Theory of codes with maximum rank distance (translation)

Article *in* Problems of Information Transmission · January 1985

1 author:

Ernst Gabidulin
Moscow Institute of Physics and Technology

ISSN 0032-9460

Russian Original Vol. 21, No. 1, January-March, 1985

July, 1985

PRITA9 21(1) 1-76 (1985)

PROBLEMS OF INFORMATION TRANSMISSION

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

(PROBLEMY PEREDACHI INFORMATSII)

TRANSLATED FROM RUSSIAN

CONSULTANTS BUREAU, NEW YORK

THEORY OF CODES WITH MAXIMUM RANK DISTANCE

È. M. Gabidulin

UDC 621.391.15

The article considers codes over $GF(q^N)$. A new metric, called the rank metric, is introduced; the maximum number of coordinates of vector $\mathbf{x} = (x_1,\ldots,x_n)$ that are linearly dependent over $GF(Q)$ is called its norm. For this metric a theory analogous to the theory of MDS codes is formulated. Codes with maximum rank distance are described; their spectrum is obtained; and encoding and decoding algorithms are given.

1. INTRODUCTION

Most studies in algebraic coding theory deal with the Hamming metric. Other metrics are also of interest, however, since the Hamming metric is not always well matched to the characteristics of real channels. In this paper we introduce a new metric, called the rank metric.

Assume that X^n is an n-dimensional vector space over field $GF(q^N)$, where q is a power of a prime. Assume that $u_1, u_2,\ldots,u_N$ is some fixed basis of field $GF(q^N)$, regarded as a vector space over $GF(q)$. Any element $x_i \in GF(q^N)$ can be uniquely represented in the form $x_i = a_{1i}u_1 + a_{2i}u_2 + \ldots + a_{Ni}u_N$. Assume that A_N^n denotes the ensemble of all $(N \times n)$ matrices with elements from $GF(q)$.

We specify the bijection $A: X^n \to A_N^n$ by the following rule: for any vector $\mathbf{x} = (x_1, x_2,\ldots,x_n)$

$$A(\mathbf{x}) = \begin{Vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ a_{N1} & a_{N2} & \ldots & a_{Nn} \end{Vmatrix}. \tag{1}$$

The rank of vector $\mathbf{x}$ over $GF(q)$ is defined as the rank of matrix $A(\mathbf{x})$. In other words, the rank of a vector is the maximum number of its coordinates that are linearly independent over $GF(q)$. We will denote the rank of $\mathbf{x}$ over $GF(q)$ by $r(\mathbf{x}; q)$. Similarly, the rank of $(r \times n)$ matrix $\mathbf{B}$ with elements from $GF(q^N)$ over $GF(q)$ is the maximum number of columns that are linearly independent over $GF(q)$. We will denote it by $r(\mathbf{B}; q)$. Obviously, $r(\mathbf{B}; q) \geqslant r(\mathbf{B}; q^N)$.

The mapping $\mathbf{x} \to r(\mathbf{x}; q)$ specifies a norm on X^n. Indeed, $r(\mathbf{x}; q) \geqslant 0$, $\forall \mathbf{x} \in X^n$ and $r(\mathbf{x}; q) = 0$ if and only if $\mathbf{x} = 0$. In addition, $r(\mathbf{x} + \mathbf{y}; q) \leqslant r(\mathbf{x}; q) + r(\mathbf{y}; q)$ in accordance with a familiar property of matrices. Finally, if for $a \in GF(q^N)$ we set $|a| = 0$ for $a = 0$ and $|a| = 1$ for $a \neq 0$, then $r(a\mathbf{x}; q) = |a| r(\mathbf{x}, q)$, since multiplication of a vector by a nonzero field element does not alter the linear relationship between its coordinates.

The norm $r(\mathbf{x}; q)$ specifies a rank metric (rank distance) on X^n:

$$d(\mathbf{x}, \mathbf{y}) = r(\mathbf{x} - \mathbf{y}; q).$$

In what follows, we will employ the standard terminology of coding theory. Code $\mathfrak{M}$ of volume M is an arbitrary set $\{\mathbf{x}_1, \mathbf{x}_2,\ldots,\mathbf{x}_M\}$ of vectors from X^n. The code distance $d = d(\mathfrak{M}) = \min d(\mathbf{x}_i, \mathbf{x}_j), i \neq j$. A linear code or (n, k)-code is a subspace of X^n of dimension k.

In this paper we present the theory of rank-error-correcting codes, for the case $n \leqslant N$. We describe constructions of codes that have maximum possible volume for specified d. We determine the spectrum of these codes, and we describe encoding and decoding algorithms.

2. MAXIMUM-RANK-DISTANCE CODES

The following elementary lemma is useful in estimating the volume of codes.

Translated from Problemy Peredachi Informatsii, Vol. 21, No. 1, pp. 3-16, January-March, 1985. Original article submitted September 7, 1984.

LEMMA 1. Assume that two norms r_1 and r_2 are specified on X^n, where $r_1(x) \leq r_2(x)$, $\forall x$. Assume that $M_1(n, d)$ and $M_2(n, d)$ are the greatest metrics. Then

$$M_1(n, d) \leq M_2(n, d).$$

Indeed, any code of volume M with distance d in metric r_1 is a code of the same volume with distance $d' \geqslant d$ in metric r_2.

COROLLARY. For any linear (n, k)-code the rank distance satisfies the inequality

$$d \leq n-k+1. \tag{2}$$

Indeed, we choose $r_1 = r(x; q)$ and $r_2 = r_H(x)$, where r_H is the Hamming norm. Obviously, $r(x; q) \leqslant r_H(x)$. Then (2) follows from Lemma 1 and the corresponding inequality for the Hamming metric.

Codes for which equality is attained in (2) are called maximum-rank-distance codes (or MRD codes).

The theory of such codes is in many respects analogous to the theory of MRD codes for the Hamming metric [1].

Assume that H and G are the check and generating matrices of linear (n, k)-code $\mathfrak{M}$.

THEOREM 1. Code $\mathfrak{M}$ has rank distance d if and only if for any $[(d-1) \times n]$ matrix Y of rank $d-1$ with elements from GF(q)

$$r(YH^T; q^N) = d-1 \tag{3}$$

and when there exists a $(d \times n)$ matrix Y_0 of rank d with elements from GF(q), for which

$$r(Y_0H^T; q^N) < d. \tag{4}$$

Proof. First we note that any vector $g = (g_1, g_2, \ldots, g_n)$ such that $r(g; q) \leqslant d$ can be represented in the form $g = zY_0$, where Y_0 is some $(d \times n)$ matrix of rank d with elements from GF(q), while $z = (z_1, z_2, \ldots, z_d)$, $z_i \in GF(q^N)$, $i = 1, \ldots, d$.

