On Single Cross Error Correcting Integer Codes with Minimum-Energy Signal Constellations

Hiroyoshi Morita, Ko Kamada
Graduate School of Information Systems
University of Electro-Communications
Chofugaoka 1-5-1, Chofu, Tokyo, Japan
{morita, kokamada}@math-sys.is.uec.ac.jp

Hristo Kostadinov
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Acad. G. Bonchev St., 1113 Sofia, Bulgaria
hristo@gmail.com

Adriaan J. van Wijngaarden
Commun. & Stat. Sciences Dept.
Bell Laboratories, Alcatel-Lucent
Murray Hill, NJ 07974, U.S.A.
alw@research.bell-labs.com

***Abstract*— Integer codes, defined over integer rings, allow the correction of single cross errors with distance 1 in a signal point constellation on a two-dimensional lattice. Several construction methods support the construction of integer codes that give constellations that have a variety of shapes. In this paper, we characterize all constellations that can be obtained from a particular integer code. In particular, we determine those that minimize the average symbol energy. In addition, we evaluate the symbol error probability when using an integer code for coded QAM constellations.**

I. Introduction

Integer codes are defined over $\mathbb{Z}_m \triangleq \mathbb{Z}/m\mathbb{Z}$, the residue ring of integers modulo m. Let $m, n, k \in \mathbb{N}$, $\boldsymbol{H} \in \mathbb{Z}_m^{k\times n}$ and $\boldsymbol{d} \in \mathbb{Z}_m^k$. An integer code $\mathcal{C}(\boldsymbol{d}, \boldsymbol{w}) \subseteq \mathbb{Z}_m^n$ of length n is defined by

$$\mathcal{C}(\boldsymbol{d}, \boldsymbol{H}) = \left\{ \boldsymbol{c} \in \mathbb{Z}_m^n \,\middle|\, \boldsymbol{c}\boldsymbol{H}^T = \boldsymbol{d} \right\} \tag{1}$$

where $\boldsymbol{H}$ is the check matrix for the integer code. Integer codes can be utilized in many applications and were shown to be particularly useful for coded modulation and magnetic recording [1], [2]. An overview of integer codes is also given in [3], [4] and references therein.

In this paper, we are concerned with the integer codes where $k = 1$. That is, $\boldsymbol{H}$ is an n-dimensional vector $\boldsymbol{w} \in \mathbb{Z}_m^n$ and $\boldsymbol{d}$ is a scalar d in $\mathbb{Z}_m$. Such an integer code $\mathcal{C}(d, \boldsymbol{w})$ can correct a single error in a codeword. A codeword of $\mathcal{C}(d, \boldsymbol{w})$ consists of $n - 1$ information symbols and one error control symbol. The rate of $\mathcal{C}(d, \boldsymbol{w})$ is $1 - 1/n$.

Let $\mathcal{E}$ be the set of error vectors that the code is required to correct. To identify each error vector in $\mathcal{E}$, it is necessary to choose the values of $\boldsymbol{w}$ and m in such a way that the syndrome value is unique for each of the error vectors in $\mathcal{E}$. Therefore, we have to satisfy the inequality

$$m \geq |\mathcal{E}| + 1. \tag{2}$$

If an integer code can correct any error vector in $\mathcal{E}$, then it is called *$\mathcal{E}$-correctable*. Such an $\mathcal{E}$-correcting code $\mathcal{C}(d, \boldsymbol{w})$ is said to be *perfect* if $m = |\mathcal{E}| + 1$.

Let a single $(1, t)$-cross error correcting integer code be an integer code that allows the correction of a single error vector in the set

$$\mathcal{E} = \{(e_1, 0, \ldots, 0), \ldots, (0, \ldots, 0, e_n)\},$$

where $e_i \in \{-t, -1, +1, +t\}$, and $1 \leq i \leq n$.

Constellations associated with a single error correcting integer code [4] have a variety of shapes, dependent on the value of t. The key issue is to determine the constellation that has the minimum average symbol energy among all possible constellations for integer codes.

In this paper, we will characterize all the constellations that can be obtained for cyclic integer codes proposed in [4], and extend this construction. Then, we show that all constellations of the OMEC codes [5], [6] are obtained using this extension of the cyclic construction.

