PAPER

Soft Decoding Of Integer Codes and Their Application to Coded Modulation*

Hristo KOSTADINOV[†], *Nonmember*, **Hiroyoshi MORITA**[†a)], ***Regular Member***, **Noboru IIJIMA**[†], **A. J. HAN VINCK**[††], ***and*** **Nikolai MANEV**[†††], ***Nonmembers***

SUMMARY Integer codes are very flexible and can be applied in different modulation schemes. A soft decoding algorithm for integer codes will be introduced. Comparison of symbol error probability (SEP) versus signal-to-noise ratio (SNR) between soft and hard decoding using integer coded modulation shows us that we can obtain at least 2 dB coding gain. Also, we shall compare our results with trellis coded modulation (TCM) because of their similar decoding schemes and complexity.

key words: *Finite rings, Integer codes, Coded modulation, QAM, PSK, AWGN, SEP.*

1. Introduction

Coded modulation is an efficiently combined scheme of coding and modulation techniques. It has been investigated extensively by Ungerboeck [1], [2], Imai and Hirakawa [3] and others. In 1982, Ungerboeck constructed a trellis code that maps the input sequence into signal points of a fixed signal constellation by a method referred to as *set partitioning*. This method is called trellis coded modulation (TCM). An alternative which allows us to deal with a variety of constellations is block coded modulation [4], [5]. In block coded modulation, each point of the signal constellation corresponds to a symbol of a finite ring of integers modulo A denoted by $\mathbb{Z}_A$. An information sequence is mapped into a sequence of symbols in $\mathbb{Z}_A$ and coded by a code over $\mathbb{Z}_A$.

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 works were given by I. Blake [6], [7]. Some other works on codes over $\mathbb{Z}_A$ are [8]–[10]. M. Nilsson [11] discusses linear block codes over integer rings in order to improve the performance of PSK communication systems.

[†]The Graduate School of Information Systems, University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo 182-8585, Japan.

[†]The Graduate School of Information Systems, University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo 182-8585, Japan.

[††]Institute of Experimental Mathematics, University of Essen, Ellernstr. 29, 4532 Essen, Germany.

[†††]Institute of Mathematics and Informatics, Bulgarian Academy of Sciences , 8 Acad. G Bonchev Str., 1113 Sofia, Bulgaria.

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

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

One class of block codes, which we investigate in this paper, is so called integer codes. The original form of integer codes have been found in [12] where an integer code to correct a single insertion/deletion error per codeword was described. A. Han Vinck and H. Morita [5], A. Geyser and H. Morita [13] investigated these codes with a view to frame synchronization and coded modulation.

Integer codes are codes defined over finite rings of integers. Their advantage over the traditional block codes is that integer codes are capable of correcting limited number of error patterns which occur most frequently while the conventional codes intend to correct all possible error patterns. Definitions of ”cross”, ”square” and ”big square” type of errors can be found in [14]. Similar to integer codes are codes over Gaussian integers [15], [16] designed for the Mannheim distance and a class of error correcting codes based on the Lee distance given in [17]. The latter codes have very high code rate and have been applied by Nakamura for differentially encoded PSK and QAM channel models [18]. The codes over Gaussian integers with the Mannheim distance 1 can correct error(s) of type ”cross”, while using single Lee-error correcting codes we are able to correct a ”square” type of error on the QAM constellation, where a signal point can be represented as a pair of symbols (a_i, b_i) of two single Lee-error codewords $\boldsymbol{a} = (a_1, a_2 \ldots, a_n)$ and $\boldsymbol{b} = (b_1, b_2 \ldots, b_n)$. Those are the only two cases in which other codes can correct exactly the same type of error(s) as integer codes do.

The aim of this paper is to show the flexibility of integer codes and their application to different modulation schemes for decreasing probability of symbol error over an Additive White Gaussian Noise (AWGN) channel. The integer codes have low encoding and decoding complexity and they will be suitable for application in real communication systems.

We are going to introduce a new upper bound for symbol error probability (SEP) in an AWGN channel for square types of QAM constellations coded independently on the in-phase and the quadrature components by integer codes. Moreover, for improving the performance of SEP of integer codes over an AWGN, we shall present a soft decoding algorithm.

In our algorithm we use a trellis whose states represent all possible syndrome values of the applied integer code. The idea of the trellis structure comes from Jack Wolf's work [19], where is given a decoding algorithm for linear block codes using a trellis. In the soft decoding algorithm, as well as in TCM, the core part is the Viterbi algorithm. Hence, the proposed soft decoding algorithm has a linear complexity. We compare our results with TCM because they are very well known and are widely applied in telephone modems, satellite and terrestrial wireless systems, as well as in digital audio and TV broadcasting. The examples of integer codes which are given in this paper are chosen in such a way that a fair comparison between them and TCM [2] can be demonstrated. Because of that we shall also compare the performance of the codes based on the probability of symbol error versus signal-to-noise ration (for energy per symbol) instead of probability of bit error versus signal-to-noise ratio (for energy per bit).

As we shall see later, using integer codes with the introduced soft decoding algorithm, we can gain approximately 2 dB over the hard decoding. Compared to TCM, integer codes with soft decoding have almost same symbol error rate for a given value of SNR.

The paper is organized as follows. In Section 2 we give the necessary definitions and several construction of integer codes. A new theoretical upper bound for SEP will be introduced in Section 3. A soft decoding algorithm will be presented in Section 4. To illustrate the advantage of using it we are going to compare it with a hard decoding algorithm of integer codes and TCM. In Section 5 will be given conclusion remarks.

2. Necessary Definitions and Constructions of Integer Codes

Herein we give some necessary definitions and several constructions of integer codes which we shall use in the next section. The reader can find more details in the cited papers.

