IEICE TRANS. FUNDAMENTALS, VOL.E86–A, NO.7 JULY 2003

PAPER

Integer Codes Correcting Single Errors of Specific Types $(\pm e_1, \pm e_2, \ldots, \pm e_s)$

Hristo KOSTADINOV[†], *Student Member*, **Hiroyoshi MORITA**[†a)], *Regular Member*, *and* **Nikolai MANEV**[††], *Nonmember*

SUMMARY In this paper, we investigate the problem how to construct integer codes capable of correcting any single error in the set $\{\pm 1, \pm t, \ldots, \pm t^{k-1}\}$ and generalize our results to obtain $(\pm e_1, \pm e_2, \ldots, \pm e_s)$ single error correctable codes where e_i's are different elements in $\mathbb{Z}_A$. Moreover, we shall give the exact form of the check matrix in most of the classes considered in this paper.

key words: *integer codes, finite rings, $\mathbb{Z}_A$, multiplicative group*

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 [2], [3]. Some other works on codes over the ring $\mathbb{Z}_A$ of integers modulo A are [4], [6], [8]. M. Nilsson [7] discusses linear block codes over integer rings in order to improve the performance of PSK communication systems. A. Han Vinck, H. Morita [9] and A. Geyser, H. Morita [5] investigated these codes with a view to frame synchronization and coded modulation.

Integer codes are codes defined over finite rings of integers. The original form of integer codes have been found in [1] where an integer code to correct a single insertion/deletion error per codeword was described.

The aim of this paper is to give some classes of single error correctable integer codes. In Sect. 2 we give necessary definitions and notations which we shall use. The advantage of integer codes is that we can correct errors of given type, which means, we can choose the type of the error and after that construct integer code capable of correcting those errors. We show a general construction for $(\pm e_1, \pm e_2, \ldots, \pm e_s)$ single error-correctable integer code. In the case of $(\pm 1, \pm t, \ldots, \pm t^{k-1})$ error type we give the exact form of the check-matrix (which consists only of one column). As one can see from the examples of Theorem 3.1, it is not easy to obtain the check-matrix in general case. These constructions are described in Sect. 3. As it is shown in [9], integer codes constructed in that way can be useful in coded modulation.

In Sect. 4 we show two decoding schemes of integer codes with an example. The first one is with using a look-up table. The second one follows from the construction of the integer code given by Theorem 3.1 in Sect. 3. Both decoding schemes need linear complexity with respect to the codeword length. Conclusion remarks are given in Sect. 5.

Manuscript received June 19, 2002.
Manuscript revised January 20, 2003.
Final manuscript received March 26, 2003.

[†]The authors are with the Graduate School of Information Systems, University of Electro-Communications, Chofu-shi, 182-8585 Japan.
[††]The author is with the Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, Bulgaria.
a) E-mail: morita@is.uec.ac.jp

2. Notations and Definitions

Herein we give only the basic definitions and refer the reader for more details to the above mentioned papers.

Any linear code $\mathcal{C}$ can be represented by a generator matrix or a parity check matrix.

In the latter case, letting $\boldsymbol{H}$ be an $m \times n$ matrix, the subset of $\mathbb{Z}_A^n$ defined by

$$\mathcal{C} = \{\boldsymbol{c} = (c_1, \ldots, c_n) \in \mathbb{Z}_A^n \mid \boldsymbol{c}\boldsymbol{H}^T = \boldsymbol{0}\} \tag{1}$$

is a linear code over $\mathbb{Z}_A$.

Sometimes it is more useful to consider the cosets of $\mathcal{C}$, i.e. to replace $\boldsymbol{0}$ in (1) with a vector $\boldsymbol{d} \in \mathbb{Z}_A^m$.

In this paper we restrict ourselves only with the case $m = 1$, namely with codes, which are defined as follows:

Definition 2.1. [9] *An integer code* of length n with *weight sequence* $\boldsymbol{w} = (w_1, w_2, \ldots, w_n) \in \mathbb{Z}_A^n$, such that $w_j \neq 0$ for $1 \leq j \leq n$, is referred to as a subset of $\mathbb{Z}_A^n$ defined by

$$\mathcal{C}(\boldsymbol{w}, d) = \left\{ \boldsymbol{c} \in \mathbb{Z}_A^n \mid \sum_{i=1}^{n} c_i w_i = d \bmod A \right\} \tag{2}$$

where $d \in \mathbb{Z}_A$.

