A CLASSES OF OPTIMAL AND BURST-ERROR-CORRECTING (n,k)-CODES

R.Megrelishvili, M.Chelidze

Faculty of Exact and Natural Sciences,
Iv. Javakhishvili Tbilisi State University
0143 University Street 2, Tbilisi, Georgia

(Received: 12.09.05; accepted: 15.03.06)

Abstract

There are discussed the classes of generalized Vandermonde determinants over Galois field $GF(q)$. The obtained results enable to synthesize the optimal (satisfying condition [1]) classes of the linear (n,k,d)-codes over $GF(2^m)$ and linear (n,k)-codes with the single and double burst-error-correction. It is considered the problem of representation of Galois $GF(2^m)$ field's elements applying matrices over $GF(2)$.

Key words and phrases: Generalized Vandermonde determinants, Matrices over $GF(q)$, Optimal (n,k,d)-codes, Burst-error-correction, Representation of field's elements applying matrices.

1 Generalized Vandermonde determinants and the optimal and burst-error-correcting (n,k)-codes

From the Theory of the error-correcting linear (n,k,d)-codes it is well known that $n-k \geq d-1$, where n is the length of the code words, k is informational symbols number and d is a minimal distance between the code words. If

$$n-k=d-1, \tag{1.1}$$

then the codes are called the optimal codes [1].

It is known that how important are the properties of Vandermonde determinants for the research and formation of the code structures. However, the generalized Vandermonde determinants, which are so well researched over the fields of real numbers, yet represent problems over Galois fields.

In the given work there are researched the structures of the quadratic matrices over $GF(p^m)$. It is demonstrated that generalized Vandermonde determinants for these matrices differ from 0, that allows to obtain optimal codes over $GF(p^m)$ satisfying the condition (1.1) and also to realize

the synthesis of effective classes of linear burst-error-correcting codes over $GF(2)$.

Let A be the matrix with $\alpha_{ij} = \alpha^{ij} \in GF(2^m), (i, j = 0, 1, ..., m)$ elements of multiplicative subgroup of the Galois field modulo $p(x) = \sum_{\nu=0}^{m} x^{\nu}$, $p(\alpha) = 0$:

$$A = \begin{bmatrix} \alpha_{0,0} & \alpha_{0,1} & .... & \alpha_{0,m} \\ \alpha_{1,0} & \alpha_{1,1} & .... & \alpha_{1,m} \\ . & . & . & . \\ \alpha_{m,0} & \alpha_{m,1} & . & \alpha_{m,m} \end{bmatrix}, \tag{1.2}$$

where m is any integer for which $p(x)$ is irreducible polynomial over $GF(2)$.

Let's consider the quadratic matrices with the elements in the arbitrary i^{th} row and j^{th} column of the matrix (1.2):

$$A_2 = \begin{bmatrix} \alpha_{i_1 j_1} & \alpha_{i_1 j_2} \\ \alpha_{i_2 j_1} & \alpha_{i_2 j_2} \end{bmatrix}, \quad A_3 = \begin{bmatrix} \alpha_{i_1 j_1} & \alpha_{i_1 j_2} & \alpha_{i_1 j_3} \\ \alpha_{i_2 j_1} & \alpha_{i_2 j_2} & \alpha_{i_1 j_3} \\ \alpha_{i_3 j_1} & \alpha_{i_3 j_2} & \alpha_{i_3 j_3} \end{bmatrix} \tag{1.3}$$

where $i_1 \neq i_2 \neq i_3$, $j_1 \neq j_2 \neq j_3 \in \{0, 1, ..., m\}$.

Suppose D_2 and D_3 determinants correspond to the matrices A_2 and A_3 (1.3). Then the following theorem is correct:

Theorem 1.1 *Let $GF(2^m)$ be the Galois Field of polynomials over $GF(2)$ modulo $p(x) = \sum_{\nu=0}^{m} x^{\nu}$, and let α is element of cyclic multiplicative subgroup of $GF(2^m)$, $p(\alpha) = 0$.*

Then

$$D_2 \neq 0, \qquad D_3 \neq 0. \tag{1.4}$$

It is not difficult to show, as well, that the determinant of matrix

$$A_2 = \begin{bmatrix} \alpha_{i,j_1} & \alpha_{i,j_2} & \alpha_{i,j_3} & \alpha_{i,j_3} \\ \alpha_{i+1 j_1} & \alpha_{i+1 j_2} & \alpha_{i+1,j_3} & \alpha_{i+1,j_3} \\ \alpha_{i+2,j_1} & \alpha_{i+2,j_2} & \alpha_{i+2,j_3} & \alpha_{i+2,j_3} \\ \alpha_{i+3,j_1} & \alpha_{i+3,j_2} & \alpha_{i+3,j_3} & \alpha_{i+3,j_3} \end{bmatrix} \tag{1.5}$$

differs from 0, $D_4 \neq 0$, where α are the elements of matrix (1,2) (i; $j_1 \neq j_2 \neq j_3 \neq j_4 \in \{0, 1, ..., \}$).