Moreover, we determine the symbol error probability when using integer codes in conjunction with QAM over an AWGN channel. Our evaluation of the error probability is based on a counting argument that gives an upper bound that is more tight than the bound presented in [7].

This paper is organized as follows. Section II describes signal constellations which can be designed by means of single $(1, t)$-cross error correcting integer codes. Section III presents a new class of integer codes derived from the theory of quadratic residues [8]. In Section IV, we compare our codes with the OMEC codes presented in [5] and show that they are equivalent. Section V gives an upper bound on the symbol error probability when an integer code is used for coded QAM. Section VI summarizes our results.

II. Signal Constellations

A single $(1, t)$ error correcting code can be used to correct single errors of the unit magnitude in a two-dimensional signal point constellation $\mathcal{Q}_m \in \mathbb{Z}^2$ with m points. We will label each of the m signal points by a unique number $a \in \mathbb{Z}_m$. A possible assignment of each grid point $\boldsymbol{a} = (a_1, a_2) \in \mathbb{Z}^2$ is given by the mapping $\xi(\boldsymbol{a}) = a_2 \cdot t + a_1 \pmod{m}$.

When such a lattice is used for coded modulation in a high signal-to-noise ratio (SNR) regime, the most common errors will be to the left, right, top, or bottom of the transmitted signal point. Using the mapping ξ, this corresponds to the errors ± 1, $\pm t$ in $\mathbb{Z}_m$. The set of most likely errors has the form of a cross on the lattice.

A signal point constellation with the mapping ξ will be denoted by $\mathrm{SPC}(m, 1, t)$. We will consider integer codes over

$\mathbb{Z}_m$ that are capable of correcting single $(1,t)$-cross errors on SPC$(m,1,t)$.

III. Construction Methods

The following cyclic construction of integer codes, presented in [4], provides a class of perfect $(1,t)$-cross error correcting codes of length n for which $m = 4n+1$ is prime and t generates the multiplicative group $\mathbb{Z}_m^* \triangleq \mathbb{Z}_m \backslash \{0\}$.

Theorem 1 (Construction A [4]): For a prime $m = 4n+1$ and t that generates $\mathbb{Z}_m^*$, there exists a perfect single $(1,t)$-cross error correcting code $\mathcal{C}(d, \boldsymbol{w}^{(a)}) \subseteq \mathbb{Z}_m^n$ with $\boldsymbol{w}^{(a)}$ such that

$$\boldsymbol{w}^{(a)} = (1, t^2, t^4, \ldots, t^{2n-2}). \tag{3}$$

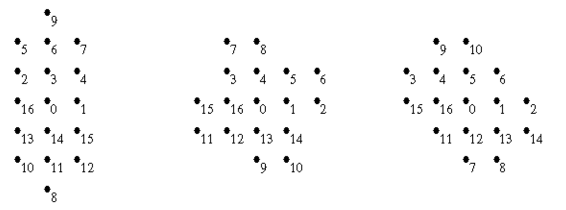
Each component $w_i^{(a)} = t^{2i-2}$ of $\boldsymbol{w}^{(a)}$ $(1 \le i \le n)$ is a quadratic residue [8] modulo m. In fact, for $q = w_i^{(a)}$, there exists a number $x = t^{i-1} \in \mathbb{Z}_m^*$ such that $x^2 = q \pmod m$. A necessary and sufficient condition that q is a quadratic residue modulo m is that q has an even order for t, i.e., $q = t^{2k}$. The remaining numbers in $\mathbb{Z}_m^*$ are called quadratic non-residues. In particular, any generator of $\mathbb{Z}_m^*$ is a quadratic non-residue modulo m.

A representative weight vector of $\boldsymbol{w}^{(a)}$ is obtained by replacing any weight $w_i^{(a)} > m/2$ by $m - w_i^{(a)}$. Therefore, the representative weight vector is uniquely determined regardless of the generator $t \in \mathbb{Z}_m^*$.

