Two error correctable codes for coded modulation

Hristo Kostadinov, Nikolai L. Manev

Institute of Mathematics and Informatics, Sofia, Bulgaria

Hiroyoshi Morita

University of Electro-Communication, Tokyo, JAPAN

Introduction

Coded modulation is the collective term for all techniques which combine and jointly optimize channel coding and modulation for digital transmission.

- **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.
- **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.

Integer codes

Integer codes have proved themselves to be very effective when they are applied to modulation schemes usually generating errors of a given type, that is, modulation schemes where all possible errors are not equally probable, and some of them occur more often. For example, M-QAM and M-PSK modulations fall in this case.

Definition. Let C be an $[n, k]$ code over the ring, $\mathbb{Z}_A$, of integers modulo A. We say that C is a t-multiple $(\pm e_1, \pm e_2, \ldots, \pm e_s)$-error correctable code if it can correct up to t errors with values from the set $\{\pm e_1, \pm e_2, \ldots, \pm e_s\}$ which are occurred in a codeword.

Integer codes

Integer codes have proved themselves to be very effective when they are applied to modulation schemes usually generating errors of a given type, that is, modulation schemes where all possible errors are not equally probable, and some of them occur more often. For example, M-QAM and M-PSK modulations fall in this case.

Definition. Let C be an $[n, k]$ code over the ring, $\mathbb{Z}_A$, of integers modulo A. We say that C is a t-multiple $(\pm e_1, \pm e_2, \ldots, \pm e_s)$-error correctable code if it can correct up to t errors with values from the set $\{\pm e_1, \pm e_2, \ldots, \pm e_s\}$ which are occurred in a codeword.

Single error correctable codes are studied in our previous papers. In this talk we address codes over integer rings which are capable of correcting up to two errors with values ± 1.

Bounds on the size of alphabet

Proposition. 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:

for $k = n - 1$

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

for $k = n - 2$

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

The codes which achieve the above bounds are called *perfect*.

Double ± 1-error correctable codes

Let C be an $[n,k]$ code over the integer ring $\mathbb{Z}_A$ with a parity-check matrix

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

where the columns are nonzero and of length $n-k$, i.e. one ($k = n-1$) or two ($k = n-2$).

The condition C is double ± 1-error correctable code is equivalent to

$$\mathbf{h}_i \neq \pm\mathbf{h}_j, \quad (\mathbf{h}_i \pm \mathbf{h}_j) \neq \pm(\mathbf{h}_l \pm \mathbf{h}_m), \quad \text{for any } i \neq j.$$

Equivalences

We may assume that the first row of $\mathbf{H}$ contains only elements of $\mathbb{Z}_A$ which are $\leq A/2$, arranged in a nondecreasing order since the multiplication of column by -1 and permutations of columns transform C into an equivalent code.

Equivalences

We may assume that the first row of $\mathbf{H}$ contains only elements of $\mathbb{Z}_A$ which are $\leq A/2$, arranged in a nondecreasing order since the multiplication of column by -1 and permutations of columns transform C into an equivalent code.

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 one.

Constructions

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

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

where $a \mid A$.

In the case $k = n - 1$ the parity-check matrix is $1 \times n$ and has the form $\mathbf{H} = (1 \; h_2 \; \dots \; h_n)$. Such codes require large cardinality, A, of the alphabet (according to Proposition 1) and are not much useful. Nevertheless a quite simple $[2, 1]$ code over $\mathbb{Z}_9$ with $\mathbf{H} = (13)$ demonstrates very good performance applied to 64-QAM.

Constructions 2

One of our recent goals is to describe up to equivalence the perfect double ± 1-error correctable codes, or codes of minimum possible cardinality A, for small code length. We have not yet completed this work, but we have already collected many examples of codes with small length and reasonable alphabet cardinality.

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.

Applications

Another task is to study the potential of double error correcting codes for applications

The consider code are very effective when they are used for improving the performance of M-QAM modulation.
The example below demonstrates a realization of such an application.

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.

