ON (± 1) ERROR CORRECTABLE INTEGER CODES

Hristo Kostadinov, Nikolai Manev, Hiroyoshi Morita

Institute of Mathematics and Informatics, Sofia, Bulgaria
University of Electro-Communications, Tokyo, Japan

06.09.2010

OUTLINE OF THE TALK

1. CONTENTS

2. INTRODUCTION

3. MAIN RESULT

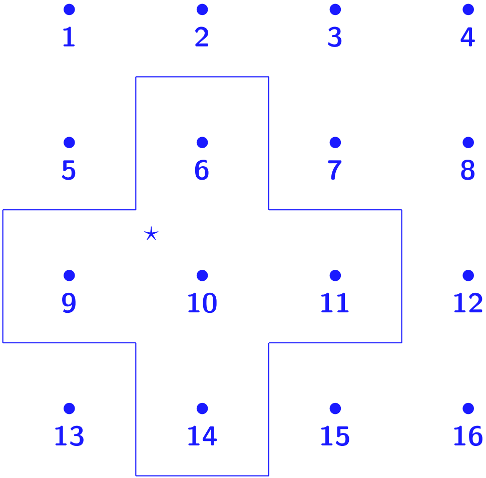
4. APPLICATION OF (± 1) ERROR CORRECTABLE INTEGER CODES

5. CONCLUSION REMARKS AND FUTURE WORK

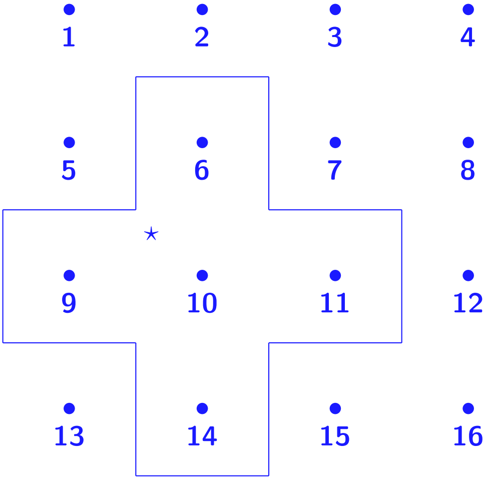
INTRODUCTION

It is well known that the beautiful algebraic theory of block codes over finite fields does have severe problems with coding for two dimensional constellation.

Huber introduced the Manheim distance and proposed block codes over Gaussian integers designed for that distance. One problem which arises when we use this code construction is that based on given code we arrange the signal points in a signal constellation.



Manheim distance 1 in 16-QAM constellation



Manheim distance 1 in 16-QAM constellation

Integer codes are codes defined over finite rings of integers. The original form of integer codes have been given by R. Varshamov and Tenengolz (1965) where an integer code to correct a single insertion/deletion error per codeword was described.

The main advantage of integer codes, over the block codes, is that we can correct errors of a given type, which means that for a given channel and modulator we can choose the type of the errors (which are the most common) and after that construct integer code capable of correcting those errors.

V. Levenstein and A. Han Vinck (1993) showed one possible application of Integer codes for magnetic recording.

A. Han Vinck, H. Morita (1998) investigated Integer codes with a view to frame synchronization and coded modulation.

H. Kostadinov, H. Morita and N. Manev (2003) used Integer codes for QAM modulation scheme.

Similar results but using different approach and coding technique:

Nakamura proposed single and double Lee-error correctable block codes designed for PSK and QAM channels. His construction of single Lee-error correctable code is equivalent to a construction of (± 1) single error correctable integer code.

Huber and Rifa presented a construction of single error correctable block codes over Gaussian integers and using Manheim distance for QAM constellations. In case of Manheim distance equal to 1 it is equivalent to a construction of single error ("cross type") correctable integer code.

MAIN RESULT

Definition 1. Let $\mathbb{Z}_A$ be the ring of integers modulo A. An *integer code* of length n with check matrix $H \in \mathbb{Z}_A^{m\times n}$, is referred to as a subset of $\mathbb{Z}_A^n$, defined by

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

where $\boldsymbol{d} \in \mathbb{Z}_A^m$.