Theorem 1 states that the code $\mathcal{C}(d, \boldsymbol{w}^{(a)})$ is a $(1,g)$-cross error correcting integer code for a generator g of $\mathbb{Z}_m^*$. We can easily extend this statement as follows:

Corollary 1: The code $\mathcal{C}(d, \boldsymbol{w}^{(a)})$ is a $(1,t)$-cross error correcting code for a quadratic non-residue t modulo m.

Figure 1 shows three signal point constellations with $m = 17$ points, where t is 3, 4, and 5, respectively. Here, 3 and 5 are quadratic non-residues modulo 17 while 4 is a quadratic residue modulo 17. In fact, $\boldsymbol{w}^{(a)}$ is given as $(1,2,4,8)$ for $m = 17$. Constellations SPC$(17,1,3)$ and SPC$(17,1,5)$ are obtained by $\boldsymbol{w}^{(a)}$ while constellation SPC$(17,1,4)$ supports a perfect integer code obtained by Construction A$^+$ presented below.



a. SPC(17,1,3) *b.* SPC(17,1,4) *c.* SPC(17,1,5)

Fig. 1. Signal point constellations for $m = 17$.

Construction A$^+$

Since $\mathbb{Z}_m^*$ consists of the same number of quadratic residues and quadratic non-residues, Corollary 1 implies that we have $2n$ types of $(1,t)$ to be corrected by $\mathcal{C}(d, \boldsymbol{w}^{(a)})$.

Here, we will present another method for constructing $(1,t)$-cross error correcting codes for quadratic residues t with a different weight vector from $\boldsymbol{w}^{(a)}$. First let $\mathcal{G}^{(r)} = \{1, g, \ldots, g^{r-1}\}$ for a divisor r of n and a generator g of $\mathbb{Z}_m^*$ where $m = 4n+1$. Then we define the weight set $\mathcal{W}_A^{(g,r)}$ as

$$\mathcal{W}_A^{(g,r)} = \bigcup_{k=0}^{n/r-1} g^{2rk}\, \mathcal{G}^{(r)} \tag{4}$$

where $g^{2rk}\,\mathcal{G}^{(r)}$ is the set that results from the scalar multiplication of the elements of $\mathcal{G}^{(r)}$ by g^{2rk}. It is easy to verify that the cardinality of $\mathcal{W}_A^{(g,r)}$ is n.

As an example, consider the situation for $n = 4$, for which $m = 17$. For the generators $g = 3$ and $g = 6$, we have

$$\begin{aligned} \mathcal{W}_A^{(3,1)} &= \{1,2,4,8\}, & \mathcal{W}_A^{(6,1)} &= \{1,2,4,8\}, \\ \mathcal{W}_A^{(3,2)} &= \{1,3,4,5\}, & \mathcal{W}_A^{(6,2)} &= \{1,4,6,7\}, \\ \mathcal{W}_A^{(3,4)} &= \{1,3,7,8\}, & \mathcal{W}_A^{(6,4)} &= \{1,2,5,6\}. \end{aligned}$$

Moreover, for $r = 1$, the weight set $\mathcal{W}_A^{(g,1)}$ is equal to the set of all components of the representative weight $\boldsymbol{w}^{(a)}$ given in Construction A.

Let $\boldsymbol{w}^{(a)}(g,r)$ be the weight vector associated with the weight set $\mathcal{W}_A^{(g,r)}$ for r that divides n.

Theorem 2: For a generator g of $\mathbb{Z}_m^*$ and a divisor r of n where $m = 4n+1$ is prime, $\mathcal{C}(d, \boldsymbol{w}^{(a)}(g,r))$ is a single $(1, g^r)$-cross error correcting integer code.

According to Theorem 2, we can obtain $(1,t)$-cross error correcting codes for a quadratic residue t if $t = g^r$ for a divisor r of n.

Table I shows the values of quadratic residues t that neither Construction A nor A$^+$ can provide single $(1,t)$-cross error correcting codes while one of the constructions gives $(1,t)$-cross error correcting codes for the remaining quadratic residues t not in the table.