Let $\mathbb{Z}_A^\star$ be the set of all invertible elements of $\mathbb{Z}_A$, where $x \in \mathbb{Z}_A$ is invertible if there exists $y \in \mathbb{Z}_A$, such that $xy = 1 \bmod A$. It is well known that $\mathbb{Z}_A^\star$ is a multiplicative group, i.e. a group under multiplication. Obviously, $\mathcal{C}(\epsilon\boldsymbol{w}, d) \equiv \epsilon^{-1}\mathcal{C}(\boldsymbol{w}, d)$, for any $\epsilon \in \mathbb{Z}_A^\star$. In the linear case, i.e. $d = 0$, $\mathcal{C}(\boldsymbol{w}, 0) \equiv \epsilon\mathcal{C}(\boldsymbol{w}, 0) \equiv \mathcal{C}(\epsilon\boldsymbol{w}, 0)$, for any $\epsilon \in \mathbb{Z}_A^\star$. Note that the code $\mathcal{C}(\boldsymbol{w}, d)$ may be the empty set for some d in the case $\text{g.c.d}(w_1, w_2, \cdots, w_n) \neq 1$. As far as $a \in \mathbb{Z}_A^\star \iff \text{g.c.d}(a, A) = 1$, the set $\mathcal{C}(\boldsymbol{w}, d)$ is nonempty for all

$d \in \mathbb{Z}_A \iff \text{g.c.d}(w_1, w_2, \cdots, w_n) = 1$. A sufficient condition for this equality to hold is at least one w_j to belong to $\mathbb{Z}_A^\star$. It is easy to see that the cardinality of the set $\mathcal{C}(\boldsymbol{w}, d)$, denoted by $|\mathcal{C}(\boldsymbol{w}, d)|$, is either A^{n-1}, or it is empty. Of course, $|\mathcal{C}(\boldsymbol{w}, 0)| = A^{n-1}$ for any $\boldsymbol{w} \neq 0$.

Assume that a signal point s_i is sent through the channel. At the other end the detector estimates the received signal and gives signal point s_j at the output. If $j \neq i$ the detector has taken a wrong decision but different signal points have different chance to be a result of decision process. The probability the 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 block codes over $\mathbb{Z}_A$ the communication process can be described in the following way. When a codeword $c \in \mathcal{C}(\boldsymbol{w}, d)$ is sent through a noisy channel the received vector can be written in the form

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

where $\boldsymbol{e} = (e_1, \ldots, e_n) \in \mathbb{Z}_A^n$ is so called error vector.

For convenience, let assume that $d = 0$. To decode corrupted codewords, the inner product $< \boldsymbol{r}, \boldsymbol{w} >$ between $\boldsymbol{r}$ and $\boldsymbol{w}$ is calculated:

$$< \boldsymbol{r}, \boldsymbol{w} >= \sum_{i=1}^{n} r_i w_i = \sum_{i=1}^{n} c_i w_i + \sum_{i=1}^{n} e_i w_i = \alpha \bmod A$$

where $\alpha \in \mathbb{Z}_A$. If the syndrome value α is unique for each of the error vectors, i.e., the value of the corresponding error vector is deducted from $\boldsymbol{r}$, then the original codeword is recovered.

Due to aforesaid all elements of $\mathbb{Z}_A$ are not equally probable as a value taken by e_j. 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, this justifies the next definition.

Definition 2.2. [9] The code $\mathcal{C}(\boldsymbol{w}, d)$ is said to be a *single* $(\pm e_1, \pm e_2, \ldots, \pm e_s)$*-error correctable* if it can correct any single error with value $\pm e_i$, $i = 1, \ldots, s$. □

Obviously, $\mathcal{C}(\boldsymbol{w}, d)$ is a single $(\pm e_1, \pm e_2, \ldots, \pm e_s)$-error correctable code if and only if the subsets $\{\pm w_j e_1, \pm w_j e_2, \ldots, \pm w_j e_s\} \subset \mathbb{Z}_A$, are pairwise disjoint and of the same cardinality $2s$, for any $j = 1, 2, \ldots, n$. Thus, we have

$$A \geq 2sn + 1. \tag{3}$$

Definition 2.3. [9] A single $(\pm e_1, \pm e_2, \ldots, \pm e_s)$-error correctable code $\mathcal{C}(\boldsymbol{w}, d)$ of block length n is called *perfect*, when $A = 2sn + 1$.

From Definition 2.3 we notice that if an integer code is perfect there is a one-to-one correspondence between $\mathbb{Z}_A$ and the error vectors. When the code is not perfect we do not have such a correspondence for some of the elements of $\mathbb{Z}_A$. 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. Several Constructions of Codes

The definition of a single $(\pm e_1, \pm e_2, \ldots, \pm e_s)$-error correctable code shows that to construct such a code of block length n is a task which is equivalent to splitting $\mathbb{Z}_A \backslash \{0\} = \{1, 2, 3, \ldots, A-1\}$ into pairwise disjoint subsets each of which contains the subset of the type $\{\pm we_1, \pm we_2, \ldots, \pm we_s\}$ with pairwise different elements. All possible such codes for a given alphabet can be found by an exhausting search but obviously it is neither practically applicable (even for not very large alphabets) nor this fact has a theoretical value. Theorem 3.1 gives one sufficiently general method for such a partitioning of $\mathbb{Z}_A$, i.e. it describes a general construction of a single $(\pm e_1, \pm e_2, \ldots, \pm e_s)$-error correctable code.

