Sixth International Workshop on Optimal Codes and Related Topics
June 16-22, 2009, Varna, Bulgaria *pp. 117–124*

On ± 1-error correctable integer residue codes

Hristo Kostadinov 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

Codes over finite rings and in particular codes over integer residue rings and their applications in coding theory have been studied for a long time. The origin of integer codes can be found in [14] where an integer code to correct a single insertion/deletion error per codeword was described. The earliest papers discussing the codes over the ring $\mathbb{Z}_A$ of integers modulo A are due to I. Blake [2, 3]. Some other works in the area are [4, 13, 6]. In [7] and [1] linear block codes over integer rings are studied in order to improve the performance of PSK communication systems.

Let $\mathbb{Z}_A$ be the ring of integers modulo A and $\mathbf{H}$ be an $m \times n$ matrix with entries in $\mathbb{Z}_A$. Recall that an *integer code* over $\mathbb{Z}_A$ of length n with a check matrix $\mathbf{H}$ is referred to as a subset of $\mathbb{Z}_A^n$, defined by

$$\mathcal{C} = \mathcal{C}(\mathbf{H}, \mathbf{d}) = \{\mathbf{c} \in \mathbb{Z}_A^n \mid \mathbf{c}\mathbf{H}^T = \mathbf{d} \bmod A\}$$

where $\mathbf{d} \in \mathbb{Z}_A^m$. Usually $\mathbf{d}$ is the all-zero vector and then we say that $\mathcal{C}$ is an $[n, n-m]$ code.

When a codeword $\mathbf{c} \in \mathcal{C}$ is sent through a noisy channel the received vector can be written in the form

$$\mathbf{r} = \mathbf{c} + \mathbf{e},$$

where $\mathbf{e} = (e_1, \ldots, e_n) \in \mathbb{Z}_A^n$ denotes the error vector. If t of the entries of $\mathbf{e}$ are nonzero, we say that t errors occurred in $\mathbf{c}$.

We do not consider integer codes in general. We are interested in a special class of these codes, namely:

Definition 1 *Let C be an $[n, k]$ code over the integer ring $\mathbb{Z}_A$. C is a t-multiple $(\pm e_1, \pm e_2, \ldots, \pm e_s)$-error correctable code if it can correct (up to) any t errors with values from the set $\{\pm e_i, \mid i = 1, \ldots, s\}$ occurred in a codeword ([15, 8]).*

The above defined codes are suitable for applications to coded modulation. Despite their variety, the coded modulation schemes can be classified in three large groups:

- **Trellis coded modulation (TCM)**: This concept requires a larger signal set than the one used in the case of uncoded modulation and involves convolutional codes. This is a well known, basic and widely used modulation technique.
- **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 ([5], [12], and others).

In this talk we present a part of our research on integer codes which are capable of correcting up to two errors with values ± 1. These codes are interesting since they can be effectively applied to improving the performance of Quadrature Amplitude Modulation (QAM) schemes. We demonstrate their practical potential by numerous simulations and comparisons with other types of coded modulations.

Single error correctable codes are discussed in [8, 9]. Herein we present only one new result (Theorem 2).

2 Why (± 1)-error correctable codes?

Let us consider M-QAM constellation of square type. In this case we have that $M = 2^{2k},\ k = 1, 2, \ldots$. Let us label each signal point in M-QAM constellation by s_{ij}, i.e., by a pair $(i, j) \in \mathbb{Z}_A \times \mathbb{Z}_A$ of elements of $\mathbb{Z}_A$ where $A \geq 2^k$. The counting begin, for example, from the left upper corner down and to right, i for the number of the row and j for the number of the column which s_{ij} is placed in. An example for the case $M = 64$ is depicted on Figure 1.