In the previous example of $m = 17$, $\mathcal{C}(d, \boldsymbol{w}^{(a)}(3,2))$ and $\mathcal{C}(d, \boldsymbol{w}^{(a)}(3,4))$ are $(1,8)$-cross and $(1,4)$-cross error correcting integer codes, respectively since $3^2 = 8 \pmod{17}$ and $3^4 = 4 \pmod{17}$. Similarly $\mathcal{C}(d, \boldsymbol{w}^{(a)}(2,6))$ is a $(1,2)$-cross error correcting code since $6^2 = 2 \pmod{17}$.

TABLE I

List of Quadratic Residues t Modulo m Except 1 Not Providing $(1,t)$-cross Error Correcting Codes of Length $n \le 28$.

n	m	t
3	13	{3, 4}
4	17	∅
7	29	{4, 5, 6, 7, 9, 13}
9	37	{3, 4, 7, 9, 10, 11, 12, 16}
10	41	{4, 10, 16, 18}
13	53	{4, 6, 7, 9, 10, 11, 13, 15, 16, 17, 24, 25}
15	61	{3, 4, 5, 9, 12, 13, 14, 15, 16, 19, 20, 22, 25, 27}
18	73	{2, 4, 8, 9, 16, 18, 32, 36}
22	89	{2, 4, 8, 11, 16, 22, 25, 32, 39, 44}
24	97	{35, 36}
25	101	{4–6,9,13,14, 16,17,19–25,30,31,33,36,37,43,45,47,49}
27	109	{4,5,7,9,12,15,16,20–22,25–29,31,34–36,38,43,45,46,48,49}
28	113	{4,7,16,28,30,49}

IV. Integer Codes versus OMEC Codes

OMEC codes [5] are linear codes over Gaussian integers which are suited for QAM signal constellations. OMEC codes can correct single errors with distance 1 in a two-dimensional lattice as well as integer codes although the value of t is uniquely determined in case of OMEC codes.

The constellation of an OMEC code is determined by the following modulo function $\mu : \mathbb{Z}[i] \to \mathbb{Z}[i]$ where $\mathbb{Z}[i]$ is the set of Gaussian integers, that is, the set of complex numbers $z = x + i \cdot y$ where x and y are integers:

$$\mu(z) = z - \left[\frac{z \cdot \pi^*}{\pi \cdot \pi^*}\right] \cdot \pi$$

where $\pi = p + i \cdot q$ such that $m = \pi \cdot \pi^* = p^2 + q^2$ for a prime $m = 1 \mod 4$ and $[\cdot]$ denotes rounding of complex numbers, that is, $[z] = [x + i \cdot y] = [x] + i \cdot [y]$ for a complex number $z = x + i \cdot y$.

If $a = \mu(b)$ and $a, b \in \mathbb{Z}_m$, then a is called the residue of b modulo π and we write $a = b \pmod{\pi}$. The set of all possible values of residues $\xi \pmod{\pi}$, where $\xi \in \mathbb{Z}[i]$, determines the constellation of the $[n, n-1, 3]$ OMEC code on the two-dimensional lattice by identifying $x + i \cdot y$ with a point (x, y).

It is easy to verify that the function μ has the following properties:

(D0) $\mu(0) = 0$.
(D1) $\mu(1) = 1$.
(D2) $\mathrm{GCD}(a, m) \neq 1 \quad \Rightarrow \quad \mu(a) = 0$.
(D3) $a = b \pmod{m} \quad \Rightarrow \quad \mu(a) = \mu(b)$.
(D4) $\mu(a \cdot b) = \mu(a) \cdot \mu(b) \pmod{\pi}$.
(D5) $\mu(a + b) = \mu(a) + \mu(b) \pmod{\pi}$.