Remember that the number of elements of the multiplicative group $\mathbb{Z}_A^\star$ of invertible elements of $\mathbb{Z}_A$ is $|\mathbb{Z}_A^\star| = \varphi(A)$, where $\varphi(A)$ is the Euler's function:

$$\varphi(A) = A \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right), \quad \text{when } A = p_1^{k_1} \cdots p_s^{k_s}.$$

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 3.1. If $e_i e_j^{-1} \notin G$, $e_i, e_j \in \mathbb{Z}_A^\star$ or the integer e_i divides A, but $|e_i G| = 2n$ and $e_i \notin e_j G$, then the code with weight sequence $\boldsymbol{w} = (1, g_2, \cdots, g_n)$ is $(\pm e_1, \pm e_2, \cdots, \pm e_s)$ single error correctable.

Proof: In the first case e_i are different coset representatives of G in $\mathbb{Z}_A^\star$:

$$\begin{aligned}
e_1 G &= \{e_1, e_1 g_2, \cdots, e_1 g_n, -e_1, -e_1 g_2, \cdots, -e_1 g_n\} \\
e_2 G &= \{e_2, e_2 g_2, \cdots, e_2 g_n, -e_2, -e_2 g_2, \cdots, -e_2 g_n\} \\
&\vdots \qquad\qquad\qquad \vdots \\
e_s G &= \{e_s, e_s g_2, \cdots, e_s g_n, -e_s, -e_s g_2, \cdots, -e_s g_n\}.
\end{aligned}$$

Hence, all $e_i G$ are pairwise disjoint. If e divides A, (denoted by $e|A$) but $|eG| = 2n$, then the subset eG consists of $2n$ different elements and has an empty intersection with other $e_i G$, $e_i \in \mathbb{Z}_A^\star$. □

Let note the following duality. If $\mathcal{C}$ is a $(\pm e_1, \pm e_2, \cdots, \pm e_s)$ single error correctable code with weight sequences $\boldsymbol{w} = (w_1, w_2, \ldots, w_n)$, then the integer code with weight sequences $(e_1, e_2, \ldots, e_s)$ is a $(\pm w_1, \pm w_2, \cdots, \pm w_n)$ single error correctable code. Therefore, taking the dual in the aforesaid sense of a code constructed by Theorem 3.1 we obtain a code with weight sequence not all of whose elements belong to $\mathbb{Z}_A^\star$.

Example 3.1: Let $A = p$ be a prime number, $p > 2$. $\mathbb{Z}_p^\star = \mathbb{Z}_p \setminus \{0\} \Rightarrow |\mathbb{Z}_p^\star| = p - 1 = 2ns$ and $\mathbb{Z}_p^\star = \cup_{i=1}^{s-1} t^i G$, where $|G| = 2n$. Note that $\mathbb{Z}_p^\star$ is a cyclic group and a unique subgroup G with $|G| = 2n$ exists.

Note that we can choose any element from $t^i G$ as

an error value, not necessarily $1, t, t^2, \ldots, t^{s-1}$.

Example 3.2: Let $A = 2p$, where p is an odd prime number. Then

$$\mathbb{Z}_{2p}^{\star} = \{1, 3, 5, \cdots, 2p-1\} \setminus \{p\},\ |\mathbb{Z}_{2p}^{\star}| = p - 1.$$

Let $p - 1 = 2ns$ and G be a subgroup of $\mathbb{Z}_{2p}^{\star}$ with $|G| = 2n$. Then

$$\begin{aligned}\mathbb{Z}_{2p}^{\star} &= e_1 G \cup e_2 G \cup \cdots \cup e_s G,\\ G &= \{1, g_2, \cdots, g_n, -1, -g_2, \cdots, -g_n\}.\end{aligned}$$

The code with $\boldsymbol{w} = (1, g_2, \cdots, g_n)$ can correct single $(\pm e_1, \pm e_2, \cdots, \pm e_s, \pm 2e_1, \pm 2e_2 \cdots, \pm 2e_s)$ error since

$$\begin{aligned}&2e_1 G \cup \cdots \cup 2e_s G = \{2, 4, \cdots, 2p-1\},\\ &2e_i G \neq e_j G.\end{aligned}$$

Also $4sn = 2(p-1)$, i.e., $A = 2(2s)n + 2$. Therefore, the code is "almost" perfect.

To construct a perfect code, we should have $n = \frac{p-1}{2}$ and $\boldsymbol{w} = (1, g_2, \cdots, g_{\frac{p-1}{2}}, p)$. The code can correct $\pm 1, \pm 2l$ in all positions except when ± 2 occurs in the last position. In this case the decoder will decide that there is no error.

