IEICE TRANS. FUNDAMENTALS, VOL.E93–A, NO.12 DECEMBER 2010

LETTER

On (±1) Error Correctable Integer Codes*

Hristo KOSTADINOV†, *Nonmember*, **Hiroyoshi MORITA**†a), *Senior Member*, *and* **Nikolai MANEV**††, *Nonmember*

SUMMARY Integer codes correct errors of a given type, which means that for a given communication channel and modulator we can choose the type of the errors (which are the most common) then construct integer code capable of correcting those errors. A new general construction of single (±1) error correctable integer codes will be presented. Comparison between single and multiple (±1) error correctable integer codes over AWGN channel using QAM scheme will be presented.

key words: *integer codes, finite rings, QAM, AWGN*

1. Introduction

Codes over finite rings and in particular codes over finite rings of integers with their applications in coding theory have been studied in numerous papers. The earliest paper is due to I. Blake [1], [2]. Some other works on codes over $\mathbb{Z}_A$ are [3]–[5]. M. Nilsson [6] discusses linear block codes over integer rings in order to improve the performance of PSK communication systems.

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. This is mainly due to the fact that in two (or higher) dimensions the usual Hamming distance is inappropriate. To improve the situation Huber [7] 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.

Rifa [8] investigated single error correctable block codes over Gaussian integers. In his construction, the codewords are sequences of elements that belong to group structures of Gaussian integers. These codes are neither group nor linear over a field, so it is not possible to use the standard techniques in these cases. There is no efficient decoding algorithm for these codes.

Integer codes are codes defined over finite rings of integers. The original form of integer codes have been found in [9] where an integer code to correct a single insertion/deletion error per codeword was described. A. Han Vinck and H. Morita [10] investigated integer codes with a view to frame synchronization and coded modulation.

The advantage of integer codes, over the conventional block codes, is that we can correct errors of a given type, which means that for a given communication 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.

Similar to integer codes are the block codes over Gaussian integers [7], [8], discussed above, and a class of error correcting codes based on Lee distance [11]. Actually, single (±1) error correctable integer codes and single Lee-error correcting codes, proposed by Nakamura, are equivalent. Nakamura showed that with his construction, we are able to obtain very high code rate and he applied them for differentially encoded PSK and QAM channel models [12]. Using his approach it is not possible to obtain single Lee-error codes of every desired code length. That motivated us to try to obtain single (±1) error correctable code for any code length.

Here, in this article, we are going to present a new general construction of integer codes capable of correcting single error of type (±1). We shall show a comparison of symbol error probability (SER) versus signal-to-noise ratio (SNR) of different (±1) single/multiple error correctable integer codes using QAM modulation scheme and AWGN channel and TCM [13].

In Sect. 2 we give necessary definitions. A new general construction of single (±1) error correcting integer codes will be presented in Sect. 3. In Sect. 4 we shall discuss an application of (±1) error correctable integer codes to QAM schemes in case of AWGN channel. Conclusion remarks are given in Sect. 5.

2. Notations and Definitions

Definition 1. [10] Let $\mathbb{Z}_A$ be the ring of integers modulo A. An *integer code* of length n with check matrix $\boldsymbol{H} \in \mathbb{Z}_A^{m\times n}$, is referred to as a subset of $\mathbb{Z}_A^n$, defined by

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

where $\boldsymbol{d} \in \mathbb{Z}_A^m$ and $\boldsymbol{H}^T$ is the transpose of $\boldsymbol{H}$.

Without loss of generality we shall assume that $\boldsymbol{d}$ =

Manuscript received November 5, 2009.
Manuscript revised May 5, 2010.

†The authors are with the Graduate School of Information Systems, University of Electro-Communications, Chofu-shi, 182-8585 Japan.
††The author is with Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 8 Acad. G Bonchev Str., 1113 Sofia, Bulgaria.

*Part of this results were presented at ISITA 2008, Auckland, New Zealand.

a) E-mail: morita@is.uec.ac.jp

DOI: 10.1587/transfun.E93.A.2758

$\boldsymbol{0} \in \mathbb{Z}_A^m$.

Suppose that a signal point s_i is sent through a communication channel. At the other end the detector estimates the received signal r_i and gives signal point s_j at the output. If $j \neq i$ the detector has taken a wrong decision. In terms of block codes over $\mathbb{Z}_A$ the aforesaid can be described in the following way. When a codeword $\boldsymbol{c} \in C(\boldsymbol{H}, \boldsymbol{d})$ is sent through a noisy channel the received vector can be written in the form

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

where $\boldsymbol{e} = (e_1, \ldots, e_n) \in \mathbb{Z}_A^n$ denotes the error vector. It is clear that the different signal points do not have the same chance to be a result of decision process. The probability signal point s_j to appear at the output of the detector depends on the Euclidean distance between s_j and really-sent signal s_i.