Properties (D1) to (D4) show that μ is a Dirichlet character modulo m. Using the properties listed above, we can show that

$$\mu(g^n)^2 = \mu(g^{2n}) = \mu(-1) = -\mu(1) = -1.$$

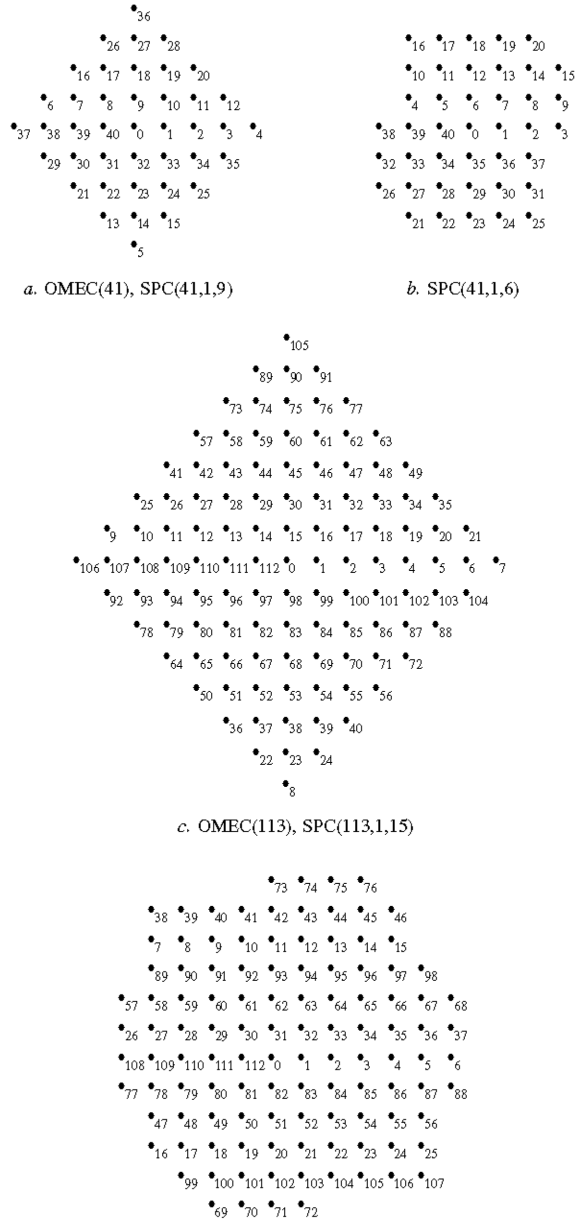
Hence, $\mu(g^n) = i$ or $-i \pmod{\pi}$. This implies that the point associated with g^n is located just above or below the origin on the two-dimensional lattice. Therefore, the constellation of the $[n, n-1, 3]$ OMEC code is given by $\mathrm{SPC}(m, 1, g^n)$. This is illustrated in Fig. 2. In fact, the parity-check matrix $\boldsymbol{H}$ of the $[n, n-1, 3]$ OMEC code is given by

$$\boldsymbol{H} = (\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{n-1})$$

where $\alpha = \mu(g)$ for a generator g of $\mathbb{Z}_m^*$. This matrix uniquely corresponds to the weight vector

$$\boldsymbol{w}^{(a)}(g, n) = (1, g, g^2, \ldots, g^{n-1}).$$

Hence, an $[n, n-1, 3]$ OMEC code is equivalent to a single $(1, g^n)$-cross error correcting code while there are $(1, t)$-cross error correcting integer codes for all $t \in \mathcal{T}$. Fig. 2 indicates that the minimum average symbol energy constellations of integer codes tend to have a rounder shape than OMEC codes as m increases. These constellations are discussed in more detail in [4].



a. OMEC(41), SPC(41,1,9) *b.* SPC(41,1,6)

c. OMEC(113), SPC(113,1,15)

d. SPC(113,1,31)

Fig. 2. Signal point constellations for $m = 41$ and 113.

V. Symbol Error Probability of IC-QAM

In this section, we will first determine the symbol-wise correct decision probability. Next, we will give a definition of the symbol error probability and present a technique to enumerate the number of erroneous symbols. We will use this technique to determine a new upper bound on the average symbol error probability.

