On ±1-error correctable integer residue codes

Hristo Kostadinov, Nikolai L. Manev\(^1\)  Hiroyoshi Morita\(^2\)

\(^1\)Institute of Mathematics and Informatics, BAS
\(^2\)University of Electro-Communication, Tokyo

Optimal Codes and Related Topics, June 16-22, 2009
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.
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

Definition

Let $\mathbb{Z}_A$ be the ring of integers modulo $A$ and $H$ be an $m \times n$ matrix with entries in $\mathbb{Z}_A$. An integer code over $\mathbb{Z}_A$ of length $n$ with a parity-check matrix $H$ is a subset of $\mathbb{Z}_A^n$, defined by

$$C = C(H, d) = \{ c \in \mathbb{Z}_A^n | cH^T = d \mod A \}$$

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

The integer codes were introduced by R. Varshamov and Tenengolz (1965) in order to correct a single insertion/deletion error per codeword.
Integer codes

- R. Varshamov and Tenengolz (1965): Ins/Del errors
- Blake 1972-75
- Spigel 1977
- Nakamura 1977: DPSK
- Nilsson 1993: PSK
- Baldini and Farrell 1994
- Vink and Morita 1998: PSK, synch
- Kostadinov, Morita Manev 2003-04: QAM
Error correcting capability

When a codeword \( c \in C \) is sent through a noisy channel the received vector can be written in the form

\[
r = c + e, \quad e = (e_1, \ldots, e_n) \in \mathbb{Z}_A^n.
\]

we say that \( t \) errors occurred in \( c \), if \( t \) of the entries of \( e \) are nonzero.

**Definition**

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 \( \{\pm e_1, \pm e_2, \ldots, \pm e_s\} \), which are occurred in a codeword.
Why $(\pm 1)$-error correctable codes?

Let us consider square $M$-QAM constellation with $M = 2^{2k}$. Let us label each signal point in $M$-QAM constellation by a pair $(i, j) \in \mathbb{Z}_A \times \mathbb{Z}_A$ of elements of $\mathbb{Z}_A$ where $A \geq 2^k$. 
Bounds on the size of alphabet

Proposition

If $C$ 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 $C$ is a double $\pm 1$-error correctable code, then

$$A \geq 2n^2 + 1; \quad \text{when } k = n - 1 \quad (1)$$

$$A \geq \sqrt{2n^2 + 1} \quad \text{when } k = n - 2. \quad (2)$$
Single $\pm 1$-errors correction

**Theorem**

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

$$H = (h_1, h_2, \ldots, h_i, \ldots, h_n),$$

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 $h_i$ 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

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

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

\[
H = \begin{pmatrix}
1 & 0 & h_{13} & \ldots & h_{1n} \\
0 & 1 & h_{23} & \ldots & h_{2n}
\end{pmatrix}
\] or

\[
H = \begin{pmatrix}
1 & h_{12} & h_{13} & \ldots & h_{1n} \\
0 & a & h_{23} & \ldots & h_{2n}
\end{pmatrix},
\]

where \(a \mid A, \ a > 1\).

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

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

- [6, 4] code over $\mathbb{Z}_{16}$ with
  \[ H = \begin{pmatrix} 5 & 4 & 3 & 2 & 1 & 0 \\ 12 & 6 & 3 & 5 & 0 & 1 \end{pmatrix} \]

- [8, 6] code over $\mathbb{Z}_{16}$ with
  \[ H = \begin{pmatrix} 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 7 & 0 & 12 & 6 & 3 & 5 & 0 & 1 \end{pmatrix} \]

- [8, 6] code over $\mathbb{Z}_{17}$ with
  \[ H = \begin{pmatrix} 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 7 & 0 & 12 & 6 & 3 & 5 & 0 & 1 \end{pmatrix} \]
Decoding

Let a sequence of signal points, $s_{i_1j_1}, s_{i_2j_2}, \ldots, s_{i_nj_n}$, be sent through the channel. In the coded case $(i_1, i_2, \ldots, i_n)$ and $(j_1, j_2, \ldots, j_n)$ are codewords. At the receiver the decoder based on the received signal sequence $r_{i_1j_1}, r_{i_2j_2}, \ldots, r_{i_nj_n}$, outputs a sequence of signal points $s'_{i_1j_1}, s'_{i_2j_2}, \ldots, s'_{i_nj_n}$. Let $q_u$ and $q_b$ be the probabilities for correct demodulations in uncoded and coded cases respectively.

\[
q_u = \frac{(1 + 15 \text{erf}(\gamma))^2}{256}, \\
q_c = \frac{(3 + 13 \text{erf}(3\gamma))}{256},
\]

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

\[
P_{SE}(C) = \frac{1}{n} \left( 1 - q_u^n - nq_u^{n-1}q_c - \binom{n}{2} q_u^{n-2}q_c^2 \right)
\]
Decoding

- **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.
Simulation results

![Graph showing BER vs. Es/No for 256-QAM: Grey, hard, and mixed decoding.]

**Figure:** 256-QAM: Grey, hard, and mixed decoding [6, 4] code over $\mathbb{Z}_{16}$. 
Simulation results

Figure: 256-QAM: $[8, 6]$ code over $\mathbb{Z}_{19}$. 
Simulation results

Figure: 256-QAM: [8, 6] code over $\mathbb{Z}_{19}$. 
Simulation results

![Graph showing simulation results for different code alternatives including uncoded, theoretical (Theor), hard (ICHard), soft (ICSoft), and TCM128state, with probability of bit error plotted against Eb/No (dB).]
Conclusions

- Simple realization and good performance
- Can be used as an inner code in cascading schemes
- Further research on their performance when are used in combinations with other coding schemes
THANK YOU
FOR ATTENTION