Definition 2.1. [5] Let $\mathbb{Z}_A$ be the ring of integers modulo A. An *integer code* of length n with parity-check matrix $H \in \mathbb{Z}_A^{m\times n}$, is referred to as a subset of $\mathbb{Z}_A^n$, defined by

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

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

Assume that a signal point s_i is sent through an AWGN-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 $\mathbf{c}\in\mathcal{C}(\mathbf{w},d)$ 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. It is clear that the different signal points have not 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. Which elements of $\mathbb{Z}_A$ are more probable depends on the chosen indexing of the signal points by the elements of $\mathbb{Z}_A$. Therefore, there is a point in considering the next definition.

Definition 2.2 The code $\mathcal{C}(H,\boldsymbol{d})$ is a t-multiple $(\pm e_1,\pm e_2,\ldots,\pm e_s)$-error correctable if it can correct up to t errors with values from the set $\{\pm e_1,\pm e_2,\ldots,\pm e_s\}$ which occur in a codeword. □

Remark: Without loss of generality in the definitions above we can assume that $\boldsymbol{d}=\boldsymbol{0}$. For convenience of a notation we shall use $\mathcal{C}$ instead of $\mathcal{C}(H,\boldsymbol{0})$.

The following general construction of single error correctable integer code can be found in [20].

Let $G=\{1,g_2,\cdots,g_n,-1,-g_2,\cdots,-g_n\}$ be a subgroup of $\mathbb{Z}_A^\star$ of even cardinality $|G|=2n$.

Theorem 2.1. [14] If $e_ie_j^{-1}\notin G$, $e_i,e_j\in\mathbb{Z}_A^\star$ or the integer e_i divides A, but $|e_iG|=2n$ and $e_i\notin e_jG$, then the integer code $\mathcal{C}$ with a parity-check matrix $H=(1,g_2,\cdots,g_n)$ is $(\pm e_1,\pm e_2,\cdots,\pm e_s)$ single error correctable.

Let us assume that we have a communication channel (AWGN, Rayleigh) and a modulation scheme (QAM, PSK) we use to transmit the information. Then we investigate the most probable errors that occur at the receiver and we define the type of error we want to correct using an integer code, i.e., we define the values of $e_i, i=1,\ldots,s$. In that situation, if it is possible, we would like to know the exact form of the parity-check matrix. In general, that is a very difficult problem. In next theorem we shall give the exact form of the parity-check matrix in case of $s=1$ and $e_i=1, i=1,\ldots,s$. We shall see that this construction is very useful for an AWGN channel and PSK modulation schemes.

Theorem 2.2. The integer code $\mathcal{C}$ over $\mathbb{Z}_{2^m}$ with a parity-check matrix $H=(1,2,3,\ldots,2^{m-1}-1)$ is a single (±1)-error correctable.

Proof: To prove that the code is (±1) single error correctable it is enough to show that all possible syndrome values are pairwise disjoint, i.e., $\pm h_i\neq\pm h_j$, where $h_i,h_j\in H$.

From the definition of H it is obvious that $h_i\neq h_j$ and $-h_i\neq -h_j$ over $\mathbb{Z}_{2^m+1}$. Also, we have that $-h_i\in\{2^{m-1}+1,2^{m-1}+2,\ldots,2^m-1\}$. Hence, $\pm h_i\neq\pm h_j$ with which the proof is completed. □

For multiple error correcting integer codes the situation is more complicated. Even in the simplest case, namely double (±1) error correctable integer code, it is rather difficult to define the exact form of the parity-check matrix H.

Let $\mathcal{C}$ have a parity-check matrix

$$H = \begin{pmatrix} h_{11} & h_{12} & h_{13} & h_{14} & \dots & h_{1n} \\ h_{21} & h_{22} & h_{23} & h_{24} & \dots & h_{2n} \end{pmatrix}.$$

The conditions for $\mathcal{C}$ to be double (± 1) error correctable code are the following

$$\begin{aligned} h_{ij} &\neq \pm h_{im}, & j &\neq m \\ h_{ij} \pm h_{im} &\neq \pm(h_{il} \pm h_{ik}), & (j,m) &\neq (l,k). \end{aligned} \qquad (1)$$

A construction of double (± 1) correctable integer codes can be found in [21].

To decode integer codes one can use a hard decoding algorithm [14]. This algorithm uses a look-up table which maps each syndrome value to the corresponding error vector. So, the complexity of the algorithm is linear with respect to the alphabet size A.

A good approximation of SEP in case of an AWGN channel using a QAM constellation coded by integer code can be found in [20]. There is given a lower bound of SEP in case of a single/multiple error correctable integer code for "cross", "square" and "big square" type of errors. In next section we shall derive a new upper bound for SEP, which is better than the previous one.

3. Theoretical Bound of Symbol Error Probability for Integer Codes on L^2-QAM over an AWGN Channel.

In this section we are going to introduce a technique for obtaining an upper bound on the average symbol error probability on square type of a QAM constellation coded independently on the in-phase and quadrature components by an integer code.

Suppose that a signal point $\boldsymbol{x} = (x^{in}, x^q)$ in a L^{2k}-QAM constellation, coded independently on the in-phase and the quadrature components by integer code $\mathcal{C} = (\mathcal{C}^{in}, \mathcal{C}^q)$ over $\mathbb{Z}_{L^k} \times \mathbb{Z}_{L^k}$ is sent through an AWGN-channel with power spectral density N_0. At the other end a detector estimates the received signal $\boldsymbol{r} = (r^{in}, r^q)$ and determines the signal point $\boldsymbol{y} = (y^{in}, y^q)$ that is the nearest to $\boldsymbol{r}$ in the constellation. The received signal $\boldsymbol{r}$ can be written as

$$\boldsymbol{r} = \boldsymbol{x} + \boldsymbol{e}$$

where $\boldsymbol{e} = (e^{in}, e^q)$ is the noise vector representing the (quantized) additive noise of the channel.

