of cosets of linear codes," Prob. Peredachi Inform., **26**, No. 1, 99-103 (1990).

20. F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam (1977).

21. S. I. Samoilenko, A. A. Davydov, V. V. Zolotarev, and E. I. Tret'yakova, Computer Networks (Adaptivity, Error-Tolerance, and Reliability) [in Russian], Nauka, Moscow (1981).

22. A. K. Aidinyan, "On matrices with nonsingular square submatrices," Prob. Peredachi Inform., **22**, No. 4, 106-108 (1986).

23. W. Tatt, Graph Theory [Russian transosetlation], Mir, Moscow (1988).