Example 3.3: Let $A = pq$, where p and q are prime and $p > q > 2$. Then $|\mathbb{Z}_A^{\star}| = |\mathbb{Z}_{pq}^{\star}| = (p-1)(q-1)$, $|\mathbb{Z}_{pq}^{\star}| = \mathbb{Z}_{pq} \setminus \{kp, lq\}$. $\mathbb{Z}_{pq}^{\star}$ is not cyclic.

Let H, $|H| = p - 1$ be a subgroup of $\mathbb{Z}_{pq}^{\star}$ and $\mathbb{Z}_{pq}^{\star} = \cup_{i=1}^{q-1} a_i H$. Let $p - 1 = 2ns$, G be a subgroup of H and $H = b_1 G \cup \cdots \cup b_s G$, where $G = \{1, g_2, \cdots, g_n, -1, -g_2, \cdots, -g_n\}$.

Then for $\mathbb{Z}_{pq}^{\star}$ we have:

$$\begin{aligned}\mathbb{Z}_{pq}^{\star} = {} & a_1 b_1 G \cup \cdots \cup a_1 b_s G \cup \cdots \cup a_{q-1} b_1 G \cup\\ & \cdots \cup a_{q-1} b_s G\end{aligned}$$

On other hand $qb_1 G \cup qb_2 G \cup \cdots \cup qb_s G \equiv qH \equiv \{q, 2q, \cdots, (p-1)q\}$ which differs from $\mathbb{Z}_{pq}^{\star}$.

Therefore, the code with $w = (1, g_2, \cdots, g_n)$ corrects any single $(\pm a_i b_j, \pm q b_j)$ error, $i = 1, \cdots, q-1, j = 1, \cdots, s$, and

$$\begin{aligned}1 + [2ns(q-1) + 2ns] &= 1 + 2nsq = 1 + q(p-1)\\ &= A - (q-1).\end{aligned}$$

Thus the exceeding of the alphabet is $(q-1)$.

Example 3.4: $A = p^k$, where p is an odd prime. $|\mathbb{Z}_{p^k}^{\star}| = p^{k-1}(p-1)$ and $\mathbb{Z}_{p^k}^{\star} = \mathbb{Z}_{p^k} \setminus \{lp\}$, where $l = 0, 1, \ldots, p^{k-1} - 1$. Let H be a subgroup, where $|H| = p - 1$. Note that $\mathbb{Z}_{p^k}^{\star}$ is a cyclic and there is a unique subgroup of any cardinality dividing $p^{k-1}(p-1)$.

Let $\mathbb{Z}_{p^k}^{\star} = a_1 H \cup a_2 H \cup \cdots \cup a_{p^{k-1}} H$ and $G \subset H$ with $|G| = 2n$, where $p - 1 = 2ns$. Then $H = b_1 G \cup \cdots \cup b_s G$. (Of course the case $n > 1$, i.e., $s < (p-1)/2$, is interesting.)

Then the subsets of $\mathbb{Z}_{p^k}$:

$$\begin{aligned}&a_i b_j G,\ pb_j G,\ p^2 b_j G, \cdots, p^{k-1} b_j G,\\ &\quad i = 1, \cdots, p^{k-1},\\ &\quad j = 1, \cdots, s\end{aligned}$$

are disjoint.

If $G = \{1, g_2, \cdots, g_n, -1, -g_2, \cdots, -g_n\}$ the code with $w = (1, g_2, \cdots, g_n)$ can correct single $(\pm a_i b_j, \pm p^l b^j)$, $l = 1, \cdots, k-1, j = 1, \cdots, s, i = 1, \cdots, p^{k-1}$ error. And we have

$$\begin{aligned}&1 + 2snp^{k-1} + 2(k-1)sn\\ &\quad = A - [p^{k-1} - (k-1)p + k - 2].\end{aligned}$$

Therefore, the exceeding of the bound is $p^{k-1} - (k-1)p + k - 2$. When $k = 2$ the code is perfect.

Theorem 3.2. Let $A = t^k + 1$. The integer code over $\mathbb{Z}_A$ with a weight sequence consisting of the elements of the set $\boldsymbol{W} = \{a_0 t^{k-1} + a_1 t^{k-2} + \cdots + a_{k-1}\}$, satisfying

$$\left|\begin{array}{rl} 0 \le a_0 \le & \lfloor \frac{t-2}{2} \rfloor\\ a_0 \le a_1 \le & t - 2 - a_0\\ \min\{1 + a_0, a_1\} \le a_2 \le & t - 1 - a_0\\ \vdots & \\ \min\{1 + a_0, a_{k-3}\} \le a_{k-2} \le & t - 1 - a_0\\ 1 + a_0 \le a_{k-1} \le & t - 1 - a_0 \end{array}\right. \tag{4}$$

is single $(\pm 1, \pm t, \ldots, \pm t^{k-1})$-error correctable. Moreover, the length of the code is given by

$$n = \sum_{a=0}^{\lfloor \frac{t-2}{2} \rfloor} \frac{(t-1-2a)^{k-2} - (t-1-2a)}{t-2-2a} + \sum_{a=0}^{\lfloor \frac{t-2}{2} \rfloor} (t-1-2a)^{k-1} \tag{5}$$