Given a L^{2k}-QAM signal constellation $\mathcal{K}$, let $q_u = (q_u^{in}, q_u^q)$ and $q_c = (q_c^{in}, q_c^q)$ be the average probability of a correct decision per signal point for uncoded $\mathcal{K}$ and coded $\mathcal{K}$, respectively.

Once we obtain q_u and q_c for $\mathcal{K}$, coded by an integer code $\mathcal{C}$, we can evaluate the error probability per symbol.

Let $X^{in}(\boldsymbol{c})$ with expectation $\mathbb{E}[X^{in}(\boldsymbol{c})]$ be the random variable that represents the number of erroneously decoded symbols in the in-phase component per a codeword when the codeword $\boldsymbol{c} \in \mathcal{C}^{in}$ is sent ($X^q(\boldsymbol{c})$ and $\mathbb{E}[X^q(\boldsymbol{c})]$, $\boldsymbol{c} \in \mathcal{C}^q$ for the quadrature component, respectively). The average symbol error probability $P_S(\mathcal{C})$ of the code $\mathcal{C}$ is defined as

$$P_S(\mathcal{C}) = 1 - (1 - P_S(\mathcal{C}^{in}))(1 - P_S(\mathcal{C}^q)) \qquad (2)$$

where

$$P_S(\mathcal{C}^{in}) = \sum_{\boldsymbol{c} \in \mathcal{C}^{in}} \frac{1}{|\mathcal{C}^{in}|} \frac{\mathbb{E}[X^{in}(\boldsymbol{c})]}{n} \qquad (3)$$

$$P_S(\mathcal{C}^q) = \sum_{\boldsymbol{c} \in \mathcal{C}^q} \frac{1}{|\mathcal{C}^q|} \frac{\mathbb{E}[X^q(\boldsymbol{c})]}{n}$$

and n is the length of code $\mathcal{C}$.

In our case we encode the in-phase and the quadrature components by same integer code, i.e., $q_u^{in} = q_u^q$, $q_c^{in} = q_c^q$ and $P_S(\mathcal{C}^{in}) = P_S(\mathcal{C}^q)$. Hence, we can rewrite (2) as

$$P_S(\mathcal{C}) = 2P_S(\mathcal{C}^{in}) - P_S(\mathcal{C}^{in})^2. \qquad (4)$$

Let $\boldsymbol{r}_i$ be the received signal when $\boldsymbol{x}_i$ is transmitted over the channel, and let $\mathcal{U}(\boldsymbol{a}) = (\mathcal{U}(a^{in}), \mathcal{U}(a^q))$ and $\mathcal{D}(\boldsymbol{a}) = (\mathcal{D}(a^{in}), \mathcal{D}(a^q))$ be the decision region of a signal point $\boldsymbol{a}$ of $\mathcal{K}$ in case of uncoded $\mathcal{K}$ and coded $\mathcal{K}$, respectively.

Let us suppose that we use single error correctable integer code. Then we can decode $\boldsymbol{x}$ correctly if either of the following two conditions holds:

1. All the received signals $\boldsymbol{r}_i$ $(1 \le i \le n)$ are in $\mathcal{U}(\boldsymbol{x}_i)$.
2. An $\boldsymbol{r}_k$ is in $\mathcal{D}(\boldsymbol{x}_k) \backslash \mathcal{U}(\boldsymbol{x}_k)$ and others in $\mathcal{U}(\boldsymbol{x}_i)(i \neq k)$.

But if a single $\boldsymbol{r}_k$ is out of $\mathcal{D}(\boldsymbol{x}_k)$ and others are in $\mathcal{U}(\boldsymbol{x}_i)$ $(i \neq k)$, then we have at most two erroneous symbols in the decoded codeword $\boldsymbol{y}$. In fact, since we use syndrome decoding, the syndrome may correspond incorrectly to a wrong single error vector.

Moreover, if ℓ signals $\boldsymbol{r}_{k_j}$ $(2 \le \ell < n, 1 \le j \le \ell)$ are out of $\mathcal{U}(\boldsymbol{x}_{k_j})$ and others in $\mathcal{U}(\boldsymbol{x}_i)$ $(i \neq k_j, 1 \le j \le \ell)$, then we have at most $\ell + 1$ erroneous symbols. Finally, in case that an $\boldsymbol{r}_k$ is in $\mathcal{U}(\boldsymbol{x}_k)$ and other $\boldsymbol{r}_i$ are out of $\mathcal{U}(\boldsymbol{x}_i)$ $(i \neq k)$ or all n signals are out of their decision regions $\mathcal{U}(\boldsymbol{x}_i)$ $(1 \le i \le n)$, then all the symbols of the decoded codeword may be erroneous.

Now we approximate the probability that each component of the received signal r_i^{in} is in $\mathcal{U}(x_i^{in})$ and $\mathcal{D}(x_i^{in})$ by q_u^{in} and q_c^{in}, respectively. This means that $X^{in}(\boldsymbol{c})$ for $\boldsymbol{c} \in \mathcal{C}^{in}$ is replaced by a common random variable X^{in} that has the probability distribution based on q_u^{in} and q_c^{in}. That is, (3) is rewritten as

$$P_S(\mathcal{C}^{in}) \approx \frac{1}{n} \mathbb{E}[X^{in}]. \qquad (5)$$

Moreover, we obtain

$$\mathbb{E}[X^{in}] \le 2\binom{n}{1}(q_u^{in})^{n-1}(1-q_c^{in}) + n\binom{n}{0}(1-q_u^{in})^n + \sum_{\ell=2}^{n-1}(\ell+1)\binom{n}{\ell}(1-q_u^{in})^{\ell}(q_u^{in})^{n-\ell}. \quad (6)$$

The right-hand side of (6), denoted by $F(q_u^{in}, q_c^{in})$, yields after a simple calculation

$$\frac{1}{n}F(q_u^{in}, q_c^{in}) = (1-q_u^{in}) - 2(q_u^{in})^{n-1}(q_c^{in} - q_u^{in}) + \frac{1}{n}(1-(q_u^{in})^n - (1-q_u^{in})^n) \quad (7)$$

Hence, in case of a single error correctable integer code, using (7) and (4) we obtain one good approximation of $P_S(\mathcal{C})$.