Assume that code $\mathfrak{M}$ contains code word g with rank norm d. Then $g = zY_0$ and

$$gH^T = zY_0H^T = 0. \tag{5}$$

Consequently, condition (4) is satisfied. Since the code does not contain words with norm less than d, for any $[(d-1) \times n]$ matrix Y of rank $d-1$ with elements from GF(q) the equation

$$(z_1, z_2, \ldots, z_{d-1}) YH^T = 0$$

should have only a trivial solution, i.e., condition (3) should be satisfied.

Sufficiency is obvious.

THEOREM 2. Code $\mathfrak{M}$ is a linear MRD (n, k)-code if and only if for any $[(n-k) \times n]$ matrix Y of rank $n-k$ with elements from GF(q)

$$r(YH^T; q^N) = n-k. \tag{6}$$

Indeed, in this case, on the basis of Theorem 1 we have $d \geqslant n-k+1$, while the corollary to Lemma 1 yields $d \leqslant n-k+1$, i.e., $d = n-k+1$.

THEOREM 3. If $\mathfrak{M}$ is an MRD code, then its dual code $\mathfrak{M}^\perp$ is also an MRD code.

Proof. The generating matrix of code $\mathfrak{M}^\perp$ is matrix H. It follows from (6) that for any word $h \in \mathfrak{M}^\perp$ and any $[(n-k) \times n]$ matrix Y of rank $n-k$ with elements from GF(q)

$$Yh^T \neq 0. \tag{7}$$

Assume that there exists a word h whose rank norm does not exceed k. Then it can be represented in the form $h = zX = (z_1, z_2, \ldots, z_k)X$, where X is a $(k \times n)$ matrix of rank k with elements from GF(q). In accordance with (7), for any Y the relation $YX^Tz^T \neq 0$ should be observed. On the other hand, for any $(k \times n)$ matrix X of rank k with elements from GF(q) there exists an orthogonal $[(n-k) \times n]$ matrix Y_0 of rank $n-k$ with elements from GF(q), i.e., $Y_0X^T = 0$, $Y_0X^Tz^T = 0$. The resultant contradiction showed that code $\mathfrak{M}^\perp$ does not contain words with norm that does not exceed k. Consequently, the code distance of $\mathfrak{M}^\perp$ is equal to $k+1$ and it is an MRD code.

3. SPECTRUM OF MRD CODES

We denote by $A_s(n, d)$ the number of words with rank norm s in a linear MRD (n, k)-code with distance $d = n - k + 1$. It turns out that the spectrum of an MRD code, i.e., the array of numbers $A_s(n, d)$, $s = 0, 1, \ldots, n$, is uniquely determined by the dimension of the code.

The following numbers play an important part in the formulation of the results:

$$\begin{bmatrix} n \\ m \end{bmatrix} = \frac{(q^n-1)(q^n-q)\ldots(q^n-q^{m-1})}{(q^m-1)(q^m-q)\ldots(q^m-q^{m-1})}. \tag{8}$$

If q is a power of a prime, then $\begin{bmatrix} n \\ m \end{bmatrix}$ is the number of m-dimensional subspaces of an n-dimensional vector space over $GF(q)$. For arbitrary real or complex q, the expression $\begin{bmatrix} n \\ m \end{bmatrix}$ is called a Gauss polynomial [2]. Let us enumerate some properties of such polynomials, which will be employed in what follows:

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = \begin{bmatrix} n \\ n \end{bmatrix} = 1, \tag{9}$$

$$\begin{bmatrix} n \\ m \end{bmatrix} = \begin{bmatrix} n \\ n-m \end{bmatrix} \quad 0 \leqslant m \leqslant n, \tag{10}$$

$$\begin{bmatrix} n \\ m \end{bmatrix} = \begin{bmatrix} n-1 \\ m \end{bmatrix} + q^{n-m}\begin{bmatrix} n-1 \\ m-1 \end{bmatrix}, \tag{11}$$

$$\begin{bmatrix} n \\ m \end{bmatrix}\begin{bmatrix} m \\ p \end{bmatrix} = \begin{bmatrix} n \\ p \end{bmatrix}\begin{bmatrix} n-p \\ n-m \end{bmatrix} \quad 0 \leqslant p \leqslant m \leqslant n, \tag{12}$$

$$\sum_{i=0}^{n} (-1)^i \begin{bmatrix} n \\ i \end{bmatrix} z^i q^{i(i-1)/2} = (-1)^n (z-1)(zq-1)\ldots(zq^{n-1}-1). \tag{13}$$

In particular, for $z = 1$ we obtain

$$\sum_{i=0}^{n} (-1)^i \begin{bmatrix} n \\ i \end{bmatrix} q^{i(i-1)/2} = 0, \quad n \geqslant 1. \tag{14}$$

Using (12) and (14), we can readily verify the pair of reciprocal relations

$$a_m = \sum_{j=0}^{m} \begin{bmatrix} d+m \\ d+j \end{bmatrix} b_j,$$

$$b_m = \sum_{j=0}^{m} (-1)^{m+j} \begin{bmatrix} d+m \\ d+j \end{bmatrix} q^{(m-j)(m-j-1)/2} a_j, \tag{15}$$

$$m = 0, 1, 2, \ldots, d-1, 2, 3, \ldots$$

LEMMA 2. Assume that H is the check matrix of an MRD (n, k)-code with distance d. Assume that Z^T is an $(n \times s)$ matrix of rank s with elements from $GF(q)$, $s \geqslant d = n - k + 1$. Then matrix $\tilde{H} = HZ^T$ is the check matrix of MRD $(s, k + s - n)$ code $\tilde{\mathfrak{M}}$ with the same distance.

It is sufficient to establish that for any $[(d-1) \times s]$ matrix W of rank $d - 1$ with elements from $GF(q)$

$$r(W\tilde{H}^T;\ q^N) = d - 1. \tag{16}$$

Obviously, however, the rank of $[(d-1) \times n]$ matrix $Y = WZ$ with elements from $GF(q)$ is equal to $d - 1$, since on the basis of Theorem 1 we have $r(YH^T;\ q^N) = r(W\tilde{H}^T;\ q^N) = d - 1$.