Let a signal point s_{ij} be sent through a communication channel. At the other end the detector estimates the received signal and gives a signal point, e.g. s_{kl}, at the output. If $(k, l) \neq (i, j)$ the detector has taken a wrong decision. Obviously not all signal points are equiprobable candidates for the detector decision. In the case of AWGN channel the probability a given signal point

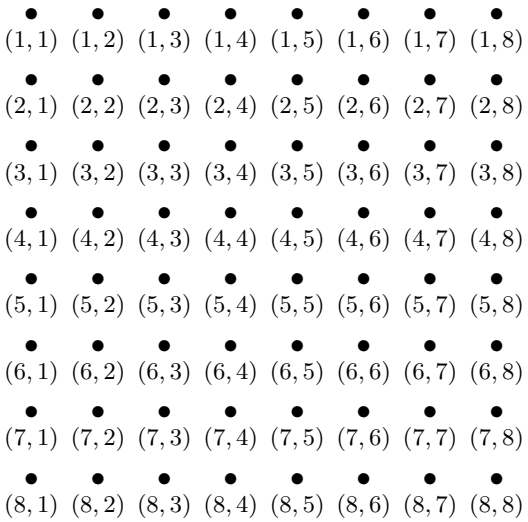

Figure 1: Indexing a 64-QAM constellation

s_{kl} to appear at the output of the detector depends on the Euclidean distance between it and really-sent signal s_{ij}. In terms of chosen labeling it means that signal points with indices $(i \pm 1, j), (i, j \pm 1), (i \pm 1, j \pm 1)$, that is, the points of the "big square" around s_{ij}, are more probable candidate. (In Figure 1 the sent points is s_{44}.)

Therefore, using (± 1)-error correctable code(s) over $\mathbb{Z}_A$ and coding independently first and second indices we can correct a wrong decision if it belongs to the "big square". This reflects in significant decreasing the symbol- and bit-error rate. The problem is discussed again below.

The (± 1)-error correctable codes are also applicable to steganography (see [11]).

3 Theoretical results

Let $\mathcal{C}$ be an $[n, k]$ code over the ring $\mathbb{Z}_A$. The analog of the Hamming bound for the considered codes gives a low bound for the cardinality, A, of the ring in terms of block length and number of errors.

Proposition 1 *If $\mathcal{C}$ correct two errors of type $(\pm e_1, \pm e_2, \ldots, \pm e_s)$ then the cardinality, A, of the ring satisfies the inequality*

$$A^{n-k} \geq 2sn(2sn - n + 1) + 1.$$

In particular if $\mathcal{C}$ is a double ± 1-error correctable code, then

$$A \geq 2n^2 + 1; \qquad \textit{when } k = n - 1 \tag{1}$$

$$A \geq \sqrt{2n^2 + 1} \qquad \textit{when } k = n - 2. \tag{2}$$

The proof is straightforward and we omit it. (Hamming bound for codes over rings and Hamming distance can be found in [].)

To achieve a transmission rate grater than $1/2$ one needs a code of length $n > 3$. But the practice and simulations show that in this case the occurrence of two or more errors per a codeword is very likely. Hence one needs a code capable to correct at least two errors. But (1) shows that the cardinality of the alphabet increases too much even for small block lengths. That is why $[n, n-2]$ codes are preferable from a practical standpoint.

Theorem 2 *Let $l > 1$ be an integer. For every $n \geq 2^{l-1}$ there exists a (± 1) single error correctable code of length n over $\mathbb{Z}_{2^l}$ with an $m \times n$ check matrix,*

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

where m is defined by

$$2^{m-2}\left(2^{(m-1)(l-1)} - 1\right) < n \leq 2^{m-1}\left(2^{m(l-1)} - 1\right)$$

and every column $\mathbf{h}_i$ belongs to

$$S^1 = \{(s_1, s_2, \ldots, s_m)^\tau \mid \ s_1 \in \mathbb{Z}^*_{2^{l-1}},\ s_i \in \mathbb{Z}_{2^{l-1}}, i = 2, \ldots, m\},$$

or to

$$S^2 = \{(s_1, s_2, \ldots, s_m)^\tau \mid \ s_1 \in \{0, 2^{l-1}\},\ s_i \in \mathbb{Z}^*_{2^{l-1}}, i = 2, \ldots, m\}.$$

Corollary 3 *A (± 1) single error correctable integer code of length n over $\mathbb{Z}_{2^l}$ with a check matrix H is quasi-perfect when $n = 2^{ml-1} - 2^{m-1}$.*

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 $n - k$.