An example of application to 64-QAM

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

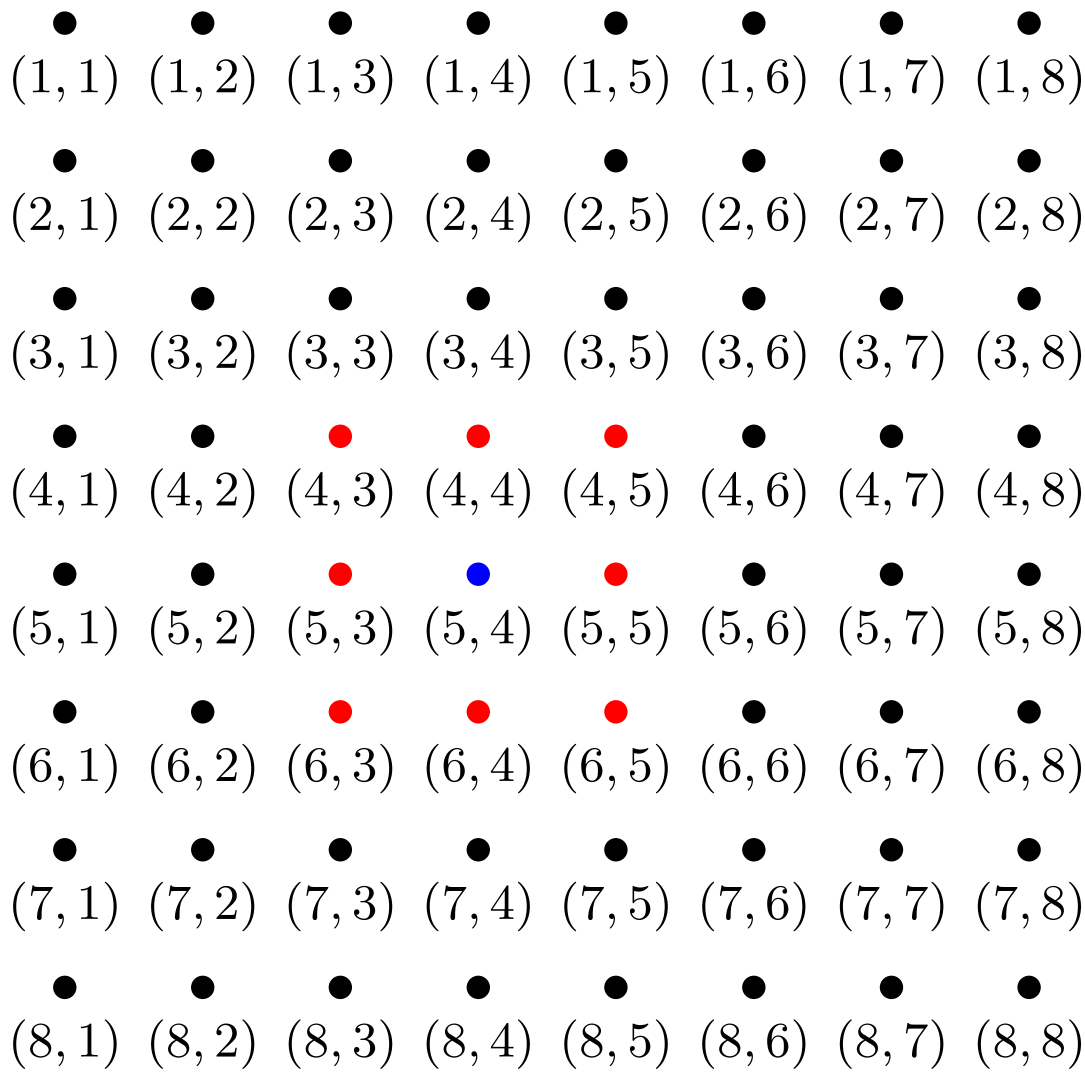
$$\mathbf{H} = \begin{pmatrix} 5 & 3 & 1 & 0 \\ 2 & 3 & 0 & 1 \end{pmatrix} \qquad \mathbf{G} = \begin{pmatrix} 1 & 0 & 4 & 7 \\ 0 & 1 & 6 & 6 \end{pmatrix}.$$

The code is double ± 1-error correctable

Each point of the constellation is indexed by a pair (x, y) of nonzero elements of an integer ring (in this example Z_9)

The encoding/decoding procedure is independently carried out on each of the axes.

Indexing a 64-QAM constellation



The encoding procedure

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. The encoding rule is

$$(a_{2i-1}, a_{2i}) \longrightarrow (a_{2i-1}, a_{2i}, 4a_{2i-1} + 6a_{2i}, 7a_{2i-1} + 6a_{2i}),$$

$$(3a, a) \longrightarrow (3a, a, 1, 1),$$

where the operations are in $\mathbb{Z}_9$.