Similarly we obtain an approximation of $P_S(\mathcal{C})$ for double error correctable integer code as well. Here $F(q_u^{in}, q_c^{in})$ has the following form:

$$\frac{1}{n}F(q_u^{in}, q_c^{in}) = 1 - q_u^{in} - 2(q_u^{in})^{n-2}(n-1)(q_c^{in} - q_u^{in})^2 + (q_u^{in})^{n-1}(2q_u^{in} - 3q_c^{in}) - q_u^{in}(1-q_u^{in})^{n-1} + \frac{2}{n}(1-(q_u^{in})^n - (1-q_u^{in})^n) + (q_u^{in})^n \quad (8)$$

In the next section Examples 3 and 4 demonstrate a comparison between the theoretical bound, (8), and experimental results for 64- and 256-QAM signal constellations coded by double (± 1) error correctable codes.

4. Soft Decoding Algorithm for Integer Codes

If we want to obtain more coding gain we should apply soft decoding algorithm instead of hard decoding algorithm (which we mentioned above). In this Section we are going to introduce a soft decoding algorithm for integer codes which is based on the algorithm given in [22].

Let us assume that a signal constellation (QAM, PSK, ASK) is coded by a single/multiple $(\pm l_1, \pm l_2, \dots, \pm l_t)$ error correctable integer code $\mathcal{C}$ of length n over $\mathbb{Z}_A$ with a parity-check matrix $H \in \mathbb{Z}_A^{m\times n}$.

Let a modulated codeword be represented by $\boldsymbol{x} = (x_1, x_2, \dots, x_n)$ where x_i is a signal point in that constellation and $\boldsymbol{x}$ is transmitted over an AWGN channel. And let the sampled channel output sequence be given by $\boldsymbol{y} = (y_1, y_2, \dots, y_n)$.

First, the decoder makes *hard decisions* on each channel output y_i, i.e., the decoder selects the nearest signal point r_j to y_i in the constellation. We denote the received sequence at the decoder with $\boldsymbol{r} = (r_1, r_2, \dots, r_n)$, where r_i is a signal point in the constellation.

In soft decoding we utilize the analog received samples y_i, $1 \le i \le n$, to find the most probable codeword to be transmitted in the sense of the maximum likelihood estimation.

We propose the following algorithm for soft decoding of a $(\pm l_1, \pm l_2, \dots, \pm l_t)$ error correctable integer code $\mathcal{C}$ of length n over $\mathbb{Z}_A$.

Basic Soft Decoding Algorithm for Integer Codes:

In: The channel output $\boldsymbol{y} = (y_1, y_2, \dots, y_n)$ and the received sequence $\boldsymbol{r} = (r_1, r_2, \dots, r_n)$.

Out: The decoded codeword $\tilde{\boldsymbol{c}} = (\tilde{c}_1, \tilde{c}_2, \dots, \tilde{c}_n)$.

Step 1. Calculate the squared distance $\Delta^2[i, \varepsilon]$ between y_i and each of the signal points associated with $r_i + \epsilon \pmod A$ where $\epsilon \in \mathcal{L} = \{-l_1, -l_2, \dots, -l_s, 0, l_1, l_2, \dots, l_s\}$.

Step 2. Compute the syndrome value $\boldsymbol{s} = \boldsymbol{r}H^T \pmod A$, $\boldsymbol{s} \in \mathbb{Z}_A^m$.

Step 3. Let $\mathcal{E}[s]$ be the set of all the vectors $\boldsymbol{e} = (e_1, e_2, \dots, e_n) \in \mathcal{L}^n$ such that

$$\boldsymbol{e}H^T = \boldsymbol{s} \pmod A.$$

Then find the vector $\boldsymbol{e}^* = (e_1^*, e_2^*, \dots, e_n^*) \in \mathcal{E}[s]$ that minimizes $\sum_{i=1}^n \Delta^2[i, e_i^*]$.

Step 4. Output $\tilde{\boldsymbol{c}} = \boldsymbol{r} - \boldsymbol{e}^*$ and stop. □

The above algorithm accomplishes the maximum likelihood decoding for an AWGN channel. In Step 3 an exhaustive search is performed to find $\boldsymbol{e}^*$ among $\mathcal{E}[s]$. It is reasonable if n is relatively small, say $n = 4$. For a large value of n, we can utilize a trellis of $n+1$ layers, in each of which there are A^m states. In our algorithm each state in the i-th layer for $i = 0, 1, \dots, n$ is indexed by $\boldsymbol{k} = (k_1, k_2, \dots, k_n) \in \mathbb{Z}_A^n$. A pair of numbers $(d_{\boldsymbol{k}}^{(i)}, e_{\boldsymbol{k}}^{(i)})$ is attached to the $\boldsymbol{k}$-th state in the i-th layer. Here $d_{\boldsymbol{0}}^{(0)} = 0$ and $d_{\boldsymbol{k}}^{(0)} = \infty$ for $k \in \mathbb{Z}_A^n \backslash \{\boldsymbol{0}\}$ and $d_{\boldsymbol{k}}^{(i)}$ is given by

$$d_{\boldsymbol{k}}^{(i)} = \min_{\epsilon \in \mathcal{L}} \left\{ d_{\boldsymbol{k}+\epsilon \boldsymbol{h}_i}^{(i-1)} + \Delta^2[i, \epsilon] \right\}, \quad (9)$$

