Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 155–160*

Double ±1-error correctable codes and their applications to modulation schemes

Hristo Kostadinov[1] hristo@math.bas.bg
Institute of Mathematics and Informatics, BAS and
University of Electro-Communication, Chofu, Tokyo 182-8585, JAPAN
Nikolai L. Manev nlmanev@math.bas.bg
Institute of Mathematics and Informatics,Bulgarian Academy of Sciences,
8 G.Bonchev str., 1113, Sofia, BULGARIA
Hiroyoshi Morita morita@is.uec.ac.jp
University of Electro-Communication, Chofu, Tokyo 182-8585, JAPAN

Abstract. Codes capable to correct two errors of value ±1 in a codeword are constructed and studied. Large number of experiments simulating the implementation of several double ±1-error correctable codes in QAM-modulation schemes have been carried out. The obtained results present in graphical form the performance of the coded modulation schemes based on the considered codes versus signal-to-noise ratio (SNR). The results confirm the good performance of integer coded modulation in comparison to the other schemes for coded modulation.

1 Introduction

Coded modulation is the collective term for all techniques which combine and jointly optimize channel coding and modulation for digital transmission. As a result of more than thirty years intensive investigation numerous and multifarious methods for coded modulation have been proposed. Despite their variety, the coded modulation schemes can be classified in the following three large groups:

- **Trellis coded modulation (TCM)**: It consists in an expanding the input bits by a binary convolutional code and partitioning the used signal constellation into smaller subsets with a larger intra-set distance. A part of coded bits are used to select one of these subsets and the remaining determine which of the signal point in the chosen subset to be transmitted. The Ungerboeck's concept requires a larger signal set than the one used in the case of uncoded modulation.

[1]This work was partially supported by the Japan Society for the Promotion Science (JSPS).

- **Integer coded modulation (ICM)**: A type of block coded modulation - each point of the signal constellation corresponds to a symbol of $\mathbb{Z}_A$ and coded by a code over $\mathbb{Z}_A$.

- **Others**: Coded modulation based on Gaussian and algebraic integers ([3], [6], and others).

Integer codes have proved themselves to be very effective for coded modulation, where errors usually have a given type (see [4, 5]), that is, in the case of modulation schemes where the error-vectors are not equally probable. In partial M-QAM modulation fall in this case.

In this talk we address codes over integer rings which are capable to correct up two errors with values ± 1. We demonstrate their practical potential by numerous simulations and comparisons with one error correctable integers codes and other types of coded modulations.

2 General remarks

Let C be an $[n, k]$ code over the integer ring $\mathbb{Z}_A$. Recall that a t-multiple $(\pm e_1, \pm e_2, \ldots, \pm e_s)$-error correctable code is a code that can correct any up to t errors with values from the set $\{\pm e_i, \mid i = 1, \ldots, s\}$ occurred in a codeword ([1, 4]). Single error correctable codes are discussed in [4, 5]. Herein we restrict our consideration only to the double ± 1-error correctable codes. These codes are interesting since they can be effectively applied to improving the performance of Quadrature Amplitude Modulation (QAM) schemes.

Proposition 1 *Let C be an $[n, k]$ code over the ring $\mathbb{Z}_A$. If C is a double ± 1-error correctable code, then the cardinality, A, of the ring satisfies the inequalities:*

when $k = n - 1$

$$A \geq 2n^2 + 1;$$

when $k = n - 2$

$$A \geq \sqrt{2n^2 + 1}$$

Proof. More generally, the number of the different error vectors when up to t error with values ± 1 occur per a codeword is

$$N_t = \sum_{j=0}^{t} \binom{n}{j} 2^j.$$

This number, N_t, has to be less or equal to the number of possible syndromes. In the case $k = n - 1$ the syndromes are elements of $\mathbb{Z}_A$, that is, their number is A. When $k = n - 2$, the syndromes $\mathbf{s} \in \mathbb{Z}_A \times \mathbb{Z}_A$, and their number is A^2. Hence we must have $A \geq N_2$, respectively $A^2 \geq N_2$, which give the statement.

Let C be a double ± 1-error correctable code with a parity-check matrix

$$\mathbf{H} = (\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n),$$

where the length of the columns is $n-k$, i.e. one ($k = n-1$) or two ($k = n-2$). Therefore $\mathbf{h}_i \neq \pm\mathbf{h}_j,\ i \neq j$, and $\mathbf{h}_i \pm \mathbf{h}_j \neq \pm(\mathbf{h}_l \pm \mathbf{h}_m)$. Also, the permutations and multiplications of columns by -1 transform C into an equivalent code. Hence, we may assume that the first row of $\mathbf{H}$ contains only elements $\leq A/2$, arranged in a nondecreasing order.

Also, the multiplication of a row of $\mathbf{H}$ by an invertible element of $\mathbb{Z}_A$ does not change the code. Hence if there exists an invertible entry of $\mathbf{H}$ we may assume that there is 1 in the first row. Otherwise there is an element that divide A, and all others have g.c.d. with A greater than 1.