If the columns of matrix H are regarded as the basis of an n-dimensional vector space over $GF(q)$, then the columns of matrix $\tilde{H} = HZ^T$ form the basis of an s-dimensional subspace of it. The number of different s-dimensional subspaces is $\begin{bmatrix} n \\ s \end{bmatrix}$. Two matrices $\tilde{H}_1 = HZ_1^T$ and $\tilde{H}_2 = HZ_2^T$ will generate the same subspace or, in other words, will be the check matrices of the same MRD code $\tilde{\mathfrak{M}}$ if and only if $Z_1^T = Z_2^T Q^T$, where Q^T is some nonsingular square matrix of order s with elements from GF(q).

Assume that H and $\tilde{H} = HZ^T$ are the check matrices of MRD codes $\mathfrak{M}$ and $\tilde{\mathfrak{M}}$ of lengths n and s, respectively. If z is some word of code $\tilde{\mathfrak{M}}$, then

$$g = zZ \tag{17}$$

is a word of code $\mathfrak{M}$. Different words z_1 and z_2 of code $\tilde{\mathfrak{M}}$ correspond to different words g_1 and g_2 of $\mathfrak{M}$. Indeed, if the equality $z_1 Z = z_2 Z$ were to hold, then the equation $vZ = 0$ would have a nontrivial solution $v = z_1 - z_2$; but this is impossible, since the rank of Z is equal to s, i.e., to the dimension of vector v.

Conversely, if the norm of vector g from $\mathfrak{M}$ is equal to s, then it corresponds to a single code $\tilde{\mathfrak{M}}$ of length s. Indeed, if $g = z_1 Z_1 = z_2 Z_2$, then the ranks of vectors z_1 and z_2 are identical and equal to s. It follows that square submatrices of order s of matrices Z_1 and Z_2, defined by the same numbers of columns, have the same rank. In particular, assume that U_1 and U_2 are such submatrices of rank s. Since $z_1 U_1 = z_2 U_2$, we have $z_2 = z_1 U_1 U_2^{-1} = z_1 Q$; Q is a nonsingular matrix with elements from GF(q). Consequently, $Z_1 = QZ_2$ and check matrices $\tilde{H}_1 = HZ_1^T = HZ_2^T Q^T$ and $\tilde{H}_2 = HZ_2^T$ define the same code $\tilde{\mathfrak{M}}$.

Thus, we have proved the following lemma.

LEMMA 3. Different words with rank norm s of code $\tilde{\mathfrak{M}}$ correspond to different words with rank norm s of code $\mathfrak{M}$. Each word with rank norm s of $\mathfrak{M}$ corresponds to a single code $\tilde{\mathfrak{M}}$.

THEOREM 4. We have the following equality:

$$A_s(n,d) = \begin{bmatrix} n \\ s \end{bmatrix} A_s(s,d), \quad d \le s \le n. \tag{18}$$

Indeed, each code $\tilde{\mathfrak{M}}$ contains $A_s(s, d)$ words with rank norm s. There are $\begin{bmatrix} n \\ s \end{bmatrix}$ such codes in all. In view of Lemma 3, the corresponding words in $\mathfrak{M}$ are different, have rank s, and exhaust the entire set of words with rank norm s.

COROLLARY. We have

$$\sum_{i=d}^{r} \begin{bmatrix} r \\ i \end{bmatrix} A_i(i,d) = (q^N)^k - 1 = Q^{r-d+1} - 1, \quad Q = q^N. \tag{19}$$

THEOREM 5. The spectrum of code $\mathfrak{M}$ is described by the formulas

$$A_0(n,d) = 1,$$
$$A_{d+m}(n,d) = \begin{bmatrix} n \\ d+m \end{bmatrix} \sum_{j=0}^{m} (-1)^{j+m} \begin{bmatrix} d+m \\ d+j \end{bmatrix} q^{(m-j)(m-j-1)/2} (Q^{j+1} - 1), \quad m = 0, 1, \ldots, n-d. \tag{20}$$

Setting $r = d + m$, $i = d + j$, $Q^{m+1} - 1 = a_m$, $m = 0, 1, \ldots$, in (19), we obtain

$$\sum_{j=0}^{m} \begin{bmatrix} d+m \\ d+j \end{bmatrix} A_{d+j}(d+j, d) = a_m = Q^{m+1} - 1.$$

On the basis of the second formula in (15), we can determine the $A_{d+j}(d + j, d)$; the $A_{d+m}(n, d)$ are obtained from (18).

4. CLASS OF MRD CODES

We will describe an extensive class of MRD codes for lengths $n \le N$. These codes are analogs of generalized Reed–Solomon codes [1]. For purposes of simplification, we introduce the notation $[i] = q^i$, $i = 0, \pm 1, \ldots$.

Assume that $h_i \in GF(q^N)$, $i = 1, 2, \ldots, n$, and assume that these elements are linearly independent over GF(q). We specify an integer $d \le n$, and we generate the matrix

$$H = \begin{vmatrix} h_1 & h_2 & \ldots & h_n \\ h_1^{[1]} & h_2^{[1]} & \ldots & h_n^{[1]} \\ \ldots & \ldots & \ldots & \ldots \\ h_1^{[d-2]} & h_2^{[d-2]} & \ldots & h_n^{[d-2]} \end{vmatrix}. \tag{21}$$

THEOREM 6. Code $\mathfrak{M}$ with check matrix H is an MRD code of length n with distance d.

Proof. In accordance with Theorem 2, it is sufficient to establish that for any [(d − 1) × n] matrix Y of rank d − 1 with elements from GF(q) we have $r(HY; q^N) = d - 1$. Square matrix HY^T has the form

$$HY^T = \begin{vmatrix} f_1 & f_2 & \dots & f_{d-1} \\ f_1^{[1]} & f_2^{[1]} & \dots & f_{d-1}^{[1]} \\ \dots & \dots & \dots & \dots \\ f_1^{[d-2]} & f_2^{[d-2]} & \dots & f_{d-1}^{[d-2]} \end{vmatrix}, \tag{22}$$

where $(f_1, f_2, \dots, f_{d-1}) = (h_1, h_2, \dots, h_n)Y^T$. The quantities $f_i \in GF(q^N)$, $i = 1, \dots, d-1$, are linearly independent over GF(q), since otherwise the h_i, $i = 1, \dots, n$, would also be linearly dependent, in contradiction to our assumption. It is known (see, e.g., [1]) that in this case matrix HY^T is nonsingular, i.e., $r(HY^T, q^N) = d - 1$.