Proof: Any element w of $\boldsymbol{W}$ satisfies the inequality

$$\begin{aligned}w \le {} & \left\lfloor \frac{t-2}{2} \right\rfloor t^{k-1} + (t-2)t^{k-2} + (t-1)t^{k-3}\\ & + \ldots + (t-1) = \left\lfloor \frac{t}{2} \right\rfloor t^{k-1} - t^{k-2} - 1 < \frac{t^k}{2}.\end{aligned}$$

Hence, $A - w > t^k/2 + 1$, which shows $(-w = A - w \in \mathbb{Z}_A)$ that

$$\boldsymbol{W} \cap (-W) = \emptyset. \tag{6}$$

Let us consider the set $t\boldsymbol{W} = \{tw \mid w \in \boldsymbol{W}\}$. Keeping in mind that $t^k = -1$ in $\mathbb{Z}_A$ we can write

$$\begin{aligned}t\boldsymbol{W} &= \{a_1 t^{k-1} + \cdots + a_{k-2} t^2 + (a_{k-1} - 1)t + (t - a_0)\}\\ &= \{a_0' t^{k-1} + a_1' t^{k-2} + \cdots + a_{k-1}'\}\end{aligned}$$

where $0 \le a_j \le t - 1$.

Let assume that $t\boldsymbol{W} \cap \boldsymbol{W} \neq \emptyset$. Then using (4) for the set $t\boldsymbol{W}$ we have

$$t - a_0 = a_{k-1}' \le t - 1 - a_0' = t - 1 - a_1.$$

Thus $a_0 \ge a_1 + 1 > a_1$ which contradicts to $a_0 \le a_1$ in

(4). Therefore

$$t\,\boldsymbol{W} \cap \boldsymbol{W} = \emptyset. \tag{7}$$

Now for $j = 2, 3, \ldots, k-2$ we have

$$\begin{aligned} t^j\,\boldsymbol{W} =& \{a_j t^{k-1} + \cdots + (a_{k-1}-1)t^j + (t-a_0-1)t^{j-1} \\ &+ (t-a_1-1)\,t^{j-2} + \cdots + (t-a_{j-2}-1)t + (t-a_{j-1})\} \\ =& \{a'_0 t^{k-1} + a'_1 t^{k-2} + \cdots + a'_{k-1}\}. \end{aligned}$$

If we assume $t^j\,\boldsymbol{W} \cap \boldsymbol{W} \neq \emptyset$, again using (4) but this time for the set $t^j\,\boldsymbol{W}$ we obtain the following inequalities

$$t - a_0 - 1 = a'_{k-j} \leq t - 1 - a'_0 = t - 1 - a_j \tag{8}$$

and

$$t - a_{j-1} = a'_{k-1} \leq t - 1 - a_j. \tag{9}$$

From (8) and (9) it follows $a_0 \geq a_j$ and $a_{j-1} \geq 1 + a_j$. But $a_j \geq \min\{a_{j-1}, 1 + a_0\}$ that implies

$$a_0 \geq \min\{a_{j-1}, 1 + a_0\} \Rightarrow \min\{a_{j-1}, 1 + a_0\} = a_{j-1}.$$

Hence, $a_j \geq a_{j-1} \geq 1 + a_j$ which results the contradiction. Thus, we have

$$t^j\,\boldsymbol{W} \cap \boldsymbol{W} = \emptyset \quad j = 2, 3, \cdots, k-2. \tag{10}$$

Since

$$\begin{aligned} t^{k-1}\,\boldsymbol{W} =& \{(a_{k-1}-1)t^{k-1} + (t-a_0-1)t^{k-2} \\ &+ \cdots + (t-a_{k-3}-1)t + (t-a_{k-2})\}, \end{aligned}$$

the assumption $t^{k-1}\,\boldsymbol{W} \cap \boldsymbol{W} \neq \emptyset$ gives

$$t - a_0 - 1 = a'_1 \leq t - 2 - a'_0 = t - 2 - a_{k-1} + 1.$$

Then $a_0 \geq a_{k-1}$. But this contradicts to $a_{k-1} \geq 1 + a_0$ in (4). Hence we obtain

$$t^{k-1}\,\boldsymbol{W} \cap \boldsymbol{W} = \emptyset. \tag{11}$$

Taking in account that $t^k = -1$ and t is invertible in $\mathbb{Z}_A$, (6), (7),(10), and (11) give

$$t^i\,\boldsymbol{W} \cap \pm t^j\,\boldsymbol{W} = \emptyset, \quad i, j = 1, 2, \ldots, k-1$$

that proves the first part of the theorem.