The obtained results enable to synthesize the optimal (by condition (1.1)) classes linear (n, k, d)-codes over $GF(2^m)$ modulo $p(x) = \sum_{\nu=0}^{m} x^{\nu}$ ($n = m + d$, $k = m + 1$, $d = 3; 5$) and their linear (n, k)-codes over $GF(2)$ with single and double-burst-error-correction (where correspondingly $n =$

$lm(m+1)+2lm$, $k = lm(m+1)$; $n = lm(m+1)+4lm$, $k = lm(m+1)$; $b = (l-1)m+1$ is the burst' length, $l \succeq 1$ is integer).

Particularly from (1.4) and (1.5) follows that the basis matrix

$$G = \begin{bmatrix} 10000 & 1 & 1 & 1 & 1 \\ 01000 & \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ 00100 & \alpha_2 & \alpha_4 & \alpha_1 & \alpha_3 \\ 00010 & \alpha_3 & \alpha_1 & \alpha_4 & \alpha_2 \\ 00001 & \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 \end{bmatrix}$$

generates the optimal ($n = 9$, $k = 5$, $d = 5$)-code over $GF(2^4)$ with double-error-correction, where, $p(x) = 1 + x + x^2 + x^3 + x^4$, and one of the corresponding (n, k)-code over $GF(2)$ has the following parameters: $n = 72$, $k = 40$, $l = 2$, which corrects two error-bursts with length $b = 5$.

Let's discuss the construction of double-burst-error-correcting (n, k)-codes over $GF(2)$ field. Besides (1.5),

$$p_0 = \begin{pmatrix} p_{ij_1} & p_{ij_2} & p_{ij_3} & p_{ij_4} \\ p_{(i+1)j_1} & p_{(i+1)j_2} & p_{(i+1)j_3} & p_{(i+1)j_4} \\ p_{(i+2)j_1} & p_{(i+2)j_2} & p_{(i+2)j_3} & p_{(i+2)j_4} \\ p_{(i+3)j_1} & p_{(i+3)j_2} & p_{(i+3)j_3} & p_{(i+3)j_4} \end{pmatrix} \tag{1.6}$$

is matrix, where P_{ij} $m * m$ matrix of the given multiplicative subgroup element a_{ij} over $GF(2)$ field. The columns of P_{ij}represent the corresponding binary vectors of elements $\alpha_{ij}, \alpha_{ij+1}, ..., \alpha_{ij+m-1}$ (this vectors are from space V_m).[1]

Let $s_{ij}m$-dimensional binary vector be any sum of the columns of matrix P_{ij}, and $s_{ij}(x)$- corresponding polynomial. Vector s_j is corresponded with the polynomial $s_j(x) = \sum\limits_{l=0}^{\gamma} x^{lm} s_{ij}(x)$.[2] Then for any $s_{j_1,...,}s_{j_\gamma}(j_1 \neq ... \neq j_\gamma \in \{0, 1, ..., m\}, \gamma \in \{1, ..., 4\}$ vectors over $GF(2)$ field can be written the following inequality:

$$4 - \gamma < |s_{ij} + ... + s_{ij}| \leq 4, \tag{1.7}$$

where $|x|_m = \min\limits_{\beta}(d(\beta, m))$ is the m-norm of vector $x = (x_0, x_1, ..., x_{n-1})$, i.e. the generalized burst- weight of Hamming weight [2], which is determined according to the following equation:

$$|x| = \sum_{i=1}^{d(\beta,m)} \sum_{i=\beta_i}^{\beta_i'} x_j,$$

[1]Note that P_{ij} matrix and α^{ij} element are equivalent to adding and multiplying operations.

[2]Vectors S_j will be represented as the elements of space V_{4m}.

$\beta_i \neq \beta_{i+1} \in \{0, m, 2m, ..., n-m\}$, $\beta_i^{'} = \beta_i + m + 1\,(i = 1, 2, ..., d(\beta, m)$, $|x|$ is the usual norm of vector x, i.e. Hamming weight.

Let us write the parity-check matrix in the following way:

$$H = (PI_{4m}), \tag{1.8}$$

where analogically to (1.2) and (1.6)

$$P = \begin{pmatrix} P_{0,0} & ... & P_{0,m} \\ P_{1,0} & ... & P_{1,m} \\ P_{2,0} & ... & P_{2,m} \\ P_{3,0} & ... & P_{3,m} \end{pmatrix},$$

$I_{4m}$is the identity matrix of $4m$ order.

It is known that if the burst-error-vector of any $2t$ and less quantity towards H matrix makes non-zero syndromes, then the code representing the zero space of H matrix can correct t burst-errors.