Symbol-Wise Correct Decision Probability

Suppose that a signal point $\boldsymbol{x}$ in the constellation $\mathrm{SPC}(m, 1, t)$ of a $(1, t)$-cross error correcting integer code over $\mathbb{Z}_m$ is sent through an AWGN-channel with power spectral density N_0. At the other end a detector estimates the received

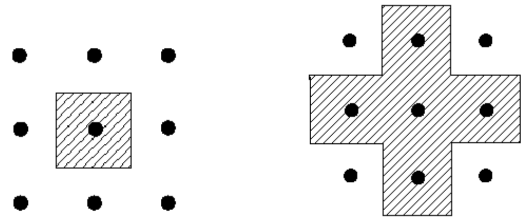


Fig. 3. An example of decision regions in the uncoded case (a) or the coded case (b)

signal $\boldsymbol{r}$ and determines the signal point $\boldsymbol{y}$ that is the nearest to $\boldsymbol{r}$ in SPC$(m, 1, t)$. The received signal $\boldsymbol{r}$ can be written as

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

where $\boldsymbol{e} = (e_1, e_2)$ is the noise vector representing the (quantized) additive noise of the channel.

In case of uncoded QAM, if $\boldsymbol{x} \neq \boldsymbol{y}$, the detector has made a wrong decision. However, if coded QAM based on an integer code is used, then a single erroneous $\boldsymbol{y}$ that is one of four neighbors around $\boldsymbol{x}$ can be corrected.

The decision region of a signal point $\boldsymbol{y}$ is the region of the received points to be decoded to $\boldsymbol{y}$ by either uncoded or coded QAM. Figure 3 (a) illustrates a typical decision region for uncoded QAM. In case of coded QAM, for one of n symbols of a codeword, its decision region is wider than others as shown in Figure 3 (b). In each case, a signal point on the border of the constellation has a wider decision region than other signal points near the center.

Given a constellation, let q_u and q_c be the average probability of a correct decision per signal point for uncoded QAM and coded QAM, respectively. For a square-shaped L^2-QAM over an AWGN channel, Kostadinov et al. [7] obtained

$$\begin{aligned} q_u &= \{1 + (L-1)\,\mathrm{erf}(\gamma)\}^2 / L^2, \\ q_c &= \{2(L-1)(L-2)\,\mathrm{erf}(\gamma)\,\mathrm{erf}(3\gamma) - (L-1)^2\,\mathrm{erf}^2(\gamma) \\ &\quad + 2(L-2)\,\mathrm{erf}(3\gamma) + 2(L-1)\,\mathrm{erf}(\gamma) + 3\} / L^2 \end{aligned}$$

where γ is a constant and $\mathrm{erf}(x)$ is the error function

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-u^2} du.$$

Definition of Symbol Error Probability

Once we obtain q_u and q_c for a given constellation SPC$(m, 1, t)$ associated with an integer code $\mathcal{C}$, we can evaluate the error probability per symbol. Let $X(\boldsymbol{c})$ be the random number of erroneous symbols in the decoded codeword when a codeword $\boldsymbol{c}$ is sent. Let $\mathbb{E}[X(\boldsymbol{c})]$ denote the expectation of $X(\boldsymbol{c})$. The average symbol error probability $P_{SE}(\mathcal{C})$ of the code $\mathcal{C}$ is defined as

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

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

TABLE II
AN UPPER BOUND OF $X(\boldsymbol{c})$ FOR ERROR EVENTS

error event	$X(\boldsymbol{c})$
one $\boldsymbol{r}$ in $\mathcal{D}$ and others in $\mathcal{U}$	0
one $\boldsymbol{r}$ in $\mathcal{D}^c$ and others in $\mathcal{U}$	≤ 2
$\cdots$	$\cdots$
ℓ $\boldsymbol{r}$'s in $\mathcal{U}^c$ and others in $\mathcal{U}$	$\leq \ell + 1$
$\cdots$	$\cdots$
one $\boldsymbol{r}$ in $\mathcal{U}$ and others in $\mathcal{U}^c$, or all $\boldsymbol{r}$'s in $\mathcal{U}^c$	$\leq n$

Enumeration of the Number of Erroneous Symbols

The ith symbol c_i $(1 \leq i \leq n)$ of $\boldsymbol{c} \in \mathcal{C}$ is mapped to a signal point $\boldsymbol{x}_i = \xi^{-1}(c_i)$ in SPC$(m, 1, t)$ where $\xi^{-1}(\cdot)$ is the inverse of the mapping function ξ : SPC$(m, 1, t) \to \mathbb{Z}_m$ which is defined in Section II. Let $\boldsymbol{r}_i$ be the received signal when $\boldsymbol{x}_i$ is transmitted over the channel, and let $\mathcal{U}(\boldsymbol{a})$ and $\mathcal{D}(\boldsymbol{a})$ be the decision region of a signal point $\boldsymbol{a}$ of SPC$(m, 1, t)$ in case of uncoded QAM and coded QAM, respectively.