We replace the check bits with 1 since their values have to be also nonzero. Note that

$4a_{2i-1} + 6a_{2i} = 0 \Leftrightarrow 7a_{2i-1} + 6a_{2i} = 0 \Leftrightarrow a_{2i-1} = 3a_{2i}.$

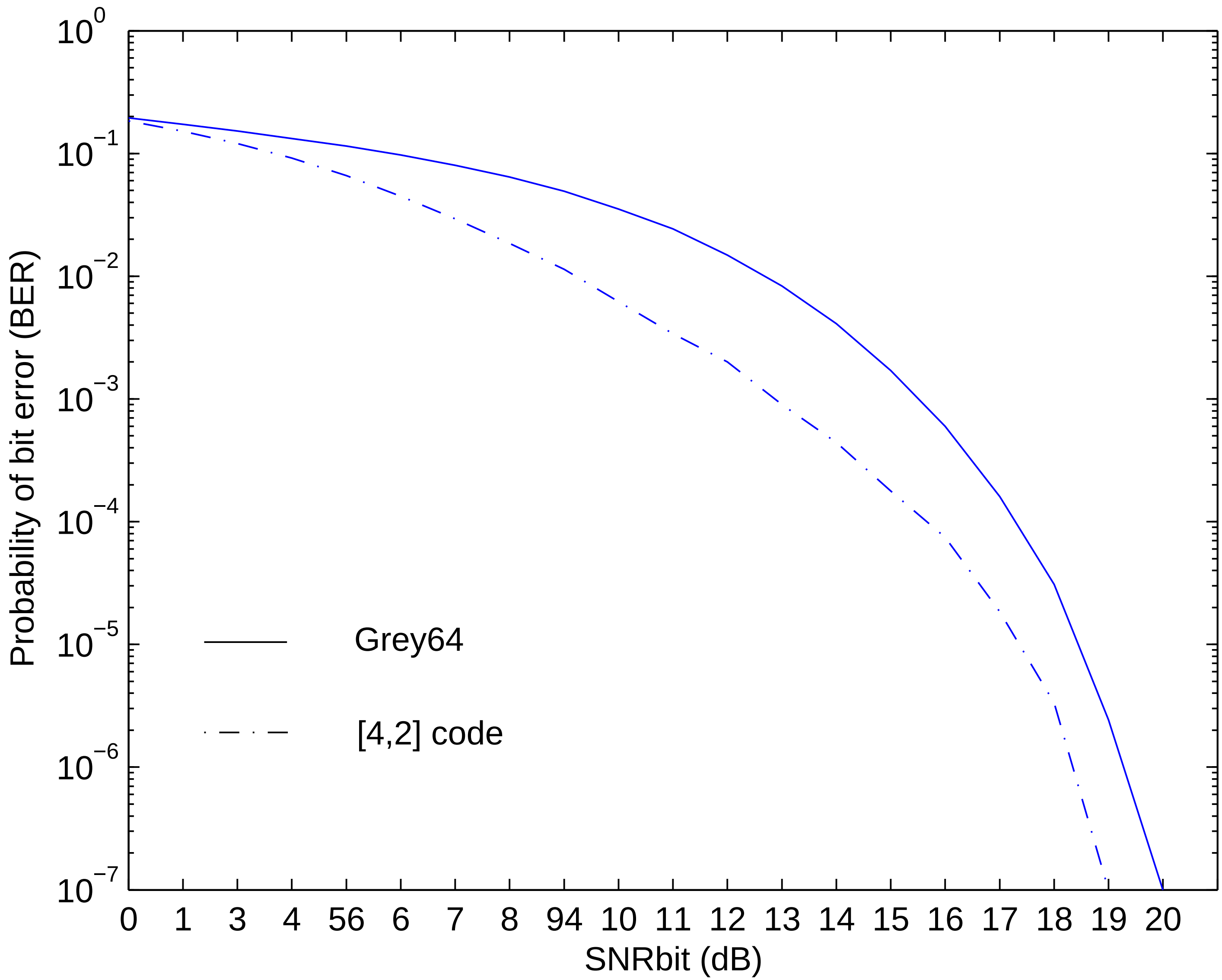
The decoding procedures

At the receiver the detection procedure gives as an output a vector $\mathbf{v} = (v_1, v_2, v_3, v_4)$, $v_j \in \mathbb{Z}_9^*$, for each of the axes. The decoder proceeds both vectors in parallel following the standard syndrome decoding algorithm giving at the output a pair (u_1, u_2). The only peculiarity is that after calculating the syndrome vector $\mathbf{s} = \mathbf{v}\mathbf{H}$ 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 $u_2 = v_2$.