Without loss of generality we shall assume that $\boldsymbol{d} = \boldsymbol{0} \in \mathbb{Z}_A^m$

Definition 2. The code $\mathcal{C}(\boldsymbol{H}, \boldsymbol{d})$ is said to be a t-$(\pm e_1, \pm e_2, \ldots, \pm e_s)$ *error correctable* if it can correct up to t errors with values $\pm e_i$, $i = 1, \ldots, s$.

Definition 3. A single $(\pm e_1, \pm e_2, \ldots, \pm e_s)$-error correctable code $\mathcal{C}(\boldsymbol{H}, \boldsymbol{d})$ of block length n is called *perfect*, when $A = 2sn + 1$.

An integer code is called *quasi-perfect* if $A \geq 2sn + 1$ is the smallest value of A for which an integer code exists.

Example 1: $(\pm 1, \pm 3, \pm 4, \pm 5)$ single error correcting code of length $n = 2$ over $\mathbb{Z}_{17}$ has a check matrix

$$H = (1, 2).$$

$$\begin{aligned}\mathcal{C}(H, \boldsymbol{0}) = \{&(0,0),(1,8),(2,16),(3,7),(4,15),(5,6),\\ &(6,14),(7,5),(8,13),(9,4),(10,12),(11,3),\\ &(12,11),(13,2),(14,10),(15,1),(16,9)\}\end{aligned}$$

α	error vector	
1	1	0
2	0	1
3	3	0
4	4	0
5	5	0
6	0	3
7	0	-5
8	0	4
9	0	-4
10	0	5
11	0	-3
12	-5	0
13	-4	0
14	-3	0
15	0	-1
16	-1	0

Table 1. Syndrome table for $(\pm 1, \pm 3, \pm 4, \pm 5)$ single-error correctable integer code of length 2 over Z_{17}.

Theorem 1. 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

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

where $m > 1$ is defined by

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

and every column $\boldsymbol{h}_i \in \boldsymbol{S}^1 \cup \boldsymbol{S}^2$, where

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

and

$$\begin{gathered} \boldsymbol{S}^2 = \{(s_1, s_2, \ldots, s_m)^\tau \ \mid s_1 \in \{0, 2^{l-1}\}, \\ s_i \in \mathbb{Z}_{2^{l-1}+1}, i = 2, \ldots, m, \\ \text{and at least for one } i : s_i \in \mathbb{Z}^\star_{2^{l-1}}\}. \end{gathered}$$

Remark 1. When $m = 1$ a construction of integer codes was given by Varshamov and Tenengolz.

Remark 2. We use the lower bound for n to obtain the highest possible rate of the integer code of length n.

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

APPLICATION OF (± 1) ERROR CORRECTABLE INTEGER CODES

We encode a A^2-QAM constellation using a product code integer code $\mathcal{C}(\boldsymbol{H}, \boldsymbol{0}) \times \mathcal{C}(\boldsymbol{H}, \boldsymbol{0})$ over $\mathbb{Z}_A \times \mathbb{Z}_A$. In such a case we can correct "square" type of error. For decoding the integer codes we use soft decoding algorithm

In the following examples we assume that our communication channel is AWGN.

Example 2. (64-QAM constellation) Let us consider the following integer codes over $\mathbb{Z}_8$:

• Single (± 1) error correctable integer code $\mathcal{C}_1(\boldsymbol{H}_1, \boldsymbol{0})$, using Theorem 1, of length $n = 4$ with a check matrix

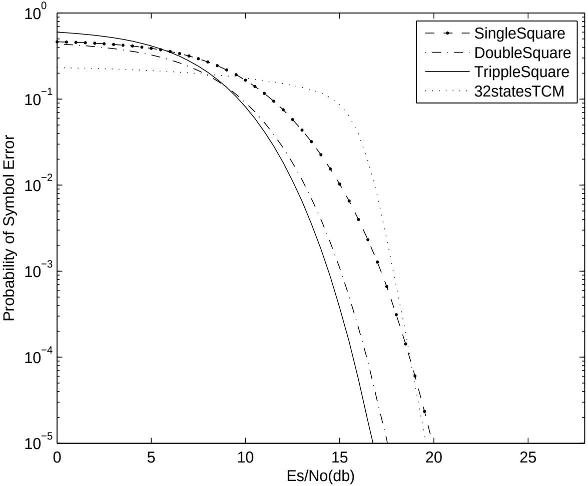
$$\boldsymbol{H}_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix}$$