Therefore we can assume that the parity check matrix of $[n, n-2]$ double ± 1-error correctable code has the form

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & h_{13} & \ldots & h_{1n} \\ 0 & 1 & h_{23} & \ldots & h_{2n} \end{pmatrix} \qquad \text{or} \qquad \mathbf{H} = \begin{pmatrix} 1 & h_{12} & h_{13} & \ldots & h_{1n} \\ 0 & a & h_{23} & \ldots & h_{2n} \end{pmatrix},$$

where $a \mid A$.

In partial an interesting case is the group of matrices of the form

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 2 & 3 & \ldots & n-1 \\ 0 & 1 & h_{23} & h_{24} & \ldots & h_{2n} \end{pmatrix}$$

over a ring $\mathbb{Z}_A$ with $A \geq 2n - 2$.
Unfortunately, if a code with a given parity-check matrix is double ± 1-error correctable for a given alphabet $\mathbb{Z}_A$ it may not preserve this property as a code over a larger cardinality of the alphabet. For example, the code with a parity-check matrix

$$\mathbf{H} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 0 & 5 & 3 & 6 & 2 & 4 \end{pmatrix}$$

is a double ± 1-error correctable code over $\mathbb{Z}_{15}$, but does not preserve this property over $\mathbb{Z}_{16}$. On the other hand the code with a parity-check matrix given in Example 1 is such a code over both $\mathbb{Z}_8$ and $\mathbb{Z}_9$.

In the case $k = n - 1$ the parity-check matrix is $1 \times n$ and has the form $\mathbf{H} = (1\ h_2\ \ldots\ h_n)$. But according Proposition 1 such codes require large cardinality, A, of the alphabet. Nevertheless a $[2,1]$ code over $\mathbb{Z}_9$ with $\mathbf{H} = (31)$ demonstrates very good performance for 64-QAM.

From practical point of view the codes over $\mathbb{Z}_{2^m}$ or $\mathbb{Z}_{2^m+1}$ are more interesting since they enable the standard 2^{2m}-QAM constellations to be used.

We have found many codes for small length and reasonable alphabet cardinality, but the full classification has not been completed yet.

3 Applications and simulation results

In this section we demonstrate how a double ± 1-error correctable code over $\mathbb{Z}_{2^m+1}$ can be used in real applications for improving the performance of 2^{2m}-QAM.

Example 1. Consider $[4,2]$ code C over $\mathbb{Z}_9$ with a parity-check matrix $\mathbf{H}$ and the corresponding generator matrix $\mathbf{G}$:

$$\mathbf{H} = \begin{pmatrix} 5 & 3 & 1 & 0 \\ 2 & 3 & 0 & 1 \end{pmatrix} \qquad \mathbf{G} = \begin{pmatrix} 1 & 0 & 4 & 7 \\ 0 & 1 & 6 & 6 \end{pmatrix}.$$

The code is double ± 1-error correctable and we apply it to 64-QAM modulation scheme in order to correct errors of type "big square" (see [5]). Recall that in such a coding scheme each point of the constellation is indexed by a pair (x, y) of nonzero elements of an integer ring (in this example Z_9) as shown in Fig.1.

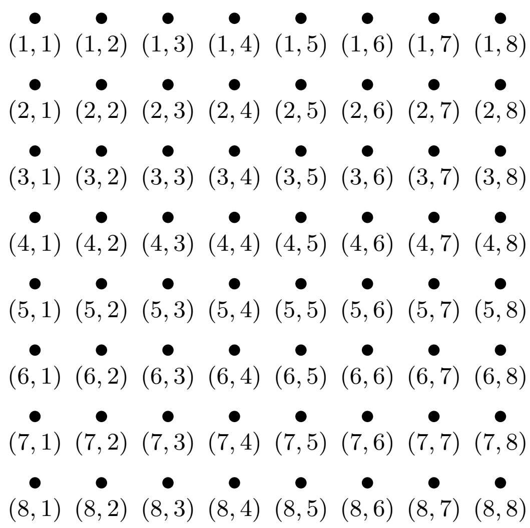

Figure 1: Indexing a 64-QAM constellation

Encoding and decoding procedures

The encoding and decoding procedure on each of the axes are separated. More detailed: Any incoming block of 6 bits is split into two 3-bit groups which are transformed into decimal integers. By adding 1 to each of them we obtain a pair (a, b) of nonzero elements of $\mathbb{Z}_9$. Each of the sequences $a_1, a_2, \ldots$, resp. $b_1, b_2, \ldots$, of the first, resp. the second, coordinates is encoded by the code C. Therefore

$$(a_1, a_2) \longrightarrow (a_1, a_2, 4a_1 + 6a_2, 7a_1 + 6a_2),$$

where the operations are in $\mathbb{Z}_9$. Note that $4a_1 + 6a_2 = 0 \Leftrightarrow 7a_1 + 6a_2 = 0 \Leftrightarrow a_1 = 3a_2$. Since the values of the check bits have to be also nonzero, we replace them with 1 when $a_1 = 3a_2$, that is, $(3a, a) \longrightarrow (3a, a, 1, 1)$.