Note the set $\boldsymbol{W}$ coincides with $\bigcup_{j=1}^{k-1} \boldsymbol{W}_j$, where $\boldsymbol{W}_1 = \{a_0 t^{k-1} + a_1 t^{k-2} + \cdots + a_{k-1}\}$ satisfying

$$\left|\begin{array}{rl} 0 \leq a_0 \leq & \lfloor \frac{t-2}{2} \rfloor \\ 1 + a_0 \leq a_1 \leq & t - 2 - a_0 \\ 1 + a_0 \leq a_2 \leq & t - 1 - a_0 \\ \multicolumn{2}{c}{\vdots} \\ \multicolumn{2}{l}{1 + a_0 \leq a_{k-1} \leq t - 1 - a_0} \end{array}\right. \tag{12}$$

and for $j = 2, \ldots k-1$ $\boldsymbol{W}_j = \{a_0 t^{k-1} + a_1 t^{k-2} + \cdots + a_{k-1}\}$ satisfying

$$\left|\begin{array}{rl} 0 \leq a_0 \leq & \lfloor \frac{t-2}{2} \rfloor \\ a_0 = a_1 = & \cdots = a_{j-1} \\ 1 + a_0 \leq a_j \leq & t - 1 - a_0 \\ \multicolumn{2}{c}{\vdots} \\ \multicolumn{2}{l}{1 + a_0 \leq a_{k-1} \leq t - 1 - a_0.} \end{array}\right. \tag{13}$$

For any a_0 we have

$$\begin{aligned} |\,\boldsymbol{W}_1(a_0)| &= (t - 2 - 2a_0)(t - 1 - 2a_0)^{k-2} \\ &= (t - 1 - 2a_0)^{k-1} - (t - 1 - 2a_0)^{k-2} \end{aligned}$$

(for $k = 2$ the value is $\sum_{a=0}^{\lfloor \frac{t-2}{2} \rfloor}(t - 1 - 2a)$).
Hence

$$|\,\boldsymbol{W}_1| = \sum_{a=0}^{\lfloor \frac{t-2}{2} \rfloor} [(t - 1 - 2a)^{k-1} - (t - 1 - 2a)^{k-2}].$$

For $j = 2, 3, \ldots, k-1$ we have

$$|\,\boldsymbol{W}_j| = \sum_{a=0}^{\lfloor \frac{t-2}{2} \rfloor} (t - 1 - 2a)^{k-j}.$$

Therefore, (5) follows from the equality

$$n = |\,\boldsymbol{W}| = \sum_{j=1}^{k-1} |\,\boldsymbol{W}_j|. \qquad \square$$

Obviously, the codes given by Theorem 3.2 do not exhaust all possible single-error correcting codes but the theorem gives an easy way to construct such codes. Using "duality" property one can enlarge the set of codes obtained by Theorem 3.2. For example, the code with $t = 4$, $k = 3$ (i.e. $A = 65 = 13 \cdot 5$) can be obtained also as a "dual" of a code using the construction described in Example 3.3. But this approach is more difficult than the other shown in Theorem 3.2.

For $k = 2$, Theorem 3.2 gives Theorem 2 of [5]. For $k = 3$ and $k = 4$, we have the following corollaries.

Corollary 3.3 Let $A = t^3 + 1$. The integer code over $\mathbb{Z}_A$ with a weight sequence $\boldsymbol{W} = \{a_0 t^2 + a_1 t + a_2\}$, where the coefficients a_j satisfy

$$\left|\begin{array}{rl} 0 \leq a_0 \leq & \lfloor \frac{t-2}{2} \rfloor \\ a_0 \leq a_1 \leq & t - 2 - a_0 \\ 1 + a_0 \leq a_2 \leq & t - 1 - a_0 \end{array}\right.$$

is a single $(\pm 1, \pm t, \pm t^2)-$error correctable code of block length

$$n = \frac{1}{6}(t^3 - t). \tag{14}$$

The exceeding of the alphabet is t. $\square$

Remark: The same result holds for $A = t^3 - 1$. But the exceeding of the alphabet is $t - 2$.

Corollary 3.4 Let $A = t^4 + 1$. The integer code over $\mathbb{Z}_A$ with a weight sequence $\boldsymbol{W} = \{a_0 t^3 + a_1 t^2 +$

Table 1

t	k	A	$\boldsymbol{w}$
4	2	17	1, 2, 3, 6
	3	65	1, 2, 3, 5, 6, 7, 9, 10, 11, 22
5	2	26	1, 2, 3, 4, 7, 8
6	2	37	1, 2, 3, 4, 5, 8, 9, 10, 15

$a_2t+a_3\}$, where the coefficients a_j satisfy (4), is a single $(\pm 1, \pm t, \pm t^2, \pm t^3)$−error correctable code of block length

$$n = \begin{cases} \dfrac{t^4}{8}, & t = 2l \\ \dfrac{t^4-1}{8}, & t = 2l+1. \end{cases} \tag{15}$$

The code is perfect when t is even and almost perfect (the exceeding of the alphabet is equal to 1) when t is odd. □

Remark: Similar result holds for $A = t^4 - 1$. But the exceeding of the alphabet is different.