• Double (± 1) error correctable integer code $\mathcal{C}_2(\boldsymbol{H}_2, \boldsymbol{0})$ of length $n = 4$ with a check matrix

$$\boldsymbol{H}_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 1 & 0 & 2 \end{pmatrix}$$

• 3-error (± 1) correctable Integer code $\mathcal{C}_3(\boldsymbol{H}_3, \boldsymbol{0})$ of length $n = 4$ with a check matrix

$$\boldsymbol{H}_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 \\ 6 & 2 & 1 & 4 \end{pmatrix}$$



SingleSquare
DoubleSquare
TrippleSquare
32statesTCM
Probability of Symbol Error
Es/No(db)
10^{0}
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
0
5
10
15
20
25

Example 3. (256-QAM constellation) In a similar way as in the previous example let us consider the following integer codes over $\mathbb{Z}_{16}$:

- Single (± 1) error correctable integer code $\mathcal{C}_4(\boldsymbol{H}_4, \boldsymbol{0})$, using Theorem 1, of length $n = 30$ with a check matrix

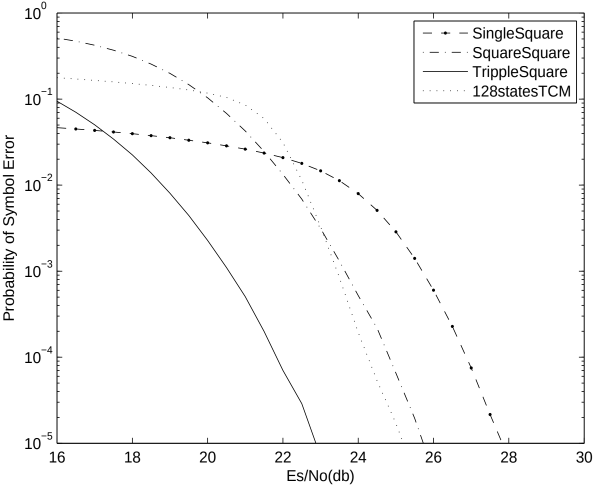
$$\boldsymbol{H}_4 = \begin{pmatrix} 1\ldots & 1 & 2\ldots & 2 & 3\ldots & 3 & 0\ldots & 0 & 4\ldots & 4 \\ 0\ldots & 7 & 0\ldots & 7 & 0\ldots & 7 & 1\ldots & 3 & 1\ldots & 3 \end{pmatrix}$$

- Double (± 1) error correctable integer code $\mathcal{C}_5(\boldsymbol{H}_5, \boldsymbol{0})$ of length $n = 8$ with a check matrix

$$\boldsymbol{H}_5 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 1 & 8 & 0 & 6 \end{pmatrix}$$

- 3-error (± 1) correctable Integer code $\mathcal{C}_6(\boldsymbol{H}_6, \boldsymbol{0})$ of length $n = 5$ with a check matrix

$$\boldsymbol{H}_6 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 3 & 8 \end{pmatrix}$$



SingleSquare
SquareSquare
TrippleSquare
128statesTCM
Probability of Symbol Error
Es/No(db)
10^0
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
16
18
20
22
24
26
28
30

CONCLUSION REMARKS AND FUTURE WORKS

Integer codes are codes defined over finite rings of integers. The advantage of integer codes is that we can choose a type of the error(s) and after that construct an integer code capable of correcting that error(s).

Because of their flexibility Integer codes can be applied in all the types of modulation schemes which are used in digital communications.

We showed that for any given l and n there exists an (± 1) single error correctable integer code of length n over $\mathbb{Z}_{2^l}$.

In case of AWGN channel and QAM schemes a comparison of symbol error probability between integer codes and TCM shows us that integer codes have better performance

The usage of integer codes capable of correcting more than one error makes it possible to improve the performance, but increases the complexity.

A construction of an integer code capable of correcting multiple errors of given type(s) is much more complicated. Even in case of (± 1) double error correcting code is difficult to define the exact form of the check matrix.

Another direction of our future research is to apply integer codes in watermarking, steganography and fading channels.

THANK YOU FOR YOUR ATTENTION