Applying (1.7) equation it is easy to show that for (1.8) matrix

$$\left| \sum_{\nu=0}^{\gamma} s_{j_\nu} \right| \neq 0,$$

where $\gamma \in \{1, ..., 4\}$, s_{j_ν} is the phased burst-syndrome, $j_1 \neq ... \neq j_\gamma \in \{0, 1, ..., m+4\}$. From (1.8) comes out that the constructed code corrects phased-burst-errors of length m. So, for any $m \geq 4$ number, for which polynomial $p(x)$ is irreducible, exists the class of linear $(m^2 + 4m, m^2)$-codes, that corrects double-phased-burst of length m.

Applying the known methods of the block-interleaving (like e.g. in [3,4]) it is possible the construction of double-burst-error-correcting linear (n, k)-codes with parameters $n = lm(m+1)+4lm$, $k = lm(m+1)$, $b = (l-1)m+1$ - length of usual bursts.

Researched codes are based on the new matrix structures. They are better than the codes discussed in [3,4].

2 Representation of Galois $GF(2^m)$ field's elements applying matrices over $GF(2)$

Obtaining operations over the elements of Galois field $GF(q)$ is quite difficult than binary operations. Below is considered the representation of elements $GF(2^m)$ in the form of square matrices of order m over Galois field $GF(2)$:

$$A = \cup A^i, \tag{2.9}$$

where

$$A^i = \begin{pmatrix} \alpha^i \\ \alpha^{i+1} \\ . \\ . \\ . \\ \alpha^{i+2^m-2} \end{pmatrix}; \tag{2.10}$$

α^i is the element of multiplicative group of field $GF(2^m)$ generated by α primitive element. α^i which is written in (2.2) as the vector (see (2.3)).

Applying (2.1) it is obtained the isomorphic field of field $GF(2^m)$ with matrix elements, where operations can be done on usual matrices.

For example, the multiplicative group of $GF(2^3)$ can generated the primitive α of polynomial $p(x) = 1 + x + x^3$ $(p(\alpha) = 0)$:

$$\begin{array}{lll} \alpha^0 = 1 & & -(100) \\ \alpha = & \alpha & -(010) \\ \alpha^2 = & \alpha^2 & -(001) \\ \alpha^3 = 1+\alpha & & -(110) \\ \alpha^4 = & \alpha+\alpha^2 & -(011) \\ \alpha^5 = 1+\alpha+\alpha^2 & & -(111) \\ \alpha^6 = 1+ & +\alpha^2 & -(101) \\ \hline \alpha^7 = 1 & & -(100) \end{array} . \tag{2.11}$$

Here applying the degrees α^i of α is obtained the multiplicative group, and by adding the zero vector is obtained the field $GF(2^m)$. On the right of (2.3) are given the corresponding binary vectors of elements α^i, which with zero vector $0 = (000)$ create vector space $V_{n=3}$ over field $GF(2)$

The corresponding matrix group of the multiplicative group (2.3) is:

$$\begin{aligned} A^0 &= I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, A^1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \\ A^3 &= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, A^4 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \\ A^5 &= \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \end{aligned} \tag{2.12}$$

It is evident, that the set (2.4) with the zero matrix 0 obtains the isomorphic field of $GF(2^m)$.

The additive and multiplicative operations in the matrix set $A = A \cup 0$ is obtained simply. For example, the result got by (2.4),

$$A^2 + A^5 = A^3,$$

corresponds to the result obtained by the elements of (2.3): $\alpha^2 + \alpha^5 = \alpha^2 + (1 + \alpha + \alpha^2) = 1 + \alpha + 2\alpha^2 = 1 + \alpha = \alpha^3$; for multiplication operation:

$$A^3 \cdot A^5 = A,$$

$$\alpha^3 \cdot \alpha^5 = \alpha.$$

It is important, that matrices (2.1), (2.4) significantly simplify the construction of codes considered in the paragraph 1.

Actually, correspondingly to (2.2) it is possible to represent the elements of any field $GF(2^m)$ over field $GF(p)$ applying matrix of order m, and therefore it is possible the construction of the isomorphic matrix field A over field $GF(p)$.

References

1. Mac Williams F.J., Stoane N.J.A. The theory of error-correcting codes. North-Holland Publishing Company, Amsterdam, New York, Oxford, 1977.

2. Megrelishvili R.P. A generalized formulation of code distance. Bulletin of the Georgian Academy of Sciences, v. XLVI, n.2. pp.315-318, 1967 (in Russian).

3. Megrelishvili R.P., Nikolaishvili T.G., Fam Hong Thai. A class of burst-error-correcting (n, k)-codes Bulletin of the Georgian Academy of Sciences, v. 81, n. 2, pp.337-339, 1976 (in Russian).

4. Megrelishvili R.P., Fam Hong Thai. A class of double-burst-error-correcting (n, k)-codes. Bulletin of the Georgian Academy of Sciences, v. 83, n. 2, pp. 321-323, 1976, (in Russian).