In terms of codes over $\mathbb{Z}_A$ it means that the elements of $\mathbb{Z}_A$ are not equally probable as a value taken by e_i. A way of indexing the signal points by elements of $\mathbb{Z}_A$ affects which elements of $\mathbb{Z}_A$ are more probable. Therefore, it makes sense to consider the next definition.

Definition 2. The code $C(\boldsymbol{H}, \boldsymbol{d})$ 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 $\pm e_i$, $i = 1, \ldots, s$.

Using Definition 2, one can easily derive the following bound for A.

Proposition 1.[10] If $C(\boldsymbol{H}, \boldsymbol{d})$ corrects t errors of type $(\pm e_1, \pm e_2, \ldots, \pm e_s)$ then the cardinality A of the ring satisfies the inequality

$$A^m \geq \sum_{i=0}^{t} \binom{n}{i} (2s)^i, \tag{1}$$

where n is the length of the code and m is the number of rows of $\boldsymbol{H}$.

Hence, taking into account (1) we have the following definition:

Definition 3. A t-$(\pm e_1, \pm e_2, \ldots, \pm e_s)$ error correctable code $C(\boldsymbol{H}, \boldsymbol{d})$ of block length n is called *perfect*, when we have equality in (1).

We notice that if an integer code is perfect there is a one-to-one correspondence between $\mathbb{Z}_A^m$ and the set of all possible error vectors. When the code is not perfect we do not have such a correspondence for some of the elements of $\mathbb{Z}_A^m$. Even if the syndrome value is one of those elements, we can say that at least an error(s) which is not of the type $(\pm e_1, \pm e_2, \ldots, \pm e_s)$ appears.

3. General Construction of Single (±1) Error Correcting Integer Codes

The definition of a t-$(\pm e_1, \pm e_2, \ldots, \pm e_s)$ error correctable integer codes shows us that to construct such a code of length n over $\mathbb{Z}_A^n$, with a check matrix $\boldsymbol{H}^{m \times n}$ is a task which is equivalent to splitting $\mathbb{Z}_A^n$ into pairwise disjoint subsets.

As we mentioned above, integer codes correcting single (±1) error are equivalent to single Lee-error correcting codes proposed by Nakamura [11], [12]. In his construction Nakamura uses a similar idea of splitting $\mathbb{Z}_A^n$ into pairwise disjoint subsets, but using polynomials. Using his method, it is not possible always to find a polynomial of a desire degree, i.e., there does not exist a single Lee-error correcting code with check matrix $\boldsymbol{H}^{m \times n}$ for any n and m. That motivated us to extend his results using integer codes. In the next theorem we shall present a construction of single (±1) error correctable integer codes for any code length n and dimension m.

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

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

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

$$\boldsymbol{S}^1 = \{(s_1, s_2, \ldots, s_m)^T \mid s_1 \in \mathbb{Z}_{2^{l-1}}^*, \\ s_i \in \mathbb{Z}_{2^{l-1}}, i = 2, \ldots, m\}, \tag{3}$$

and

$$\boldsymbol{S}^2 = \{(s_1, s_2, \ldots, s_m)^T \mid s_1 \in \{0, 2^{l-1}\}, \\ s_i \in \mathbb{Z}_{2^{l-1}+1}, i = 2, \ldots, m, \\ \text{and at least for one } i : s_i \in \mathbb{Z}_{2^{l-1}}^*\}. \tag{4}$$

(As usual, $\mathbb{Z}_A^*$ denotes the subset of invertible elements of $\mathbb{Z}_A$, i.e., the elements coprime with A.)

Proof: To prove the theorem it is enough to show that the vectors $\boldsymbol{s} = \boldsymbol{e}\boldsymbol{H} \in \mathbb{Z}_{2^l}^m$ are pairwise disjoint, where $\boldsymbol{e} = (0, \ldots, 0, e_i, 0, \ldots, 0), e_i \in \{-1, 1\}, 1 \leq i \leq n$. This is equivalent to prove that $\pm\boldsymbol{S}^1 \cap \pm\boldsymbol{S}^2 = \emptyset, \boldsymbol{S}^1 \cap (-\boldsymbol{S}^1) = \emptyset$ and $\boldsymbol{S}^2 \cap (-\boldsymbol{S}^2) = \emptyset$, where $-\boldsymbol{S}$ is the set obtained after multiplications of elements of $\boldsymbol{S}$ by -1.