The condition C is double ± 1-error correctable code means that the set

$$\{\pm\mathbf{h}_i, \quad \pm(\mathbf{h}_i \pm \mathbf{h}_j), \quad \text{for any } i \neq j\} \tag{3}$$

consists of different (there is no repeating) vector-columns.

Proposition 2 [10] *Up to equivalence the parity check matrix of an* $[n, n-2]$ *double* ± 1*-error correctable code over* $\mathbb{Z}_A$ *has the form*

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

where $a \mid A,\ a > 1$.

Note that every code with a parity check matrix

$$\mathbf{H} = \begin{pmatrix} 0 & 1 & 2 & 3 & \dots & n-1 \\ 1 & 0 & h_{23} & h_{24} & \dots & h_{2n} \end{pmatrix} \tag{4}$$

over a ring $\mathbb{Z}_A$ with $A \geq 2n-1$ is at least single ± 1-error correctable code.

List of codes of small block lengths and over the ring with minimum possible cardinality A can be found at *http://sharoacademy.math.bas.bg/ Research/CommunRes.html*.

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 for the application of a code over $\mathbb{Z}_{2^m+1}$ is given in [10]

Given a signal constellation $\mathcal{K}$ and an integer code $\mathcal{C}$, let q_u and q_c be the average probabilities of a correct decision of the decoder per signal point without and with using the code, respectively. For the both quantities it is well known how to be calculated (for the coded case see [8]). Knowing q_u and q_c, we can evaluate the error probability per symbol for both cases.

Let $X(\mathbf{c})$ be the random variable that represents the number of erroneously decoded symbols per a codeword when the codeword $\mathbf{c}$ is sent. Let $\mathbb{E}X(\mathbf{c})$ denote the expectation of $X(\mathbf{c})$. The average symbol error probability $P_{SE}(\mathcal{C})$ of the code $\mathcal{C}$ is defined as

$$P_{SE}(\mathcal{C}) = \frac{1}{n|\mathcal{C}|} \sum_{\mathbf{c} \in \mathcal{C}} \mathbb{E}X(\mathbf{c}) \tag{5}$$

where n is the length of code $\mathcal{C}$. Since the codewords are equiprobable and usually $\mathbb{E}X(\mathbf{c})$ does not depend on $\mathbf{c}$ we can rewrite (5) as

$$P_{SE}(\mathcal{C}) = \frac{1}{n} \mathbb{E}X(\mathbf{c}) \tag{6}$$

Let a sequence of signal points, $s_{i_1 j_1}, s_{i_2 j_2}, \dots, s_{i_n j_n}$, be sent trough the channel. In the coded case $(i_1, i_2, \dots, i_n)$ and $(j_1, j_2, \dots, j_n)$ are codewords. At the receiver the decoder based on the received signal sequence $r_{i_1 j_1}, r_{i_2 j_2}, \dots, r_{i_n j_n}$, outputs a sequence of signal points $s'_{i_1 j_1}, s'_{i_2 j_2}, \dots, s'_{i_n j_n}$.

The probability of error decision per symbol (for a block of n symbols) in the uncoded case is

$$P_{SE} = \frac{1}{n}(1 - q_u^n). \tag{7}$$

The average symbol error probability $P_{SE}(\mathcal{C})$ depends on the chosen decoding method. In the case of hard decision decoding with a double ± 1-error correctable code applied (as described in Section 2), the following value approximates well the symbol error probability

$$P_{SE}(\mathcal{C}) = \frac{1}{n}\left(1 - q_u^n - nq_u^{n-1}q_c - \binom{n}{2}q_u^{n-2}q_c^2\right) \tag{8}$$

The values of q_u and q_c as a function of M are given in [9].