THEOREM 7. Assume that $\mathfrak{M}$ is a code with check matrix (21). Then generating matrix G has the form

$$G = \begin{vmatrix} g_1 & g_2 & \dots & g_n \\ g_1^{[1]} & g_2^{[1]} & \dots & g_n^{[1]} \\ \dots & \dots & \dots & \dots \\ g_1^{[k-1]} & g_2^{[k-1]} & \dots & g_n^{[k-1]} \end{vmatrix}, \tag{23}$$

where $k = n - d + 1$, while the elements $g_1, g_2, \dots, g_n$ are linearly independent over GF(q).

Indeed, this is obvious for $d = n - 1$, since on the basis of Theorem 6 there exist elements $\lambda_1, \lambda_2, \dots, \lambda_n$ that are linearly independent over GF(q) and satisfy the relations

$$\sum_{i=1}^{n} \lambda_i h_i^{[s]} = 0, \quad s = 0, 1, \dots, n-2. \tag{24}$$

We take the elements $g_1 = \lambda_1^{[-n+1]}, \dots, g_n = \lambda_n^{[-n+1]}$ to be the first row in matrix (23). These elements are linearly independent over GF(q), and, using (24), it is easy to establish that $GH^T = 0$.

Polynomials with coefficients from $GF(q^N)$ play an important part in the theory of MDS codes. Generalized Reed–Solomon codes, cyclical codes, and so forth can be described in terms of them. Linearized polynomials play a similar role in the theory of MRD codes. A linearized polynomial is one of the form $F(z) = \sum_{i=0}^{n} f_i z^{[i]}$ (see, e.g., [1, 3]; we recall the notation $[i] = q^i$). Let us cite some known results regarding linearized polynomials that will be required in what follows.

Sums of polynomials are defined in the customary fashion: $F(z) + G(z) = \sum_i f_i z^{[i]} + \sum_i g_i z^{[i]} = \sum_i (f_i + g_i) z^{[i]}$. We will utilize the symbolic product $F * G = F(G(z))$ as the multiplication operation. This operation is not commutative; generally speaking, $F * G \neq G * F$. The operations we have introduced convert the ensemble of all linearized polynomials into a noncommutative ring without divisors of zero with polynomial $f_1(z) = z$ as an identity element. Euclid's algorithm regarding division (whether left or right) of one polynomial by another exists in this ring. In what follows, we will consider only right division.

Assume that $F_0(z)$ and $F_1(z)$ are two linearized polynomials, where $\deg F_1(z) \leqslant \deg F_0(z)$. Then there exists a sequential chain of equalities

$$\begin{aligned} &F_0(z) = G_1(z) * F_1(z) + F_2(z), && \deg F_2 < \deg F_1, \\ &F_1(z) = G_2(z) * F_2(z) + F_3(z), && \deg F_3 < \deg F_2, \\ &\dots\dots\dots\dots\dots\dots \\ &F_{s-1}(z) = G_s(z) * F_s(z) + F_{s+1}(z), && \deg F_{s+1} < \deg F_s, \\ &F_s(z) = G_{s+1}(z) * F_{s+1}(z). \end{aligned} \tag{25}$$

The last nonzero remainder $F_{s-1}(z)$ in this chain is the right symbolic LCD of polynomial $F_0(z)$ and $F_1(z)$. If we introduce polynomials $U_i(z)$, $A_i(z)$, $V_i(z)$, and $B_i(z)$, defined recursively for $i \geqslant 1$,

$$
\begin{aligned}
U_i(z) &= U_{i-1}(z) * G_i(z) + U_{i-2}(z), & U_0(z) &= z, & U_{-1}(z) &= 0, \\
A_i(z) &= G_i(z) * A_{i-1}(z) + A_{i-2}(z), & A_0(z) &= z, & A_{-1}(z) &= 0, \\
V_i(z) &= V_{i-1}(z) * G_i(z) + V_{i-2}(z), & V_0(z) &= 0, & V_{-1}(z) &= z, \\
B_i(z) &= G_i(z) * B_{i-1}(z) + B_{i-2}(z), & B_0(z) &= 0, & B_{-1}(z) &= z,
\end{aligned}
\tag{26}
$$

then

$$
\begin{aligned}
F_0(z) &= U_i(z) * F_i(z) + U_{i-1}(z) * F_{i+1}(z), \\
F_1(z) &= V_i(z) * F_i(z) + V_{i-1}(z) * F_{i+1}(z).
\end{aligned}
\tag{27}
$$

In addition,

$$F_i(z) = (-1)^i (B_{i-1}(z) * F_0(z) - A_{i-1}(z) * F_1(z)). \tag{28}$$

Besides the ring introduced above, we consider its factor-ring R_N modulo the polynomial $z^{[N]} - z$, consisting of right classes of reduces with respect to this modulus. The elements of this ring can also be identified with linearized polynomials of degree not higher than $[N - 1]$. Let $F(z) = \sum_{i=0}^{N-1} f_i z^{[i]} \in R_N$. Then

$$F^{[1]}(z) = f_{N-1}^{[1]} z^{[0]} + f_0^{[1]} z^{[1]} + \ldots + f_{N-2}^{[1]} z^{[N-1]}.$$

Thus, raising of a polynomial in ring R_N to the power q is equivalent to raising all its coefficients to the power q and then performing a cyclical shift. This operation will be called a q-cyclical shift. The ideals in R_N are principal ideals and are generated by polynomials $G(z)$ that satisfy the relation $z^{[N]} - z = H(z) * G(z)$, i.e., they are right divisors of polynomial $z^{[N]} - z$ [note, incidentally, that if the high-order coefficient of $G(z)$ is equal to 1, then polynomials $G(z)$ and $H(z)$ commute]. Ideal $\{G\}$ is invariant under q-cyclical shift, i.e., if $g \in \{G\}$, then $g^{[1]} \in \{G\}$ as well.