Let us look at the first coordinate of the vector $\boldsymbol{s} = (s_1, s_2, \ldots, s_m)$. If $s_1 \in \{0, 2^{l-1}\}$ then $\boldsymbol{s} \notin \boldsymbol{S}^1$ and $\boldsymbol{s} \notin (-\boldsymbol{S}^1)$. In this case $\boldsymbol{s} \in \boldsymbol{S}^2$ or $\boldsymbol{s} \in (-\boldsymbol{S}^2)$. That is, $\boldsymbol{S}^1 \cap \boldsymbol{S}^2 = \boldsymbol{S}^1 \cap -\boldsymbol{S}^2 = -\boldsymbol{S}^1 \cap \boldsymbol{S}^2 = -\boldsymbol{S}^1 \cap -\boldsymbol{S}^2 = \emptyset$.

If $s_1 \in \mathbb{Z}_{2^{l-1}}^{\star}$ then $\boldsymbol{s} \in \boldsymbol{S}^1$ and $\boldsymbol{s} \notin (-\boldsymbol{S}^1)$ because $-s_1 \in \{2^{l-1}+1, 2^{l-1}+2, \ldots, 2^l - 1\}$. So we obtain that $\boldsymbol{S}^1 \cap (-\boldsymbol{S}^1) = \emptyset$.

In a similar way we can prove that $\boldsymbol{S}^2 \cap (-\boldsymbol{S}^2) = \emptyset$. Here we have that in $\boldsymbol{s}$ at least one component, s_i is in $\mathbb{Z}_{2^{l-1}}^{\star}$. Then using the same arguments as above it follows that if $\boldsymbol{s} \in \boldsymbol{S}^2$ then $\boldsymbol{s} \notin (-\boldsymbol{S}^2)$ with which the proof is completed. □

Remark 1. When $m = 1$ a construction of integer codes was given by Varshamov and Tenengolz [9].

Remark 2. In (2) we use the lower bound for n to obtain the highest possible rate of the integer code of length n.

Table 1 Exact form of the check matrix $\boldsymbol{H}$ for some values of n using the construction of Theorem 1, where $l = 3$ and $m = 2$.

n	$\boldsymbol{H}$
4	$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix}$
7	$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$
12	$\begin{pmatrix} 0 & 1 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 1 & 0 & 0 & 1 & 2 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$
18	$\begin{pmatrix} 0 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 4 & \dots & 4 \\ 1 & 0 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 4 & 0 & \dots & 7 \end{pmatrix}$
25	$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 \dots 2 & 3 \dots 3 \\ 1 & 0 & 2 & 3 & 4 & 5 & 6 & 7 & 0 \dots 7 & 0 \dots 7 \end{pmatrix}$
30	$\begin{pmatrix} 1 \dots 1 & 2 \dots 2 & 3 \dots 3 & 0 & 0 & 0 & 4 & 4 & 4 \\ 0 \dots 7 & 0 \dots 7 & 0 \dots 7 & 1 & 2 & 3 & 1 & 2 & 3 \end{pmatrix}$

Note that the set $\boldsymbol{S}^1 \cup \boldsymbol{S}^2$ contains all possible vectors we can use to construct a check matrix. Hence, we have the next result, as a corollary of Theorem 1.

Corollary 3.1. 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 $n = 2^{ml-1} - 2^{m-1}$. □

Table 1 shows check matrices of single (±1) error correcting integer codes for some values of n using Theorem 1. When $l = 2$ and $m = 3$ we obtain that $3 < n \leq 30$. One easily see that using the last check matrix in Table 1 we can obtain the others. Actually, we have a freedom to chose from any of those 30 vector columns to construct the check matrices of length $n < 30$.

4. Application of (±1) Error Correctable Integer Codes to QAM Scheme in AWGN Channel

Before starting the discussion about the application of integer codes in coded modulations let us first say something more for multiple error correcting integer codes.

In the definition of integer codes we do not specify the check matrix $\boldsymbol{H}^{m\times n}$. It is rather difficult to be found the exact form of the check matrix, even for relatively small values of m and n. One construction of the check matrix when $m = 2$, i.e., for double (±1) error correctable integer code is given in [14].