4 Applications and simulation results

Example 1. Consider $[6, 4]$ code C over $\mathbb{Z}_{16}$ with a parity-check matrix $\mathbf{H}$ and the corresponding generator matrix $\mathbf{G}$:

$$\mathbf{H} = \begin{pmatrix} 5 & 4 & 3 & 2 & 1 & 0 \\ 12 & 6 & 3 & 5 & 0 & 1 \end{pmatrix} \qquad \mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 11 & 4 \\ 0 & 1 & 0 & 0 & 12 & 10 \\ 0 & 0 & 1 & 0 & 13 & 13 \\ 0 & 0 & 0 & 1 & 14 & 11 \end{pmatrix}.$$

The code is double ± 1-error correctable and we apply it to 256-QAM modulation scheme in order to correct errors of type "big square" (see [9]).

The encoder maps any bite into signal point s_{ij}, where the binary representation of i and j are the first four and the last four bits of the bite, respectively. To any four signal points $s_{i_1j_1}, s_{i_2j_2}, s_{i_3j_3}, s_{i_4j_4}$ the decoder adds two points $s_{i_5j_5}$, $s_{i_6j_6}$ such that $(i_1, i_2, \ldots, i_6)$ and $(j_1, j_2, \ldots, j_6)$ are codewords.

In the case of the 256-QAM and the correction type "big square" we have (see [9]):

$$q_u = \{1 + 15\,\mathrm{erf}(\gamma)\}^2/256,$$
$$q_c = \left\{196\,\mathrm{erf}^2(3\gamma) + 56\,\mathrm{erf}(3\gamma) + 4\right\}/264$$

where $\gamma = \sqrt{E_s/170N_0}$ and $\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-u^2}du$.

The described above evaluation of the symbol error probability leaves the decoding algorithm out of account. The choice of a proper decoding algorithm can improve error rate with several dBs. Also, the bit error rate is more relevant than symbol error probability.

We have performed simulations in order to determine the bit error rate using three types of decoding algorithms:

- **Hard decoding**: If a syndrome of the received vector does not belong to the list of possible syndromes the decoder leaves the values (on the corresponding axis) unchanged.
- **Soft decoding**: The classical soft decoding for "big square"(i.e., there are 9 possible values for each signal point).

- **Mixed decoding**: The decoder applies soft decoding when the syndromes are not among the possible ones.

Figure 2 presents the obtained results by simulations of communications through an AWGN channel.

Figure 2: 256-QAM: Grey, hard, and mixed decoding $[6, 4]$ code over $\mathbb{Z}_{16}$. (Example 1).

5 Acknowledgements

The first author is partially supported by the Japan Society for the Promotion Science (JSPS).

The work on simulations was supported by the National Science Fund of Bulgaria under Grant No. D002-146/16.12.2008.

References

[1] R. Baldini, P. G. Farrell, Coded modulation based on rings of integers modulo q, *IEE Proc. Commun.*, 1, 141, 1994, 129-136.

[2] I. Blake, Codes over certain rings, *Inform. Contr.* 20, 1972, 396-404.

[3] I. Blake, Codes over integer residue rings, *Inform. Contr.* 29, 1975, 295-300.

[4] A. R. Calderbank, N. J. A. Sloane, Modular and $p-$adic cyclic codes, *Des., Codes Crypt.* 6, 1995, 21-36.

[5] K. Huber, Codes over Gaussian integers, *IEEE Trans. Inform. Theory* 40, 1994, 207-216.

[6] V. I. Levenstein, A. J. Han Vink, Perfect (d, k)-codes capable of correcting single peak-shifts, *IEEE Trans. Inform. Theory* 39, 1993, 656-662.

[7] M. Nilsson, Linear block codes over rings for phase shift keying, Thesis no. 331, Linköping University, 1993.

[8] 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.

[9] 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.

[10] H. Kostadinov, N. Manev, H. Morita, Double ± 1-error correctable codes and their applications to modulation schemes, *Proc. Elev. Intern. Workshop ACCT*, June 16-22, 2008, Pamporovo.

[11] P. Lisonek, Sum covers in stegonography,*Proc. Elev. Intern. Workshop ACCT*, June 16-22, 2008, Pamporovo.

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

[13] E. Spiegel, Codes over Z_m, *Inform. Cont.* 35, 1977, 48-51.

[14] R. R. Varshamov, G. M. Tenengolz, One asymmetrical error-correctable codes, *Avtom. Telem.* 26, 1965, 288-292, in Russian.

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