In terms of linearized polynomials, codes with a generating matrix of form (23) can be described as follows. Assume that $g_1, g_2, \ldots, g_n$ are specified elements, linearly independent over $GF(q)$, of field $GF(q^N)$. Then all vectors of the following form are code words:

$$g = (F(g_1), F(g_2), \ldots, F(g_n)), \tag{29}$$

where $F(z)$ extends over all linearized polynomials of degree not higher than $[k - 1] = q^{k-1}$, with coefficients from $GF(q^N)$.

Now we introduce a class of codes that are analogs of ordinary cyclical codes.

Code $\mathfrak{M}$ is called q-cyclical if a q-cyclical shift of any code vector is also a code vector, i.e., if $(g_0, g_1, \ldots, g_{n-1})$ belongs to $\mathfrak{M}$, then $(g_{n-1}^{[1]}, g_0^{[1]}, \ldots, g_{n-2}^{[1]})$ also belongs to $\mathfrak{M}$. In what follows, we will consider only linear q-cyclical codes, and for simplicity, only the case $n = N$.

Linear q-cyclical code $\mathfrak{M}$ is an ideal of ring R_N. Assume that $G(z) = \sum_{i=0}^{r} G_i z^{[i]}$ is any right divisor of polynomial $z^{[N]} - z$. Then the code consists of all polynomials of the form $c(z) * G(z)$, where $c(z)$ is an arbitrary linearized polynomial of degree not higher than $[N - r - 1]$. In other words, a vector is a code vector if and only if the corresponding polynomial can be divided on the right without remainder by generating polynomial $G(z)$. The dimension of the code is $k = N - r$. Its generating matrix G has the form

$$
G = \begin{vmatrix}
G_0 & G_1 & \ldots & G_r & 0 & \ldots & 0 \\
0 & G_0^{[1]} & \ldots & G_{r-1}^{[1]} & G_r^{[1]} & \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & G_0^{[k-1]} & \ldots & & G_r^{[k-1]}
\end{vmatrix}.
\tag{30}
$$

A code can also be specified using a check polynomial determined from the expression $z^{[N]} - z = G(z) * H(z)$. Vector g is a code vector if and only if the corresponding polynomial $g(z)$ satisfies the relation $g(z) * H(z) = 0 \bmod z^{[N]} - z$.

If $H(z)=\sum_{i=0}^{k} H_i z^{[i]}$ is a check polynomial, then the check matrix has the form

$$H=\begin{vmatrix} H_k & H_{k-1}^{[1]} & \dots & H_0^{[k]} & 0 & \dots & 0 \\ 0 & H_k^{[2]} & \dots & H_1^{[k]} & H_0^{[k+1]} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & & H_k^{[r-1]} & & \dots & H_0^{[N-1]} \end{vmatrix} = \begin{vmatrix} h_0 & h_1 & \dots & h_k & 0 & \dots & 0 \\ 0 & h_0^{[1]} & \dots & h_{k-1}^{[1]} & h_k^{[1]} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & & h_0^{[r-1]} & & \dots & h_k^{[r-1]} \end{vmatrix}, \tag{31}$$

where we have set $H_i^{[k-i]} = h_{k-i}$.

Let us also describe an analog of Reed–Solomon codes. Assume that $\gamma, \gamma^{[1]}, \dots, \gamma^{[N-1]}$ is a normal basis of field $GF(q^N)$. Assume that $G(z)$ is a linearized polynomial whose roots are all possible linear combinations with coefficients from $GF(q)$ of elements $\gamma, \gamma^{[1]}, \dots, \gamma^{[d-2]}$. Then a q-cyclical code with generating polynomial $G(z)$ has rank distance d. Indeed, if $g(z)=\sum_{i=0}^{N-1} g_i z^{[i]}$ is a code polynomial, then $g(z) = c(z) * G(z)$ and hence

$$g(\gamma^{[s]})=\sum_{i=0}^{N-1} g_i \gamma^{[i+s]}=0, \quad s=0, 1, \dots, d-2. \tag{32}$$

Expressions (32) are equivalent to the equality $gH^T = 0$, where $g = (g_0, g_1, \dots, g_{N-1})$, while H is a check matrix:

$$H=\begin{vmatrix} \gamma & \gamma^{[1]} & \dots & \gamma^{[N-1]} \\ \gamma^{[1]} & \gamma^{[2]} & \dots & \gamma^{[N]} \\ \dots & \dots & \dots & \dots \\ \gamma^{[d-2]} & \gamma^{[d-1]} & \dots & \gamma^{[N+d-3]} \end{vmatrix}.$$

This matrix has the same form as matrix (21), so that the rank distance of the code is indeed equal to d. Similarly, the generating matrix of this code can be represented as follows:

$$G=\begin{vmatrix} \beta & \beta^{[1]} & \dots & \beta^{[N-1]} \\ \beta^{[1]} & \beta^{[2]} & \dots & \beta^{[N]} \\ \dots & \dots & \dots & \dots \\ \beta^{[k-1]} & \beta^{[k]} & \dots & \beta^{[N+k-2]} \end{vmatrix},$$

where $\beta, \beta^{[1]}, \dots, \beta^{[N-1]}$ is also some normal basis.

5. CODING OF MRD CODES

In many instances, coding reduces to calculation of the values of linearized polynomials in field $GF(q^N)$. Assume that the generating matrix has the form (23). Then, in accordance with (29), a code word has the form $g = (F(g_1), F(g_2), \dots, F(g_n))$, where $F(z)=\sum_{i=0}^{k-1} u_i z^{[i]}$, $u_0, \dots, u_{k-1}$ are information symbols.

Nonsystematic coding of q-cyclic codes is a particular case of what is described above; here it is necessary to calculate the vector $(F(\beta), F(\beta^{[1]}), \dots, F(\beta^{[N-1]}))$.

As in the case of ordinary cyclic codes, systematic coding can be effected either by means of a check polynomial or by means of a generating polynomial. If $H(z)=\sum_{i=0}^{k} H_i z^{[i]}$ is a check polynomial, then each polynomial $g(z)=\sum_{i=0}^{N-1} g_i z^{[i]}$ satisfies the equality $g(z) * H(z) = 0$, i.e., the conditions

$$\sum_{j=0}^{k} g_{N-t-j+k} H_j^{[N-k-t+j]}=0, \quad t=0, 1, \dots, N-1. \tag{33}$$

If we assume that $g_{N-1}, g_{N-2}, \dots, g_{N-k}$ are information symbols, then we can determine the check symbols $g_{N-k-1}, \dots, g_0$.