Let $C(\boldsymbol{H}, \boldsymbol{d})$ be a t-error correctable integer code over $\mathbb{Z}_A$ with an $m \times n$ check matrix $\boldsymbol{H} = (\boldsymbol{h}_1, \boldsymbol{h}_2, \dots, \boldsymbol{h}_i, \dots, \boldsymbol{h}_n)$. The condition $C(\boldsymbol{H}, \boldsymbol{d})$ is t − (±1) error correctable code means that the set

$$\{\pm\boldsymbol{h}_{i_1}, \pm(\boldsymbol{h}_{i_1} \pm \boldsymbol{h}_{i_2}), \pm(\boldsymbol{h}_{i_1} \pm \boldsymbol{h}_{i_2} \pm \boldsymbol{h}_{i_3}), \dots,$$
$$\pm(\boldsymbol{h}_{i_1} \pm \boldsymbol{h}_{i_2} \pm \boldsymbol{h}_{i_3} \pm, \dots, \pm\boldsymbol{h}_{i_t}), i_1 \neq i_2 \neq \dots \neq i_t\},$$

where $1 \leq i_j \leq n$, consists of different (there is no repeating) vector-columns.

Multiple error correcting integer codes are beyond the scope this paper. Below we give few examples of multiple error correcting codes for comparison with single error correctable codes based on the symbol error rate (SER) versus signal-to-noise ratio (SNR) for AWGN channel and QAM scheme.

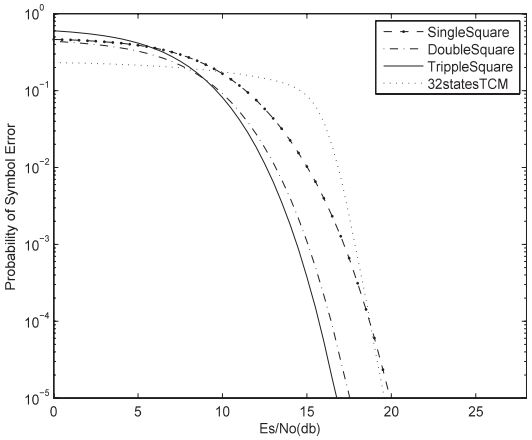

Fig. 1 A comparison of symbol error probability versus signal-to-noise ratio between coded 64-QAM with the integer codes from example 1 using soft decoding algorithms and 32 state TCM.

Example 1. (64-QAM constellation) Let us consider the following integer codes over $\mathbb{Z}_8$:

• Single (±1) error correctable integer code $C_1(\boldsymbol{H}_1, \boldsymbol{0})$, 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 $C_2(\boldsymbol{H}_2, \boldsymbol{0})$ 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 $C_3(\boldsymbol{H}_3, \boldsymbol{0})$ of length $n = 4$ with a check matrix

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

We encode a 64-QAM constellation using a product code $C_i(\boldsymbol{H}_i, \boldsymbol{0}) \times C_i(\boldsymbol{H}_i, \boldsymbol{0})$ over $\mathbb{Z}_8 \times \mathbb{Z}_8$. In such a case we can correct "square" type of error. For decoding the integer codes we use soft decoding algorithm [15]. □

The comparison of symbol error probability (based on information symbol) of these 3 codes and 32 state TCM [13] is given on Fig. 1. Surprisingly, at high SNR single (±1) integer code has same SER as TCM. We can gain about 2 and 3 dB using double and triple error correctable integer code respectively.

Example 2. (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 $C_4(\boldsymbol{H}_4, \boldsymbol{0})$, using Theorem 1, of length $n = 30$ with a check matrix

$$\boldsymbol{H}_4 = \begin{pmatrix} 1\dots1 & 2\dots2 & 3\dots3 & 0\dots0 & 4\dots4 \\ 0\dots7 & 0\dots7 & 0\dots7 & 1\dots3 & 1\dots3 \end{pmatrix}$$

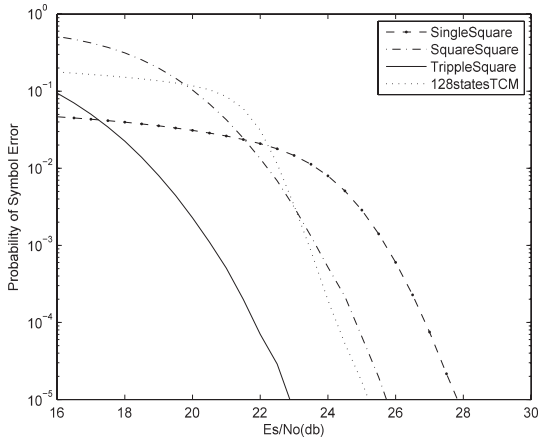

Fig. 2 A comparison of symbol error probability versus signal-to-noise ratio between uncoded and coded 256-QAM - with the integer codes from example 2 using soft decoding algorithms and 128 state TCM.