We can decode $\boldsymbol{x}$ correctly if either of the following two conditions holds:

1) All the received signals $\boldsymbol{r}_i$ $(1 \leq i \leq n)$ 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 may have at most two erroneous symbols. In fact, since we use syndrome decoding, the syndrome may correspond incorrectly to a wrong single error vector.

Moreover, if ℓ signals $\boldsymbol{r}_{k_j}$ $(2 \leq \ell < n, 1 \leq j \leq \ell)$ are out of $\mathcal{U}(\boldsymbol{x}_{k_j})$ and others in $\mathcal{U}(\boldsymbol{x}_i)$ $(i \neq k_j, 1 \leq j \leq \ell)$, then we may have at most $\ell + 1$ erroneous symbols in the decoded codeword $\boldsymbol{y}$. 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 $\mathcal{U}(\boldsymbol{x}_i)$ $(1 \leq i \leq n)$, then all the symbols of the decoded codeword may be erroneous. Our observation described above is summarized in Table II.

An Upper Bound on the Average Symbol Error Probability

Now we approximate the probability that the received signal $\boldsymbol{r}_i$ is in $\mathcal{U}(\boldsymbol{x}_i)$ and $\mathcal{D}(\boldsymbol{x}_i)$ by q_u and q_c, respectively. This means that $X(\boldsymbol{c})$ for $\boldsymbol{c} \in \mathcal{C}$ is replaced by a common random variable X that has the probability distribution based on q_u and q_c. That is, (5) is rewritten as

$$P_{SE}(\mathcal{C}) \approx \frac{1}{n} \mathbb{E}[X]. \tag{6}$$

Moreover, we obtain

$$\begin{aligned} \mathbb{E}[X] \leq\ & 2\binom{n}{1} q_u^{n-1}(1-q_c) + \sum_{\ell=2}^{n-1} (\ell+1) \binom{n}{\ell} (1-q_u)^{\ell} q_u^{n-\ell} \\ & + n\binom{n}{0}(1-q_u)^n. \end{aligned} \tag{7}$$

The right-hand side of (7), denoted by $F(q_u, q_c)$, yields after a simple calculation

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

Hence, (8) can be utilized as an approximation of $P_{SE}(\mathcal{C})$.

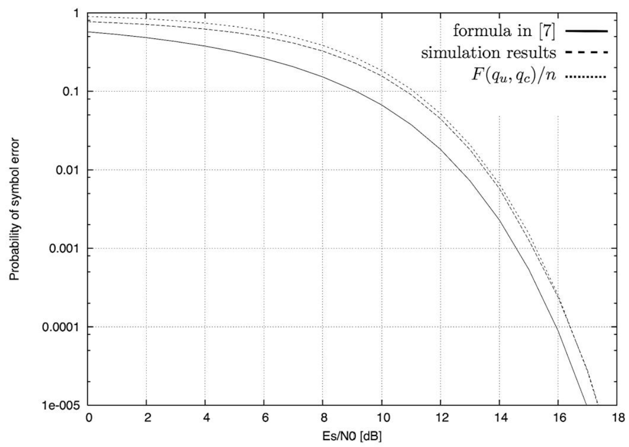


Fig. 4. Comparison between the simulation results of the symbol error probability and the theoretical evaluations.