Assume that we are given generating polynomial $G(z)=\sum_{i=0}^{N-k} G_i z^{[i]}$. We divide polynomial $G_0(z) = g_{N-1} z^{[N-1]} + \ldots + g_{N-k} z^{[N-k]}$ on the right by $G(z)$:

$$G_0(z)=Q(z)*G(z)+F_1(z),\ \deg F_1<[N-k]. \tag{34}$$

Then the coefficients g_{N-i} for degrees $[N - i]$, $i = k + 1,\ldots,N$, of the remainder will be check symbols.

Usually, calculations in $GF(q^N)$ reduce to calculations in $GF(q)$, with each element of the initial field being represented by some state of an N-position q-ary register. The successive positions of this register are identified with the basis elements of $GF(q^N)$, generally with elements $1, \alpha, \alpha^2,\ldots,\alpha^{N-1}$, where α is a primitive field element. To calculate the values of linearized polynomials, however, it is more convenient to identify the register positions with the normal basis elements $\gamma, \gamma^{[1]},\ldots,\gamma^{[N-1]}$. In this case, raising of any field element to a power amounts nearly to a cyclical shift of the contents of the register that represents this element. In general, operations over linearized polynomials (addition, multiplication, left or right division) are of roughly the same complexity as operations with ordinary polynomials, but we cannot examine this issue in greater detail here.

6. DECODING OF MRD CODES

Codes with check matrices of the form (21) can be decoded using an algorithm that is similar to the one used for generalized Reed-Solomon codes [1].

Assume that $\mathbf{g} = (g_1,\ldots,g_n)$ is the code vector; $\mathbf{e} = (e_1,\ldots,e_n)$ is the error vector; and $\mathbf{y} = \mathbf{g} + \mathbf{e}$ is the received vector. We calculate the syndrome

$$\mathbf{s}=(s_0, s_1,\ldots, s_{d-2})=\mathbf{y}\mathbf{H}^T=\mathbf{e}\mathbf{H}^T. \tag{35}$$

The decoder's problem is to determine the error vector on the basis of the known syndrome vector $\mathbf{s}$. Assume that the rank norm of the error vector is m. Then it can be written in the form

$$\mathbf{e}=\mathbf{E}\mathbf{Y}=(E_1,\ldots, E_m)\mathbf{Y}, \tag{36}$$

where $E_1,\ldots,E_m$ are linearly independent over $GF(q)$, while $\mathbf{Y} = (Y_{ij})$ is an $(m \times n)$ matrix of rank m with elements from $GF(q)$. Then instead of (35) we can write

$$\mathbf{s}=\mathbf{E}\mathbf{Y}\mathbf{H}^T=\mathbf{E}\mathbf{X}, \tag{37}$$

where matrix $\mathbf{X} = \mathbf{Y}\mathbf{H}^T$ has the form

$$\mathbf{X}=\begin{vmatrix} x_1 & x_1^{[1]}\ldots x_1^{[d-2]} \\ x_2 & x_2^{[1]}\ldots x_2^{[d-2]} \\ \cdots & \cdots \\ x_m & x_m^{[1]}\ldots x_m^{[d-2]} \end{vmatrix},$$

and

$$x_p=\sum_{j=1}^{n} Y_{pj}h_j, \quad p=1,\ldots,m, \tag{38}$$

are linearly independent over $GF(q)$. Equation (36) is equivalent to the following system of equations in the unknowns $E_1,\ldots,E_m$, $x_1,\ldots,x_m$:

$$\sum_{i=1}^{m} E_i x_i^{[p]}=s_p, \quad p=0, 1,\ldots, d-2. \tag{39}$$

Assume that a solution of this system has been found. Then we can determine matrix $\mathbf{Y}$ and error vector $\mathbf{e}$ from (38) and (36), respectively. Note that system (39) has many solutions for specified m; for $m \leqslant (d - 1)/2$, however, all the solutions lead to the same vector $\mathbf{e}$.

Thus, the decoding problem reduces to solution of system (39) for the smallest possible value of m.

We introduce polynomial $S(z)=\sum_{j=0}^{d-2} s_j z^{[j]}$. Assume that $\Delta(z)=\sum_{p=0}^{m} \Delta_p z^{[p]}$, $\Delta_m=1$, denotes a polynomial whose roots are all possible linear combinations of $E_1, E_2,\ldots,E_m$ with coefficients from GF(q). Let $F(z)=\sum_{i=0}^{m-1}F_i z^{[i]}$, where $F_i=\sum_{p=0}^{i}\Delta_p s_{i-p}^{[p]}$, $i=0,1,\dots,m-1$.

LEMMA 4. We have the equality

$$F(z)=\Delta(z)*S(z)\ \mathrm{mod}\ z^{[d-1]}. \qquad (40)$$

Indeed

$$\Delta(z)*S(z)=\sum_{p=0}^{m}\Delta_p(S(z))^{[p]}=\sum_{i=0}^{m+d-2}z^{[i]}\Big(\sum_{p+l=i}\Delta_p s_l^{[p]}\Big).$$

But for $m\leqslant i\leqslant d-2$ we have

$$\sum_{p+l=i}\Delta_p s_l^{[p]}=\sum_{p=0}^{m}\Delta_p s_{i-p}^{[p]}=\sum_{p=0}^{m}\Delta_p\Big(\sum_{j=1}^{m}E_j x_j^{[i-p]}\Big)^{[p]}=\sum_{j=1}^{m}x_j^{[i]}\Delta(E_j)=0,$$

since $\Delta(E_j)=0$, $j=1,\dots,m$.

If the coefficients of polynomial $F(z)$ are known, then the coefficients of polynomial $\Delta(z)$ can be determined recursively; specifically, let $s_0=\dots=s_{j-1}=0$, $s_j\neq 0$. Then

$$\Delta_0=F_j/s_j,$$
$$\Delta_p=\Big(F_{j+p}-\sum_{l=0}^{p-1}\Delta_l s_{p+j-l}^{[l]}\Big)\Big/ s_j^{[p]},\quad p=1,2,\dots,m, \qquad (41)$$

where for $j+p\geqslant m$ we set $F_{j+p}=0$.