At the receiver, for each of the axes, the detection procedure (hard or soft) gives as an output a vector $\mathbf{v} = (v_1, v_2, v_3, v_4)$, where $v_j \in \mathbb{Z}_9^*$, . The decoder proceeds both vectors in parallel following the standard syndrome decoding scheme giving at the output a pair (u_1, u_2). The only peculiarity is that after calculating the syndrome vector $\mathbf{s} = \mathbf{vH}$ the decoder uses the syndrome-error table two times: for $\mathbf{s}$ and for $\mathbf{s} - (1, 1)$. In the latter case if the output pair (u_1, u_2) does not satisfy $u_1 = 3u_2$, the result is discarded. Also, if $\mathbf{s}$ does not match to any vector in the table, the decoder gives $u_1 = v_1$ and $u_2 = v_2$.
The correspondence between error frames and syndromes (error-syndrome table) is s given in Table 1.

Error vector	Syndrome	Error vector	Syndrome
1 0 0 0	(5,2)	-1 0 0 0	(4,7)
1 1 0 0	(8,5)	-1 -1 0 0	(1,4)
1 -1 0 0	(2,8)	-1 1 0 0	(7,1)
1 0 1 0	(6,2)	-1 0 -1 0	(3,7)
1 0 -1 0	(4,2)	-1 0 1 0	(5,7)
1 0 0 1	(5,3)	-1 0 0 -1	(4,6)
1 0 0 -1	(5,1)	-1 0 0 1	(4,8)
0 1 0 0	(3,3)	0 -1 0 0	(6,6)
0 1 1 0	(4,3)	0 -1 -1 0	(5,6)
0 1 -1 0	(2,3)	0 -1 1 0	(7,6)
0 1 0 1	(3,4)	0 -1 0 -1	(6,5)
0 1 0 -1	(3,2)	0 -1 0 1	(6,8)
0 0 1 0	(1,0)	0 0 -1 0	(8,0)
0 0 1 1	(1,1)	0 0 -1 -1	(8,8)
0 0 1 -1	(1,8)	0 0 -1 1	(8,1)
0 0 0 1	(0,1)	0 0 0 -1	(0,8)

Table 1: Error-syndrome table.

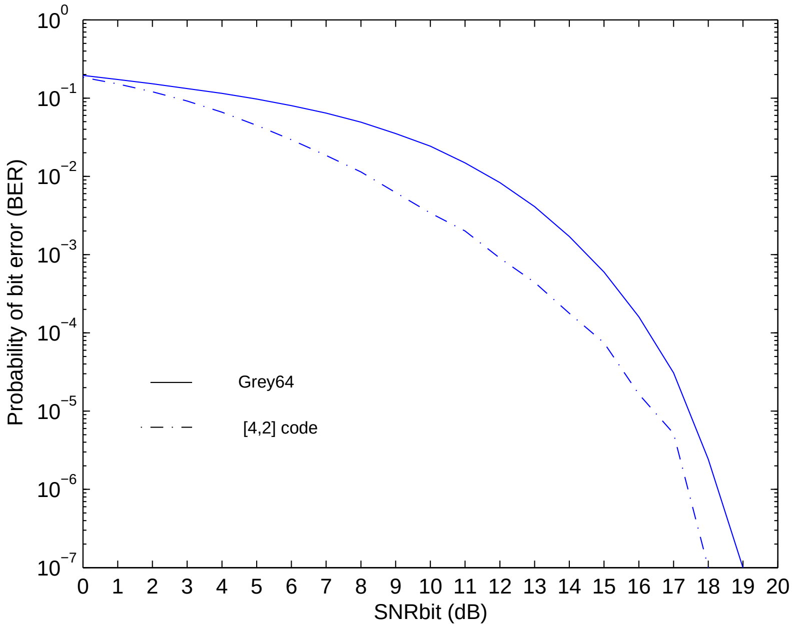

Figure 2: 64-QAM–Grey and $[4,2]$ code over $\mathbb{Z}_9$. (Example 1).

References

[1] A. J. Han Vinck, H. Morita, Codes over the ring of integer modulo m, *IEICE Trans. Fundam.* E81-A, 1998, 2013-2018.

[2] G. Ungerboeck, Channel coding with multilevel/phase signals, *IEEE Trans. Inform. Theory* 28, 1982, 55-66.

[3] K. Huber, Codes over Gaussian integers, —it IEEE Trans. Inform. Theory 40, 1994, 207-216.

[4] H. Kostadinov, H. Morita, N. Manev, Integer codes correcting single errors of specific types $(\pm e_1, \pm e_2, \cdots, \pm e_s)$," *IEICE Trans. Fundam.* E86-A, 2003, 1843-1849.

[5] H. Kostadinov, H. Morita, N. Manev, Derivation on bit error probability of coded QAM using integer codes, *IEICE Trans. Fundam.* E87-A, 2004, 3397-3403.

[6] J. Rifa, Groups of complex integers used as QAM signals, *IEEE Trans. Inform. Theory* 41, 1995, 1512-1517.