where $\boldsymbol{h}_i$ is the i-th row of the parity-check matrix H, $i = 1, 2, \dots, n$ and $\boldsymbol{k} \in \mathbb{Z}_A^n$. The addition in $\boldsymbol{k} + \epsilon \boldsymbol{h}_i$ is in the ring $\mathbb{Z}_A^n$. Moreover, $e_{\boldsymbol{k}}^{(i)} = \epsilon^*$ where ϵ^* is an element in $\mathcal{L}$ that achieves the minimum value of (9). The Viterbi algorithm can sequentially calculate $\{(d_{\boldsymbol{k}}^{(i)}, e_{\boldsymbol{k}}^{(i)}), \boldsymbol{k} \in \mathbb{Z}_A^n\}$ for $i = 1, 2, \dots, n$ in a similar way discussed in [19], [23]. After the calculation is completed, e_n^* is given by the value of $e_{\boldsymbol{s}}^{(n)}$ associated to the $\boldsymbol{s}$-th state in the n-th layer where $\boldsymbol{s}$ is the syndrome value obtained in Step 2. The other $e_{n-1}^*, \dots, e_1^*$ are computed in descending order by using the following recursive equations on $\boldsymbol{k}^{(i)}$, $i = n-1, \ldots, 1$ with the initial value $\boldsymbol{k}^{(n)} = \boldsymbol{s}$:

$$\begin{aligned} \boldsymbol{k}^{(i)} &= \boldsymbol{k}^{(i+1)} + e^*_{i+1}\boldsymbol{h}_{i+1}, \quad \boldsymbol{k}^{(i)} \in \mathbb{Z}_A^n, \\ e^*_i &= e^{(i)}_{\boldsymbol{k}^{(i)}}. \end{aligned}$$

It is well known that the computational complexity of the Viterbi algorithm (VA) grows only linearly with the length of the information sequence [24].

Let us suppose we want to transmit n symbols over an AWGN channel and a constellation (PSK, QAM) with 2^k signal points using two different codes, that is, integer code of length $n_1, n_1|n$ over $\mathbb{Z}_{2^k}$ with a parity-check matrix $H \in \mathbb{Z}_{2^k}^{m\times n}$ and a 2^{k-1} state TCM of length n_2 (in bits), $n_2|n$.

In this paper we apply the soft decoding algorithm (SDA) only for single and double error correctable integer codes, so we have that $m = 1$ or $m = 2$. Moreover, if $k|2$ we encode independently the in-phase and quadrature components of a QAM constellation by a double error correctable integer over $\mathbb{Z}_{2^{k/2}}$. So, the transition matrix of the trellis for the SDA, using single/double error correctable integer codes, has a size $2^k \times 2^k$, while the TCM has a transition matrix of size $2^{k-1} \times 2^{k-1}$.

We can say that the SDA for integer codes is a modified VA. The main difference is that some operations (addition, multiplication) in the SDA are in $\mathbb{Z}_A$. For both, integer and TCM codes, we can apply the truncated Viterbi algorithm to make the comparison fair. Hence, we can conclude that the two algorithms have linear complexity with respect to n.

Note that we can apply the soft decoding algorithm to any modulation schemes (QAM, ASK, PSK).

Below, with several examples, we shall demonstrate how the soft decoding algorithm works for PSK and QAM modulation schemes. As we mentioned above, to make the comparison between TCM and integer codes fair, we use a 2^{k-1} state TCM to encode a constellation consisting of 2^k signal points. For more accurate results of SEP in our experiments, for a given value of SNR we transmit 10^8 bits over a signal constellation coded separately by TCM and an integer code.

Example 1. (8-PSK constellation) Let us assume that the signal points of 8-PSK constellation are numbered by integers from 1 to 8 (consecutively).

Substituting $m = 3$ in Theorem 2.2 we obtain a (± 1) single error correctable integer code of length $n = 3$ over $\mathbb{Z}_8$ with a parity-check matrix $H = (1, 2, 3)$.

In Figure 1 we show the comparison of the simulation results on symbol error probability for TCM, uncoded and coded (using hard and soft decoding algorithms) 8-PSK. From the simulation results we can conclude that using the soft decoding algorithm for a coded 8-PSK with a single (± 1) error correcting integer code we gain approximately 2 dB compared to the hard decoding. In this case the TCM (8 state TCM with code rate 2/3 given by Ungerboeck [2]) has slightly better performance than the integer code. □

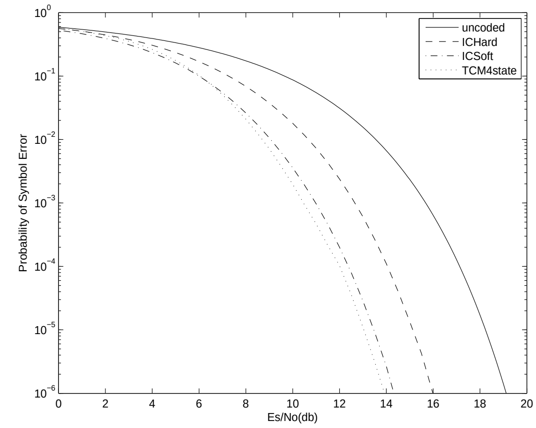

Fig. 1 A comparison of symbol error probability versus signal-to-noise ratio between 8 state TCM, uncoded and coded 8-PSK (using the integer code in Example 1 with the hard and soft decoding algorithms).

Example 2. (16-QAM constellation) Let us assume that the points of a 16-QAM constellation are numbered by the integers from 1 to 16 beginning from the left upper corner to the bottom right corner. Index each signal point. Using Theorem 2.1 we can construct a single $(\pm 1, \pm 3, \pm 4, \pm 5)$-error correctable code $\mathcal{C}$ of length $n = 2$ over $\mathbb{Z}_{17}$ with a parity-check matrix $H = (1, 2)$. In this case the code is perfect and the error type it can correct is a "square".

Note that to assign each symbol in a codeword with a signal point in the constellation, we exclude codewords that contain zeros. In this case it is only one codeword $c = (0, 0)$. The rate of the code is 1/2.