Table of syndromes

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)

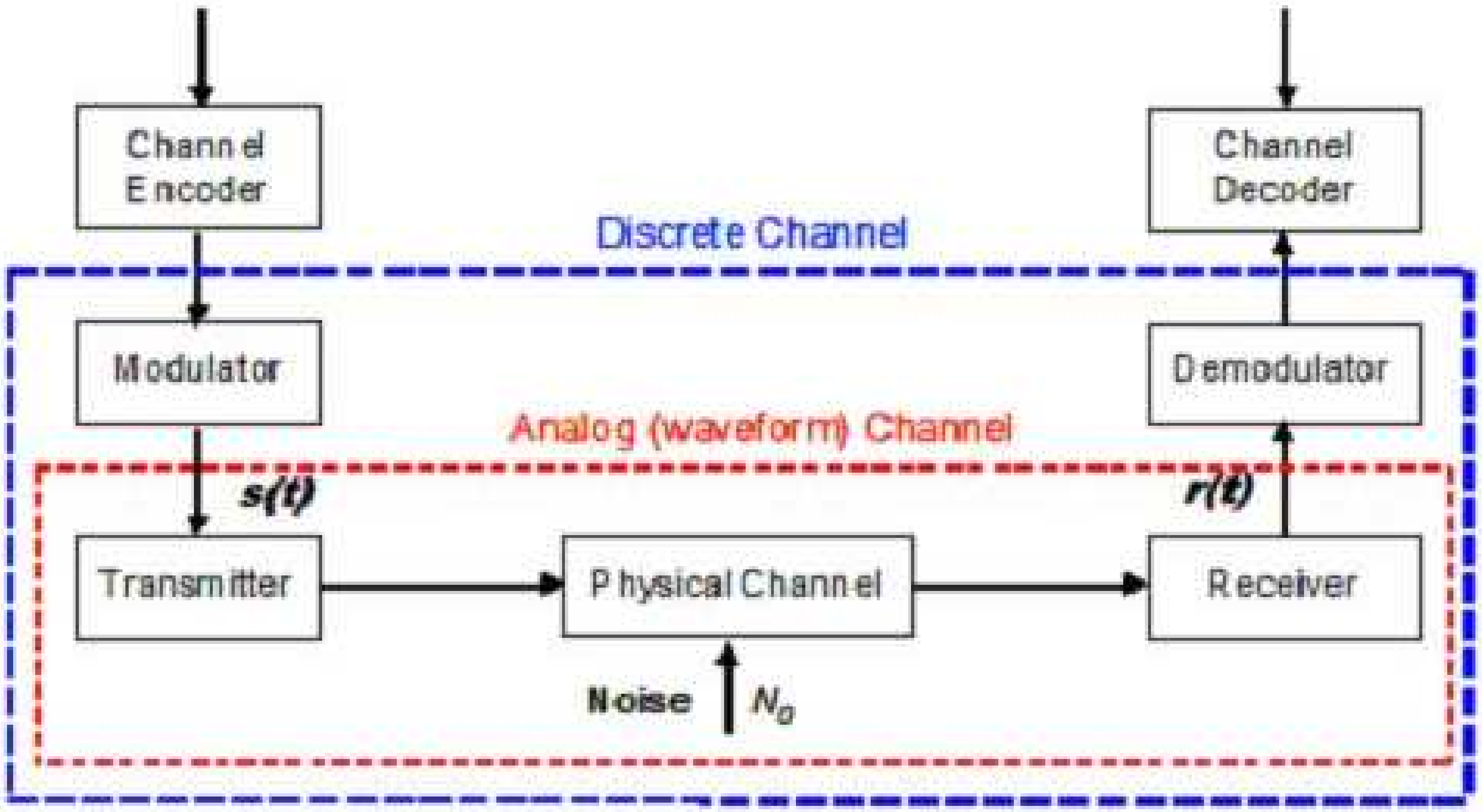
64-QAM–Grey and $[4,2]$ code over $\mathbb{Z}_9$.



Conclusions

This talk should be considered as a part of our recent efforts to popularize integer codes as an effective tool for code modulation.

Integer coding decreases the error rate of the discrete channel and it is independent from the channel coding. Integer codes may thus be combined with various channel coding schemes.


Channel
Encoder
Channel
Decoder
Discrete Channel
Modulator
Demodulator
Analog (waveform) Channel
s(t)
r(t)
Transmitter
Physical Channel
Receiver
Noise
N_0

The end

Thank You for Attention!