Mathematical Problems of Computer Science 43, 57--61, 2015.

Encoding and Decoding Procedures for Double ± 1 Error Correcting Linear Code over Ring Z_5

Hamlet K. Khachatryan

Institute for Informatics and Automation Problems of NAS RA
e-mail: hamletxachatryan.08@gmail.com

Abstract

From practical point of view the codes over Z_{2m} or Z_{2m+1} are interesting, because they can be used in 2^{2m} **–QAM (Quadrature amplitude modulation) schemes.** In this paper a construction of encoding and decoding procedures for double ± 1 error correcting optimal(12,8) linear code over ring Z_5 is presented.

Keywords: Error correcting codes, Codes over the ring Z_5, Encoding and Decoding procedures.

1. Introduction

Codes over finite rings, particularly over integer residue rings and their applications in coding theory have been studied for a long time. Errors happening in the channel are basically asymmetrical; they also have a limited magnitude and this effect is particularly applicable to flash memories.There are many constructed codes capable to correct up to two errors of value ± 1 .The earliest paper discussing the codes over the ring Z_A of integers modulo A are due to Blake [1], [2].

The optimality criteria for the linear code over fixed ring Z_m was considered in 2 ways in [3]. First of all, recall that the code of the length n is optimal-1 if it has a minimum possible number of parity check symbols. Secondly, optimality-2 criteria for the code is that for a given number of parity check symbols it has a maximum possible length. Here, we propose to construct encoding and decoding algorithms for the optimal codes. The code presented in this paper satisfies the optimality criteria-1([3]). At this point we do not know any codes that satisfy the optimality criteria-2. There have been encoding and decoding procedures for the (4, 2) code over ring Z_9 in [4]. Implementation of codes over large alphabets is much more difficult compared with small alphabets. In this paper a construction of encoding and decoding procedures of (12, 8) linear code over ring Z_5 correcting double ± 1 errors is presented.

2. Presentation of the Code

Let a linear (12, 4) code over ring Z_5 be given by the following parity check matrix H:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 1 & 2 & 3 & 4 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 2 & 2 & 2 & 2 & 2 & 1 & 1 \\ 3 & 2 & 4 & 4 & 2 & 3 & 2 & 4 & 4 & 2 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 3 & 2 & 4 & 4 & 2 & 0 & 4 \end{bmatrix}.$$

A linear code over Z_5 given by the parity check matrix H can correct up to two errors of the type ±1, because H has a property according to which all the syndromes resulting from adding and subtracting operations between any two columns of the matrix H are different ($\pm h_i \pm h_j$ and $h_i \neq h_j$)(proof of this you can see in [3]).
In this case the number of combinations for each code word that can be corrected is $(1 + 12 * 2 + (12\, choose\, 2) * 4) = 289$.
For encoding every vector in Z_5 we should have the generator matrix G. For this we should construct a combinatorial equivalent matrix H' from matrix H.

$$H' = \begin{bmatrix} 1 & 0 & 0 & 0 & 3 & 1 & 0 & 3 & 4 & 3 & 4 & 0 \\ 0 & 1 & 0 & 0 & 2 & 2 & 4 & 4 & 0 & 2 & 4 & 3 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 4 & 2 & 1 & 3 & 1 \\ 0 & 0 & 0 & 1 & 1 & 3 & 2 & 0 & 4 & 4 & 3 & 3 \end{bmatrix}.$$

In this matrix all 289 possible syndromes will be different, too.
From [5] we know, that

$$GH'^T = 0. \quad (1)$$

If $\mathrm{H}' = [-\mathrm{P}^{\mathrm{T}}|\mathrm{I}_{\mathrm{n-k}}]$, then $\mathrm{G} = [\mathrm{I}_{\mathrm{k}}|\mathrm{P}]$ (the reverse statement is also true), where I_{k} is a $k * k$ identity matrix and P is a $k * (n - k)$ matrix[5].
Thus, we can construct the generator matrix G:

$$G = \begin{bmatrix} 2 & 3 & 0 & 4 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 3 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 3 & 3 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 3 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & 3 & 4 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 2 & 4 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

3. Encoding and Decoding Procedures

3.1 Encoding Procedure

In our scheme the message was presented by 8-tuples in Z_5. Let G be a generator matrix for (12,8) linear code. $v = (a_1, a_2, a_3, \dots, a_8)$ is an arbitrary 8-tuple, and consider the vector u that is the linear combination of columns G with a_i is the i^{th} coefficient.

$$u = vG = (c_1, c_2, c_3, c_4, a_1, a_2, a_3, \dots, a_8),$$

where the first 4 components of the code vector are the check symbols, the next 8 components are information symbols and

$$c_j = \left(\sum_{i=1}^{k} a_i p_{ij}\right) mod 5. \quad (2)$$

Example.
Let (3 4 0 0 2 1 1 4) be the message vector in Z_5. From (2) we can obtain check symbols. For example, the first check symbol is c_1:

$$c_1 = (3*2) + (4*4) + (0*0) + (0*2) + (2*1) + (1*2) + (1*1) + (4*0) =$$
$$= 6 + 16 + 0 + 0 + 2 + 2 + 1 + 0 = 27 mod 5 = 2 .$$

Similarly, we can find other 3 check symbols:

$$c_2 = 3, \; c_3 = 3, \; c_4 = 3.$$

After performing other multiple operations with matrix G we obtain this encoded vector: (2 3 3 3 3 4 0 0 2 1 1 4).