For example, we can apply an integer code of $m = 17$ to coded 16-QAM [7]. Let $2d$ be the minimum distance between the signal points. Then the average symbol energy E_S of 16-QAM is given by $E_S = 10d^2$. Putting $\gamma = d/\sqrt{N_0}$, we have

$$\gamma = \sqrt{\frac{E_S}{10N_0}}.$$

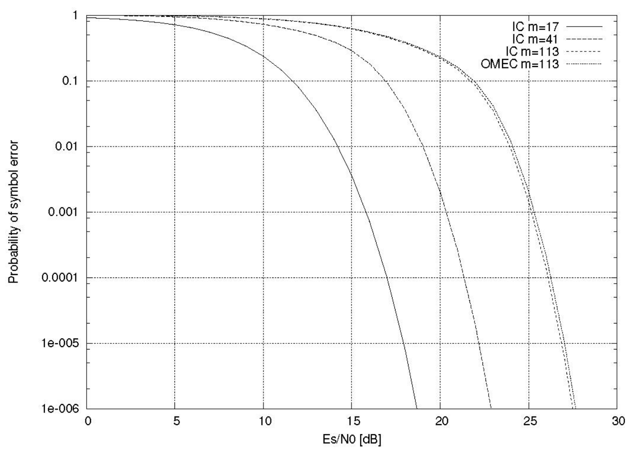


Fig. 5. Evaluation of $P_{SE}(\mathcal{C})$ for $m = 17, 41$, and 113

Since $L = 4$ for 16-QAM, we obtain

$$q_u = \frac{1}{16}\{1 + 3\,\text{erf}(\gamma)\}^2,$$
$$q_c = \frac{1}{16}\{12\,\text{erf}(\gamma)\,\text{erf}(3\gamma) - 9\,\text{erf}^2(\gamma) + \\ +4\,\text{erf}(3\gamma) + 6\,\text{erf}(\gamma) + 3\}.$$

As shown in Figure 4, substituting these values of q_u and q_c into $F(q_u, q_c)/n$ gives an upper bound that is much closer to the simulation results than the formula presented in [7].

We evaluated $P_{SE}(\mathcal{C})$ for integer codes with the minimum average symbol energy constellations of $m = 17, 41, 113$ given in Figures 1 and 2. The results are shown in Figure 5. We also obtained the curves for the OMECs of $m = 17, 41, 113$ by means of computer simulations. The difference is very small for $m = 17$ but it becomes larger as m increases. In case of $m = 113$, at the same level of the symbol error probability, the SNR of the integer codes is 0.2dB lower than that of the OMECs.

VI. Conclusions

We characterized all possible values of t suited to $(1, t)$-cross error correcting integer codes over $\mathbb{Z}_m$ where m is a prime such that $m = 1 \pmod 4$. Moreover, we showed that all the constellations associated with the OMEC codes are obtained by Construction A$^+$. It is important to select the value of t of single $(1, t)$-cross error correcting codes when we minimize the average symbol energy on their constellations. We also discussed the average symbol error probability when an integer code is used with QAM. We obtain a tight upper bound on the symbol error probability by enumerating the number of erroneous symbols.

References

[1] V. I. Levenshtein and A. J. H. Vinck, "Perfect (d, k)-codes capable of correcting single peak-shifts," *IEEE Trans. Inf. Theory*, vol. 39, no. 2, pp. 656–662, Mar. 1993.

[2] U. Tamm, "On perfect integer codes," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Adelaide, Australia, Sept. 2005, pp. 117–120.

[3] A. J. H. Vinck and H. Morita, "Codes over the ring of integers modulo m," *IEICE Trans. Fundamentals*, vol. E81-A, no. 10, pp. 2013–2018, Oct. 1998.

[4] H. Morita, A. J. van Wijngaarden, and A. Geyser, "On the construction of integer codes with minimal signal constellation points," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Seattle, WA, July 2006, pp. 1075–1079.

[5] K. Huber, "Codes over Gaussian integers," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 207–216, Jan. 1994.

[6] ——, "Decoding of icyclic codes for the Mannheim metric," in *Proc. Int'l Symposium on Inform. Theory and its Applications*, Oct. 2004, pp. 1337–1340.

[7] H. Kostadinov, H. Morita, and N. Manev, "Derivation on bit error probability of coded QAM using integer codes," *IEICE Trans. Fundamentals*, vol. E87-A, no. 12, pp. 3397–3403, Dec. 2004.

[8] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed. Oxford, U.K.: Oxford University Press, 1979.