In Table 1, using Theorem 3.2 we give the weight sequence $\boldsymbol{w}$ for several cases:

In case of $k = 5$, the set $\boldsymbol{W}$ defined by (4) is not a complete set of coset representatives of $\{\pm 1, \pm t, \pm t^2, \pm t^3, \pm t^4\}$, i.e. the value n defined by (5) is not the maximum possible. Another set, $\boldsymbol{E}$, of coset representatives is defined as follows:

$$\boldsymbol{E} = \left\{a_0t^4 + a_1t^3 + a_2t^2 + a_3t + a_4\right\}$$

where

$$\begin{vmatrix} 0 & \le a_0 \le & \lfloor \frac{t-3}{2} \rfloor, \ a_1 = t-1-a_0 \\ 1+a_0 & \le a_2 \le & t-2-a_0, \ a_3 = t-1-a_0 \\ 1+a_0 & \le a_4 \le & t-1-a_0. \end{vmatrix} \tag{16}$$

The relation $\boldsymbol{E} \cap \boldsymbol{W} = \emptyset$ is an implication from the equality $a_1 = t - 1 - a_0$.

Theorem 3.5. Let $A = t^5 + 1$. The integer code over $\mathbb{Z}_A$ with a weight sequence $\boldsymbol{W} \cup \boldsymbol{E}$ is single $(\pm 1, \pm t, \ldots, \pm t^4)$−error correctable and it has block length

$$n = \frac{1}{10}(t^5 - t). \tag{17}$$

Proof: For any $x \in \boldsymbol{E}$,

$$x = a_0t^4 + a_1t^3 + a_2t^2 + a_3t + a_4 < t^5/2.$$

Thus, we have

$$\boldsymbol{E} \cap (-\boldsymbol{E}) = \boldsymbol{E} \cap (-\boldsymbol{W}) = \emptyset. \tag{18}$$

Since $t - 1 - a_0 > \lfloor \frac{t-2}{2} \rfloor$, it is easy to see

$$t\boldsymbol{E} \cap \boldsymbol{W} = \emptyset. \tag{19}$$

If we assume $t\boldsymbol{E} \cap (-\boldsymbol{W}) \neq \emptyset$ then we have $a_0 = a_2' \ge \min\{a_1', 1+a_0'\} = \min\{t-1-a_2, 1+a_0\}$. Hence $1+a_0 > t-1-a_2$, i.e. $a_2 > t-2-a_0$, which contradicts (16).

Thus

$$t\boldsymbol{E} \cap (-\boldsymbol{W}) = \emptyset. \tag{20}$$

Also, just looking at (16) one can see that

$$t\boldsymbol{E} \cap (\pm\boldsymbol{E}) = \emptyset. \tag{21}$$

Now, let us consider $t^2\boldsymbol{E} = \{a_2t^4 + (t-1-a_0)t^3 + (a_4-1)t^2 + (t-1-a_0)t + (a_0+1)\}$. The assumption $t^2\boldsymbol{E} \cap \boldsymbol{E} \neq \emptyset$ leads to $1 + a_0 = a_4' \ge 1 + a_0' = 1 + a_2 > 2 + a_0$, which is a contradiction. Hence,

$$t^2\boldsymbol{E} \cap \boldsymbol{E} = \emptyset. \tag{22}$$

In a similar manner, one can obtain that

$$t^2\boldsymbol{E} \cap \boldsymbol{W} = \emptyset. \tag{23}$$

Moreover, we have:

$$\begin{aligned} t^3\boldsymbol{E} \cap \boldsymbol{W} &= t^3\boldsymbol{E} \cap \boldsymbol{E} = \emptyset, t^4\boldsymbol{E} \cap \boldsymbol{E} \\ &= t^4\boldsymbol{E} \cap \boldsymbol{W} = \emptyset. \end{aligned} \tag{24}$$

Therefore, similar arguments in Theorem 3.2 based on (18) to (24) complete the first part of the proof.

Now let us calculate the length of the code, i.e. the cardinality $|\boldsymbol{W} \cup \boldsymbol{E}|$. Hence we have

$$\begin{aligned} n &= |\boldsymbol{W}| + |\boldsymbol{E}| = \\ &= \begin{cases} \displaystyle\sum_{m=1}^{l} (2m)^4 + 2\sum_{m=1}^{l} (2m)^2, & t = 2l+1 \\ \displaystyle\sum_{m=2}^{l} (2m-1)^4 + 2\sum_{m=2}^{l} (2m-1)^2, & t = 2l \end{cases} \end{aligned}$$

where $m = l - a$.