Now assume that the $E_1,\dots,E_m$, as well as the coefficients of $\Delta(z)$, are known. We consider the following "truncated" system in the unknowns:

$$\sum_{j=1}^{m}E_j x_j^{[p]}=s_p,\quad p=0,1,\dots,m-1. \qquad (42)$$

We will solve (42) using the method of successive elimination of variables. We set $A_{1j}=E_j$, $Q_{1p}=s_p$; we multiply the $(p+1)$-th equation of the system by A_{11}^{q-1}; we extract the root of degree q, and we subtract from the p-th equation. As a result we obtain a system that does not contain x_1:

$$\sum_{j=2}^{m}A_{2j}x_j^{[p]}=Q_{2p},\quad p=0,1,\dots,m-2, \qquad (43)$$

where

$$A_{2j}=A_{1j}-\Big(\frac{A_{1j}}{A_{11}}\Big)^{[-1]}A_{11},\quad j=2,\dots,m,$$
$$Q_{2p}=Q_{1p}-\Big(\frac{Q_{1p+1}}{A_{11}}\Big)^{[-1]}A_{11},\quad p=0,1,\dots,m-2. \qquad (44)$$

Repeating this procedure $m-1$ times, and retaining the first equations obtained from the systems at each step, we arrive at a system of linear equations with a triangular coefficient matrix:

$$\sum_{j=i}^{m}A_{ij}x_j=Q_{i0},\quad i=1,2,\dots,m, \qquad (45)$$

where

$$A_{1j}=E_j,\ j=1,\dots,m;$$
$$A_{ij}=\begin{cases}0, & j<i,\\ A_{i-1,j}-\Big(\dfrac{A_{i-1,j}}{A_{i-1,i-1}}\Big)^{[-1]}A_{i-1,i-1}, & j\geqslant i,\quad i=2,\dots,m,\end{cases} \qquad (46)$$

$$
\begin{aligned}
&Q_{1p}=s_p,\ p=0,1,\ldots,m-1,\\
&Q_{ip}=Q_{i-1,p}-\left(\frac{Q_{i-1,p+1}}{A_{i-1,i-1}}\right)^{[-1]} A_{p-1,i-1},\ p=0,1,\ldots,m-i,\ i=2,\ldots,m.
\end{aligned}
\tag{47}
$$

The solution of system (45) can be found from the recursive formulas

$$
\begin{aligned}
&x_m=Q_{m1}/A_{mm},\\
&x_{m-i}=\left(Q_{m-i,1}-\sum_{j=m-i+1}^{m} A_{m-i,j}x_j\right)\Big/ A_{m-i,m-i},\quad i=1,\ldots,m-1.
\end{aligned}
\tag{48}
$$

Let us now describe the decoding algorithm.

I. We calculate the syndrome $s = (s_0,\ldots,s_{d-2})$ and the corresponding polynomial $S(z) = \sum_{i=0}^{d-2} s_i z^{[i]}$.

II. We set $F_0(z) = z^{[d-1]}$, $F_1(z) = S(z)$ and employ Euclid's algorithm (25) until we reach a $F_{m+1}(z)$ such that

$$
\deg F_m(z)\geq q^{(d-1)/2},\ \deg F_{m+1}(z)<q^{(d-1)/2}. \tag{49}
$$

Then

$$
\begin{aligned}
&\Delta(z)=\gamma A_m(z),\\
&F(z)=\gamma(-1)^m F_{m+1}(z),
\end{aligned}
\tag{50}
$$

where γ is chosen in such a way that the coefficient Δ_m is equal to 1.

Indeed, if the number of rank errors does not exceed $(d-1)/2$, then Eqs. (50) follow from (28) and Lemma 4. The fact that polynomials $F(z)$ and $\Delta(z)$ are unique can be proved in exactly the same way as for the decoding algorithm for ordinary generalized Reed–Solomon codes (see [1]).

Polynomial $\Delta(z)$ can be determined either on the basis of the first formula in (50), if polynomials $A_i(z)$, $i = 1, 2, \ldots$, are calculated in parallel in the course of Euclid's algorithm, or using formulas (41), which employ the coefficients of the remainder $F_{m+1}(z)$ calculated in the course of the algorithm. Then any roots $E_1,\ldots,E_m$ of $\Delta(z)$ that are linearly independent over GF(q) are determined. Some methods of obtaining roots are described in [3]. Some methods of obtaining roots are described in [3].

III. Using (45)–(48), the known $E_1,\ldots,E_m$ are used as a basis for determining $x_1,\ldots,x_m$. Representing these quantities in the form (38), we can obtain matrix **Y**. Finally, we calculate the error vector **e** using formula (36).

As an example, let us consider the case $d = 3$, $q = 2$, in which it is possible to correct single rank errors in a field of characteristic 2.

We calculate the syndrome $s = (s_0, s_1)$.

1. If $s_0 = 0$, $s_1 = 0$, then we conclude that there are no errors.
2. If $s_0 \neq 0$, $s_1 \neq 0$, then the use of Euclid's algorithm leads to a polynomial $\Delta(z) = -(s_0^{[1]}/s_1)z + z^{[1]}$. We conclude that a single error has occurred. We obtain E as the nonzero root of the equation $\Delta(z) = 0$: $E = (s_0^{[1]}/s_1)$. From the single equation of system (44) we determine $x = s_1/s_0 = y_1h_1 + y_2h_2 + \ldots + y_nh_n$, where $y_i = 0$ or 1. The error vector is equal to $e = (y_1E, y_2E,\ldots,y_nE)$.
3. If $s_0 = 0$, $s_1 \neq 0$ or $s_0 \neq 0$, $s_1 = 0$, then we conclude that an error of rank 2 or more has occurred, since the use of Euclid's algorithm in these cases would yield polynomials $\Delta(z) = z^{[1]}$ and $\Delta(z) = z^{[2]}$ that do not have nonzero solutions.

7. ERROR CORRECTION IN HAMMING METRIC

MRD codes are simultaneously MDR codes, and therefore it is natural to raise the question of which errors in Hamming metric will be corrected by the above algorithm. First of all, these include, of course, all Hamming errors of multiplicity not exceeding $t = (d-1)/2$.

Their number is equal to the volume of a Hamming sphere of radius t, i.e., $N=\sum_{i=1}^{t} C_n^i (q^N-1)^i$. For ordinary MBD codes in the general case, Berlekamp's algorithm or its modifications provide correction of only these errors. The decoding algorithm for MRD codes corrects a much greater number of errors, equal to

$$N_t=\sum_{i=1}^{t} L_i(n)=\sum_{i=1}^{t}\begin{bmatrix} n \\ i \end{bmatrix}(q^N-1)(q^N-q)\dots(q^N-q^{i-1}). \tag{51}$$

Here $L_i(n)$ is the number of vectors of length n with elements from $GF(q^N)$, whose rank norm is equal to i.