• Double (±1) error correctable integer code $C_5(\boldsymbol{H}_5, \boldsymbol{0})$ 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 $C_6(\boldsymbol{H}_6, \boldsymbol{0})$ of length $n = 5$ with a check matrix

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

The encoding and decoding procedures of 256-QAM are the same as for 64-QAM. □

In Fig. 2 is shown the symbol error probability (per information symbol) versus SNR of the codes $C_4(\boldsymbol{H}_4, \boldsymbol{0})$, $C_5(\boldsymbol{H}_5, \boldsymbol{0})$, $C_6(\boldsymbol{H}_6, \boldsymbol{0})$ and 128 state TCM [13]. The situation is similar as in the previous example. The difference is that TCM has better performance than (±1) error correcting integer code.

5. Conclusions

In this paper we presented a new general construction of single (±1) error correcting integer codes. We compared the symbol error probability of these codes with multiple (±1) integers codes and with TCM. The simulation results confirmed our expectations concerning the performance of (±1) integers codes. These codes possess a relatively simple structure, flexibility of code length and low complexity of the decoding algorithms. The hard decoding is with a linear complexity, and the soft decoding is equivalent to the Viterbi algorithm (see for details [14] and [15]). The integer codes can be suitable for real application in the communication systems. Their usage for correcting more than one error improves the performance with the price of slightly increasing the decoding complexity.

Acknowledgement

This work was partially supported by "FY2007 Japan Society for the Promotional Science (JSPS) Postdoctoral Fellowship for Foreign Researchers."

References

[1] I. Blake, "Codes over certain rings," Information and Control, vol.20, pp.396–404, 1972.
[2] I. Blake, "Codes over integer residue rings," Information and Control, vol.29, pp.295–300, 1975.
[3] A.R. Calderbank and N.J.A. Sloane, "Modular and $p-$adic cyclic codes," Des. Codes Cryptogr., vol.6, no.1, pp.21–36, 1995.
[4] E. Spiegel, "Codes over Z_m," Information and Control, vol.35, pp.48–51, 1977.
[5] V.I. Levenstein and A.J. Han Vink, "Perfect (d, k) — Codes capable of correcting single peak-shifts," IEEE Trans. Inf. Theory, vol.39, no.2, pp.656–662, 1993.
[6] M. Nilsson, Linear block codes over rings for phase shift keying, Thesis no.331, Linköping University, 1993.
[7] K. Huber, "Codes over Gaussian integers," IEEE Trans. Inf. Theory, vol.40, no.1, pp.207–216, Jan. 1994.
[8] J. Rifa, "Groups of complex integers used as QAM signals," IEEE Trans. Inf. Theory, vol.41, no.5, pp.1512–1517, Sept. 1995.
[9] R.R. Varshamov and G.M. Tenengolz, "One asymmetrical error-correctable codes," (in Russian) Avtomatika i Telematika, vol.26, no.2, pp.288–292, 1965.
[10] A.J. Han Vinck and H. Morita, "Codes over the ring of integer modulo m," IEICE Trans. Fundamentals, vol.E81-A, no.10, pp.2013–2018, Oct. 1998.
[11] K. Nakamura, "A class of error correcting codes for DPSK channels," Proc. International Conference on Communications (ICC'79), pp.45.4.1–45.4.5, 1979.
[12] K. Nakamura, "Error correcting scheme for differentially encoded M-ary quadrature amplitude modulation system," Proc. Symposium on Information Theory and its Applications (SITA), pp.44–52, 1982.
[13] G. Ungerboeck, "Trellis-coded modulation with redundant signal sets," IEEE Commun. Mag., vol.25, no.2, pp.5–21, Feb. 1987.
[14] H. Kostadinov, H. Morita, and N. Manev, "On ±1-error correctable integer residue codes," Proc. International Workshop on Optimal Codes and Related Topics, pp.117–124, June 2009.
[15] H. Morita, A.J. Han Vink, and H. Kostadinov, "On soft decoding of coded QAM using integer codes," International Symposium on Information Theory and its Applications (ISITA), pp.1321–1325, Parma, Italy, Oct. 2004.