The comparison of our simulation results of symbol error probability versus the signal-to-noise ratio using that code (applying hard and soft decoding), an 8-state TCM [2] and an uncoded 16-QAM is given in Figure 3.

$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(0,4)$	$(0,5)$	$(0,6)$	$(0,7)$
$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(1,4)$	$(1,5)$	$(1,6)$	$(1,7)$
$(2,0)$	$(2,1)$	$(2,2)$	$(2,3)$	$(2,4)$	$(2,5)$	$(2,6)$	$(2,7)$
$(3,0)$	$(3,1)$	$(3,2)$	$(3,3)$	$(3,4)$	$(3,5)$	$(3,6)$	$(3,7)$
$(4,0)$	$(4,1)$	$(4,2)$	$(4,3)$	$(4,4)$	$(4,5)$	$(4,6)$	$(4,7)$
$(5,0)$	$(5,1)$	$(5,2)$	$(5,3)$	$(5,4)$	$(5,5)$	$(5,6)$	$(5,7)$
$(6,0)$	$(6,1)$	$(6,2)$	$(6,3)$	$(6,4)$	$(6,5)$	$(6,6)$	$(6,7)$
$(7,0)$	$(7,1)$	$(7,2)$	$(7,3)$	$(7,4)$	$(7,5)$	$(7,6)$	$(7,7)$

Fig. 2 Indexing of the signal points in a 64-QAM

Here, because the rate of the code is relatively low, applying the soft decoding algorithm we gain approximately 4 dB compared with hard decoding and about 0.5 dB more than TCM. □

Let us consider an M-QAM constellation of square type. In this case we have that $M = 2^{2k},\ k = 1, 2, \ldots$. Let us index each signal point s_{ij} in an M-QAM constellation with a pair $(i, j) \in \mathbb{Z}_{2^k} \times \mathbb{Z}_{2^k}$ of elements of $\mathbb{Z}_{2^k}$ where i is the number of the row and j is the number of the column which s_{ij} is placed in. The counting begins from the left bottom corner and goes upwards and to the right, respectively (see Fig. 2 for the case $M = 64$). A given byte is mapped into a signal point s_{ij}, if its left k bits and its right k bits are the binary representation of i and j, respectively.

Example 3. (64-QAM constellation) Let us index each signal point s_{ij} with a pair $(i, j) \in \mathbb{Z}_8 \times \mathbb{Z}_8$ as we described above (see Fig. 2). Using (1) it is easy to check that we can construct a double (±1)-error correctable code $\mathcal{C}$ of length $n = 4$ over $\mathbb{Z}_9$ with a parity-check matrix

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

In this case, any two signal points $s_{i_1 j_1}$ and $s_{i_2 j_2}$ are followed by two additional signals $s_{a_1 b_1}$ and $s_{a_2 b_2}$ such that (i_1, i_2, a_1, a_2) and (j_1, j_2, b_1, b_2) are codewords of $\mathcal{C}$.

Note that we can not use all the codewords of the code $\mathcal{C}$. The error type the code $\mathcal{C}$ can correct is a "square" type.

We can obtain a theoretical bound for this code using (7) and (4) with values of q_u^{in} and q_c^{in} [20]:

$$q_u^{in} = (1 + 7\,\mathrm{erf}(\gamma))/8,$$
$$q_c^{in} = (1 + 3\,\mathrm{erf}(3\gamma))/4,$$

where $\gamma = \sqrt{E_s/42N_0}$.

The SEP of our simulation results and the theoretical bound as well as the approximation of error probability given in [20] are plotted in Figure 4. In Figure 5 we show the comparison of the simulation results on SEP versus the signal-to noise ratio of uncoded, coded 16-QAM (using the integer code with hard and soft decoding), and TCM with 32 states [2]. Here, using the soft decoding algorithm we gain about 3 dB over the hard decoding and 2 dB over the TCM with 128 states [2]. □

Example 4. (256-QAM constellation) Let us index each signal point s_{ij} with a pair $(i, j) \in \mathbb{Z}_{17} \times \mathbb{Z}_{17}$ as we did in the previous example. Using (1) we can check that the code over $\mathbb{Z}_{17}$ with a parity-check matrix

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

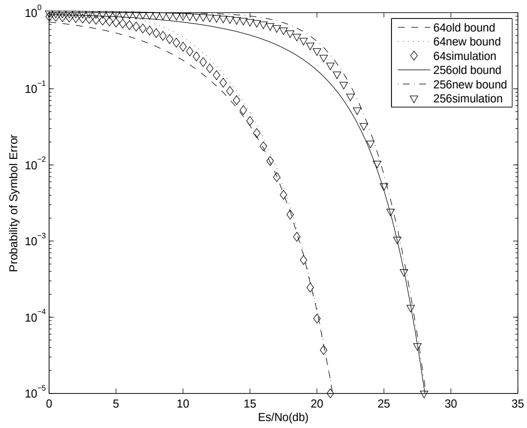

Fig. 3 A comparison of symbol error probability versus signal-to-noise ratio between simulation results, the new theoretical bound derived here and the bound given in [20] for 64- and 256-QAM .

is a double (±1)-error correctable code $\mathcal{C}$ of length 8.

As in the previous two examples we can not use all the codewords of the code. We exclude the codewords that contain a zero as a symbol. Because of that the information rate slightly decreases - from R=3/4 to R=17/24 (in bits).

The theoretical bound of the code is given by (7) and (4) with values of q_u^{in} and q_c^{in} [20]:

$$q_u^{in} = (1 + 15\,\mathrm{erf}(\gamma))/16,$$
$$q_c^{in} = (1 + 7\,\mathrm{erf}(3\gamma))/8,$$

where $\gamma = \sqrt{E_s/170N_0}$.