Let us calculate the number of errors of the Hamming norm s that can be corrected by the algorithm. We denote by $A_n(s, i)$ the number of vectors of length i whose rank and Hamming norms are equal to i and s, respectively. For $s < i$ we set $A_n(s, i) = 0$.

LEMMA 5. We have

$$A_n(s,i)=C_n^s\sum_{k=i}^{s}(-1)^{s+k}C_s^k L_i(k). \tag{52}$$

Indeed, $A_n(s, i) = C_n^s A_s(s, i)$. In addition, for any $i \leqslant s \leqslant n$

$$\sum_{s=i}^{n} A_n(s,i)=\sum_{s=i}^{n} C_n^s A_s(s,i)=L_i(n). \tag{53}$$

Inverting system (53), we arrive at (52).

Lemma 5 yields the following theorem.

THEOREM 8. The decoding algorithm for MRD codes makes it possible to correct

$$M_s=\sum_{i=1}^{t} A_n(s,i)=C_n^s\sum_{i=1}^{t}\sum_{k=i}^{s}(-1)^{s+k}C_s^k L_i(k),\quad s=1,2,\dots,n, \tag{54}$$

errors with Hamming norm s. It can be shown that for $s \leqslant t$ we have $M_s = C_n^s(q^N - 1)^s$.

As an illustration, let us consider codes over $GF(2^N)$ for $n = N$ and $d = 3$. In this case $t = 1$ and the overall number of errors that can be corrected is $N_1 = (2^N - 1)^2$, in accordance with (51). Of these, $M_1 = C_N^1(2^N - 1)$ have Hamming norm 1, while $M_2 = C_N^2(2^N - 1)$ have Hamming norm 2. The proportion of correctable binary errors is $1/(2^N - 1)$. The norm of the remaining correctable errors is greater than or equal to 3. By some improvement of the algorithm, it is also possible to interpret these errors as Hamming binary errors. Assume, for example, that in the basic algorithm we have obtained error vector (E, E,...,E, 0,...,0), whose rank norm is 1, and whose Hamming norm $s \geqslant 3$. We solve the system

$$\begin{aligned} Xh_1+Yh_2&=E(h_1+h_2+\dots+h_s),\\ Xh_1^{[1]}+Yh_2^{[1]}&=E(h_1^{[1]}+h_2^{[1]}+\dots+h_s^{[1]}), \end{aligned} \tag{55}$$

where $h_1, h_2,\dots,h_N$ are the elements of the first row of the check matrix of the code. Then vector (X, Y, 0,...,0) has Hamming norm 2 and lies in the same coset as vector (E, E,...,E, 0,...,0). For the Hamming metric, therefore, the improved algorithm makes possible an appreciable approximation to the complete decoding algorithm. The complete algorithm corrects $2^{2N} - 1$ single and double errors. Our proposed algorithm corrects $(2^N - 1)^2$ single and double errors, i.e., only $2^{N+1} - 2$ double errors remain uncorrected as compared to the complete algorithm.

Similar improvements are also possible for codes with greater code distances, although the complexity of the additional part of the algorithm increases rapidly with the number of errors to be corrected.

LITERATURE CITED

1. F. J. McWilliams and N. J. A. Sloane, Theory of Error-Correcting Codes [in Russian], Svyaz', Moscow (1979).
2. G. Andrews, Theory of Partitions [Russian translation], Nauka, Moscow (1982).
3. E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill (1968).

CONVOLUTIONAL-BLOCK CODING IN CHANNELS WITH DECISION FEEDBACK

B. D. Kudryashov

UDC 621.391.15

The article describes a method of transmitting information over channels with decision feedback, based on combined use of block and convolutional coding principles. A bound is obtained for the decoding error probability as a function of the length of the code constraint and the transmission rate. It is shown that the error probability decreases exponentially as the complexity of implementation of encoding and decoding increases linearly.

1. INTRODUCTION

Bounds for the error probability that can be achieved using block codes in systems with decision feedback (DF) were obtained by Forney in [1]. It was shown in [2] that the use of convolutional codes yields some gain in error probability as compared to block codes, for equal complexity of implementation of decoding. The decoding procedures required to attain the bounds in [1, 2] require excessive amounts of computation to obtain a bound for each message, and therefore, despite their good asymptotic characteristics, they cannot compete with the transmission method that is most widely employed in actual communications systems, namely transmission with error detection and repeat transmission of combinations with detected errors.

The transmission method that we will consider here is based on the concatenation principle. The "internal" transmission method is ordinary transmission with DF with block encoding. The "external" method is transmission using a convolutional code with decoding analogous to sequential decoding. When the convolutional-code decoder discovers that the path it has chosen is unsuccessful, it sends a request signal over the feedback channel, in response to which both the encoder and decoder return and repeat the transmission of already-transmitted blocks. It turns out that this concatenated arrangement yields a simple-to-implement transmission method that provides a decoding error probability that is close to the best available bounds for the error probability that can be achieved in systems with DF.

2. DESCRIPTION OF TRANSMISSION METHOD

Let us assume that we employ a discrete memoryless channel for transmission, with input and output alphabets $X = \{x\}$ and $Y = \{y\}$ and transition-probability matrix $\mathcal{P} = \{p(y|x)\}$; there is also a noiseless and delayless feedback channel. The feedback channel can be used to transmit one bit of information over the transmission time for some number n of symbols over the main channel.

A convolutional code is specified as a set of sequences of symbols of alphabet X, corresponding to different paths in some lattice diagram or lattice. We denote by M the number of edges that depart from each node of the lattice, and by n the number of symbols of alphabet X corresponding to each edge of the lattice. Let us assume that messages comprise equiprobable integers $m = 0, 1, \ldots, M-1$. Each sequence of messages $m_1, m_2, \ldots$ corresponds to some path in the diagram (message m_i indicates the number of an edge departing from a node on the i-th tier of the lattice). The sequence of input symbols of the channel corresponding to this path constitutes the code word used to encode the specified sequence of messages. The rate of the convolutional code described above is $R = (\ln M)/n$.

Translated from Problemy Peredachi Informatsii, Vol. 21, No. 1, pp. 17-27, January-March, 1985. Original article submitted June 8, 1982.

0032-9460/85/2101-0012$09.50