3.2 Decoding Procedure

In this section we describe the decoding procedure:

1. Receiver multiplies the vector with every column of matrix H' and gets the syndrome $S = vH'$. If $S = (0,0,0,0)$ then there were not any errors in the received vector.
2. If the calculated syndrome S is a nonzero vector, then there are some errors. This (12,8) code can correct only up to two errors with magnitude ±1. We know that all possible syndromes of matrix H' are different ($\pm h_i, \pm h_j$ and $h_i \neq h_j$) (the number of them is 288 and syndrome (0,0,0,0)). After calculating the syndrome the receiver knows from which two columns of the matrix H' the syndrome was resulted, consequently, he can find the two corresponding components of the vector, where the error was occurred and the direction of the error (if $+h_i$, then upward direction or if $-h_i$ downward direction). On the other hand, if in the table of syndromes we do not have the resulted syndrome, then we cannot correct this kind of errors.
3. After finding the error components the receiver adds or subtracts 1 from them (he adds if downward, else subtracts) and obtains the sent code vector $(\boldsymbol{c_1}, \boldsymbol{c_2}, \boldsymbol{c_3}, \boldsymbol{c_4}, \boldsymbol{a_1}, \boldsymbol{a_2}, \boldsymbol{a_3}, \dots, \boldsymbol{a_8})$. So $(\boldsymbol{a_1}, \boldsymbol{a_2}, \boldsymbol{a_3}, \dots, \boldsymbol{a_8})$ ***is our message vector.***

Example.

$(2\ 3\ 3\ 3\ 3\ 4\ 0\ 0\ 2\ 1\ 1\ 4)$ is an encoded vector from the previous example. Let there occur 2 errors in the channel, and the receiver get the vector $(2\ 3\ 3\ 3\ 3\ 4\ 0\ 4\ 2\ 2\ 1\ 4)$. After performing multiple operations with rows of matrix H' the receiver obtains the syndrome $(0\ 3\ 2\ 4)$. Next from the table of syndromes he finds the corresponding columns, now they are -8 and 10. Hence, the syndrome $(0\ 3\ 2\ 4)$ was resulted from adding a negated column 8 of matrix H to column

$$\begin{matrix}-3 & +3 & 0\\ -4 & +2 & -2\\ -4 & +1 & -3\\ 0 & +4 & 4\end{matrix} \quad = \quad (mod 5) \ = \ (0\ 3\ 2\ 4),$$

(because in $Z_5, 0 = 5, -1 = 4, -2 = 3, -3 = 2, -4 = 1$).
Hence, the error positions of encoded vector are 8 and 10 (in 8^{th} downward direction and in 10^{th} upward).
So, he adds 1 to 8^{th} component and subtracts 1 from 10^{th} of vector $(2\ 3\ 3\ 3\ 3\ 4\ 0\ 4\ 2\ 2\ 1\ 4)$ and obtains the sent encoded vector $(2\ 3\ 3\ 3\ 3\ 4\ 0\ 0\ 2\ 1\ 1\ 4)$. Consequently, the message vector is $(3\ 4\ 0\ 0\ 2\ 1\ 1\ 4)$.

4. Conclusion

In this paper a construction of encoding and decoding procedures of optimal-1 (12,8) linear code over ring Z_5 correcting double ± 1 errors is presented. We propose that this approach can be extended for constructing similar procedures for the optimal codes over other rings Z_n and the research in this direction will follow.

References

[1] I. Blake, "Codes over certain rings", *Information and Control*, vol. 20, pp. 396-404, 1972.
[2] I. Blake, "Codes over integer residue rings", *Information and Control*, vol. 29, 1975, 295-300.
[3] G. Khachatrian and H. Morita, "Construction of optimal 1 double error correcting linear codes over ring Z_5", *3th International Workshop on Advances in Communications*, Boppard, Germany, pp. 10-12, May 2014.
[4] H. Kostadinov, N. Manev and H. Morita, "Double ± 1-error correctable codes and their applications to modulation schemes", *Proc. Elev. Intern. Workshop ACCT*, Pamporovo,June 16-22, pp 155-160,2008.
[5] W. W. Peterson and E.J. Weldon, *Error-Correcting Codes*, M.I.T. Press, Cambridge, Mass.,1972.

Submitted 15.10.2014, accepted 12. 02. 2015.

Կոդավորման և ապակոդավորման ալգորիթմը Z5 օղակում ±1 մեծությամբ կրկնակի սխալ ուղղող կոդերի համար

Հ. Խաչատրյան

Ամփոփում

Պրակտիկ տեսանկյունից մեծ հետաքրքրություն են առաջացնում $\boldsymbol{Z_{2m}}$ կամ $\boldsymbol{Z_{2m+1}}$ օղակների վրա դիտարկված կոդերը, քանի որ նրանք ունեն լայն կիրառություն $\mathbf{2^{2m}}$ **–QAM** մոդուլյացիոն սխեմաներում: Այս հոդվածի շրջանակներում ներկայացված է կոդավորման և ապակոդավորման ալգորիթմը **Z5** օղակում ± 1 մեծության մինչև 2 սխալ ուղղող օպտիմալ (12, 8) գծային կոդի համար:

Алгоритм кодирования и декодирования в кольце Z5 для кодов исправляющих двойные ошибки размера ±1

Г. Хачатрян

Аннотация

С практической точки зрения большой интерес вызывают коды на кольцах Z_{2m} и Z_{2m+1}, так как они имеют широкое применение в 2^{2m} **–К А М** модуляционных схемах. В данной статье представлен алгоритм кодирования и декодирования в кольце Z5 для оптимального (12,8) линейного кода, исправляющего до двух ошибок размера ± 1.