The SEP obtained by the simulations, the theoretical bound, and the approximation of error probability given in [20] are plotted in Figure 4. The symbol error probability versus the signal-to-noise ratio obtained by simulations of uncoded 256-QAM, 128-states TCM [2], and coded modulation with the aforesaid integer code (applying hard and soft decoding), are given in Figure 6. These results show that applying the soft decoding algorithm we gain 2 dB in SNR over the hard decoding for a given value of symbol error probability. The TCM with 128-state [2] has the same performance as the soft decoding. □

5. Conclusions

In this paper we presented applications of integer codes in different modulation schemes. A new upper bound on symbol error probability was derived in the case of square QAM constellations coded by an integer code. This bound is very tight compared with simulation results, and even better than the known bound [20] for small values of SNR. For a high SNR, these two bounds as well as the simulation results give almost same value

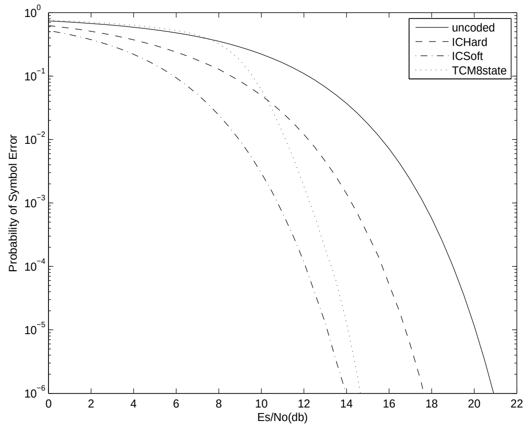

Fig. 4 A comparison of symbol error probability versus signal-to-noise ratio between the coded 16-QAM (with the integer code from Example 2, using hard and soft decoding algorithms), the 8 state TCM and the uncoded 16-QAM.

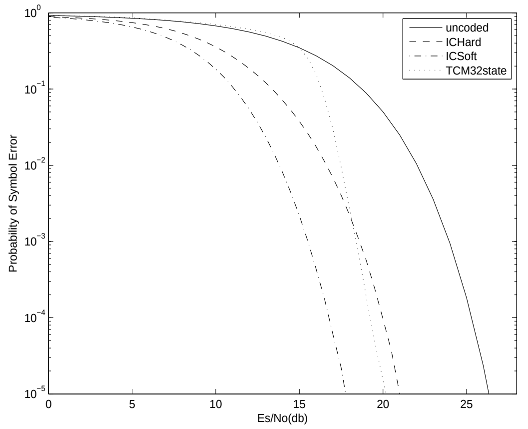

Fig. 5 A comparison of symbol error probability versus signal-to-noise ratio between the coded 64-QAM (with the integer code from example 3, using hard and soft decoding algorithms), the 32 state TCM and uncoded 64-QAM.

of SEP. Moreover, to improve the error rate of integer codes we proposed a soft decoding algorithm.

Experimental results of the comparison on the symbol error probability versus the signal-to-noise ratio over an AWGN channel between integer codes and TCM schemes show us that they have very similar error performances. In some case using the soft decoding we can gain up to 2 dB over the TCM in Example 4, while in another TCM scheme is better than the integer code (Example 1). That gives us a motivation to continue our research on multiple error correcting integer codes with different types of errors.

Also, we can conclude that the proposed soft decoding algorithm, compared with the hard decoding, has a better performance for a small value of code length n. For a larger value of n the soft decision decoder is substantially more complex than the hard decision decoder. **However, in this case the hard decision decoder has more space complexity, which can result in increasing the circuit complexity in case of a hardware implementation**.

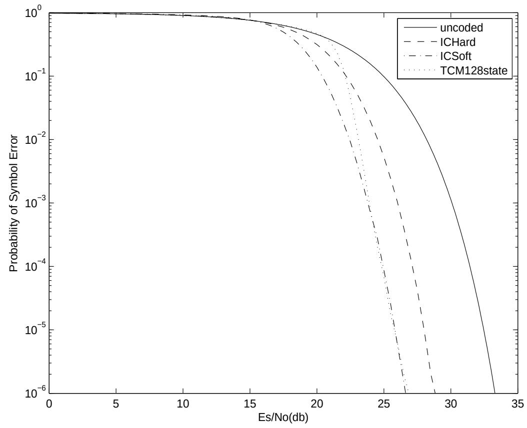

Fig. 6 A comparison of symbol error probability versus signal-to-noise ratio between the coded 256-QAM (with the integer code from example 4, using hard and soft decoding algorithms), the 128 state TCM and uncoded 256-QAM.

Integer codes could be applied for fading channels (Rayleigh, Rician). For our future research plans we consider to start with slow-fading channels, which are similar to AWGN channels.

As a conclusion we can say that because of their flexibility integer codes will be very suitable for application in real communication systems.

6. Acknowledgement

This work was partially supported by "FY2007 Japan Society for the Promotional Science (JSPS) Postdoctoral Fellowship for Foreign Researchers". **The authors would like to thank the anonymous reviewers for their helpful comments which improved the quality of this paper**.

References

[1] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. Inform. Theory*, vol. IT-28, no. 1, pp. 55–66, Jan. 1982.
[2] G. Ungerboeck, "Trellis-coded modulation with redundant signal sets," *IEEE Communications Magazine*, pp. 5–21, Feb. 1987.
[3] H. Imai and S. Hirakawa, "A new multilevel coding method using error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-23, No. 1, pp. 656–662, Jan. 1977.
[4] R. Baldini F and P. G. Farrell, "Coded modulation based on rings of integers modulo-q," *IEE Proc. Commun.*, part 1, vol. 141, no. 3, pp. 129-136, 1994.
[5] A.J. Han Vinck and H. Morita, "Codes over the ring of integer modulo m," *IEICE Trans. on Fundamantals*, vol. E81-A, pp. 2013–2018, Oct. 1998.
[6] I. Blake, "Codes over certain rings ," *Information and Control*, v. 20, pp. 396-404, 1972.

[7] I. Blake, "Codes over integer residue rings ," *Information and Control*, v. 29, pp. 295-300, 1975.

[8] A. R. Calderbank, N. J. A. Sloane, "Modular and $p-$adic Cyclic Codes," *Designs, Codes and Cryptography*, vol 6, No 1, pp. 21-36, 1995.

[9] E. Spiegel, "Codes over Z_m, " *Information and Control*, vol. 35, pp. 48-51, 1977.

[10] V. I. Levenstein and A. J. Han Vink, "Perfect (d, k) - codes capable of correcting single peak-shifts, " *IEEE Trans. Inform. Theory*, vol. 39, No. 2, pp. 656-662, 1993.

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

[12] 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.

[13] A. Geyser and H. Morita, "Performance of Integer Coded Modulation over Rayleigh Fading Channels," *Proc. of the 22nd SITA*, Yuzawa, Japan, pp. 745-748, 1999.

[14] H. Kostadinov, H. Morita and N. Manev, " Integer Codes Correcting Single Errors of Specific Types $(\pm e_1, \pm e_2, \ldots, \pm e_s)$," *IEICE Trans. on Fundamentals*, vol. E86-A, No. 7, pp. 1843-1849, July 2003.

[15] J. Rifa, "Groups of complex integers used as QAM signals," *IEEE Trans. Inform. Theory,* vol. IT-41, No. 5, pp. 1512-1517, Sept. 1995.

[16] K. Huber, "Codes over Gaussian Integers", *IEEE Trans. Inform. Theory,* vol. IT-40, No. 1, pp. 207-216, Jan. 1994.

[17] K. Nakamura, "A class of error correcting codes for DPSK channels", *Proc. of International Conference on Communications (ICC'79)*, pp. 45.4.1- 45.4.5, 1979.

[18] K. Nakamura, "Error correcting scheme for Differentially Encoded M-ary Quadrature Amplitude Modulation System", *Proc. of Symposium on Information Theory and its Applications (SITA)*, pp. 44 - 52, 1982.

[19] J. K. Wolf, "Efficient Maximum Likelihood Decoding of Linear Block Codes Using a Trellis," *IEEE Trans. Inform. Theory*, vol. IT-24, no. 1, pp. 76–80, Jan. 1978.

[20] H. Kostadinov, H. Morita and N. Manev, "Derivation on Bit Error Probability of Coded QAM using Integer Codes," *IEICE Trans. on Fundamentals*, vol. E87-A, No. 12, pp. 3397-3403, Dec. 2004.

[21] H. Kostadinov, H. Morita, N. Iijima and N. Manev, "Double Error Correctable Integer Code and Its Application to QAM," *Proc. of International Symposium on Information Theory and its Applications (ISITA)*, Auckland, New Zealand, pp. 566-571, Dec 2008.

[22] 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)*, Parma, Italy, pp. 1321-1325, Oct 2004.

[23] E. Zehavi and J. K. Wolf, "On the Performance Evaluation of Trellis Codes," *IEEE Trans. Inform. Theory*, vol. IT-33, no. 2, pp. 196–202, Mar. 1987.

[24] S. Benedetto and E. Biglieri, *Principles of Digital Transmission With Wireless Applications*, Kluwer Academic, New York 1999.

Hristo Kostadinov was born in Sofia, Bulgaria, in 1974. He received the B. Sc. degree and M. Sc. degree in 1998, and 2001, respectively at Sofia University, Sofia, Bulgaria. In March 2005, he received his Ph. D. degree at the University of Electro-Communications, Tokyo, Japan. Since April 2005 he is Assistant Professor at the Institute of Mathematics and Informatics of the Bulgarian Academy of Sciences. Currently he is a Postdoctoral Fellow at the University of Electro-Communications, Tokyo. His research interests are in coding theory, information theory and communication theory and signals.

Hiroyoshi Morita received the B. Eng. degree, the M. Eng. degree, and D. Eng. degree from Osaka University, in 1978, 1980 and 1983, respectively. In 1983, he joined Toyohashi University of Technology, Aichi, Japan as a Research Associate in the School of Production System Engineering. In 1990, he joined University of Electro-Communications, Tokyo, Japan, first as an Assistant Professor at the Department of Computer Science and Information Mathematics, where from 1992, he was an Assosiate Professor. Since 1995 he has been with the Graduate School of Information Systems. He was Visiting Fellow at the Institute of Experimental Mathematics, University of Essen, Essen, Germany during 1993-1994. His research interests are in combinatorial theory, information theory, and coding theory, with applications to the digital communication systems.

Noboru IIjima was born in Shizuoka, in 1983. He received the B. Sc. degree in 2007 and his M. Sc. degree in 2009, both from the University of Electro-Communications, Tokyo, Japan. Since April 2009 he works at NEC, Japan.

A. J. Han Vinck was born in Breda, The Netherlands, in 1949. He received the M. Sc. degree in 1974 and his Ph. D. degree in 1980, both from the Technical University of Eindhoven, Eindhoven, The Netherlands. From 1985 to 1990, he was an Associate Professor at the University of Eindhoven, and became a Full Professor at 1990 at the university of Essen, Essen, Germany. From 1992 to 1994, he was Director of the Institute for Experimental Mathematics at the University of Essen. His interest is digital communications. He organized the Veldhoven Workshop on Information Theory in 1990 and was Cochairman of the International Symposium on Information Theory (ISIT'97) in Ulm, Germany.

Nikolai Manev received his M.Sci. in mathematics in 1977 from Sofia University and Ph. D. in 1984 from the Institute of Mathematics and Informatics of the Bulgarian Academy of Sciences.In 1977 he joined the Institute of Mathematics and Informatics of the Bulgarian Academy of Sciences as a Researcher. Since 1990 he is an Associate Professor in the same institute. His research interests are in algebraic and combinatorial coding theory, cryptography and their applications to the digital communication systems.