In both cases we have

$$n = \frac{1}{10}(t^5 - t).$$

Therefore the exceeding of the alphabet is t, since

$$2kn + 1 = 2 \cdot 5 \cdot \frac{1}{10}(t^5 - t) + 1 = t^5 - t + 1 = A - t.$$

□

Analogously to Theorem 3.2 one can also prove the following theorem.

Theorem 3.6. Let $A = t^2 + t + 1$ where $t = 3k$ or $t = 3k - 1, k > 1$. The integer code over $\mathbb{Z}_A$ with a weight sequence consisting of the elements of the set

$$\boldsymbol{W} = \{w | w = a_0t + a_1\}$$

where

$$0 \le a_0 \le \left\lfloor \frac{t-1}{3} \right\rfloor, \ 2a_0 + 1 \le a_1 \le t - 1 - a_0 \tag{25}$$

is perfect and single $(\pm 1, \pm t, \pm(t+1))$-error correctable.

4. Two Decoding Algorithms

Herein, we will discuss how to decode a single $(\pm e_1, \pm e_2, \ldots, \pm e_s)$-error correctable code $\mathcal{C}(\boldsymbol{w}, 0)$ where any $e_i \in \mathbb{Z}_A^\star$. Let $\mathcal{E}$ be the set of all possible error vectors $\boldsymbol{e}$ to be correctable by $\mathcal{C}(\boldsymbol{w}, 0)$. That is, each $\boldsymbol{e} \in \mathcal{E}$ consists of all zeroes but one element in $E = \{\pm e_1, \pm e_2, \ldots, \pm e_s\}$. To decode a corrupted codeword $\boldsymbol{r}$, the simplest way is to use a look-up table which maps each syndrome value $\alpha =< \boldsymbol{r}, \boldsymbol{w} >$ to the corresponding error vector. For example, in case of a $(\pm 1, \pm t, \cdots, \pm t^{k-1})$ single error-correctable integer code with $t = 4, k = 2$, and $A = t^k + 1 = 17$, the weight sequence of $\mathcal{C}(\boldsymbol{w}, 0)$ is given as $\boldsymbol{w} = (1, 2, 3, 6)$ and we have the look-up table in Table 2. It is noted that the cost of obtaining α is proportional to the codeword length n and the size of the table is $A - 1 = 2sn$.

If the size of A is large, it is not always reasonable to build such a table because of memory limitation. In that case, we have an alternative as follows: In advance, we calculate the inverses e_i^{-1} for all possible errors. Then, we get all values $\pm\alpha e_i^{-1}$ for the syndrome $\alpha =< \boldsymbol{r}, \boldsymbol{w} >$ obtained from the received $\boldsymbol{r}$. If a single error $e \in E$ occurs at the position j in the codeword and no errors at other positions, then $\alpha e^{-1} = w_j$. Besides, no other product $\pm\alpha e_i^{-1}$ take any values in $\{w_1, w_2, \ldots, w_n\}$. Otherwise, we would have two different error vectors $\boldsymbol{e}$ and $\boldsymbol{e}'$ in $\mathcal{E}$ such that $< \boldsymbol{e}, \boldsymbol{w} >=< \boldsymbol{e}', \boldsymbol{w} >= \alpha$ which contradicts to the correctability of $\mathcal{C}(\boldsymbol{w}, 0)$. Therefore the error e has occurred in the jth component of $\boldsymbol{r}$. For example, for the same code considered above, if we received $\boldsymbol{r} = (6, 2, 0, 2)$, then $\alpha = 5$. Since $E^{-1} = \{\pm 1, \pm 13\}$, we have $\alpha E^{-1} = \{\pm 5, \pm 14\}$ mod 17. Only $-14 = 3$ mod 17 belongs to $\boldsymbol{w}$. Therefore, the error -4 has occurred at the third position, i.e. the error vector is $(0, 0, -4, 0)$ and the vector $(6, 2, 4, 2)$ has been sent. This decoding procedure needs calculations proportional to the codeword length n for each corrupted codeword $\boldsymbol{r}$. As a remark, we see that if $2s < \log_2 n$, a binary search algorithm finds out which element of αE^{-1} is in $\boldsymbol{w}$ with $\log_2 n$ comparisons.

No matter which using the look-up table or calculating αE^{-1} will be done, the complexity of the decoding procedure would have the linear complexity with respect to the codeword length.

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

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

5. Conclusions

In this paper we proposed a general construction for single $(\pm e_1, \pm e_2, \cdots, \pm e_s)$-error correctable codes. In a specific case when $(\pm e_1, \pm e_2, \cdots, \pm e_s) = (\pm 1, \pm t, \cdots, \pm t^{k-1})$ we showed the exact form of the check-matrix. We presented two decoding schemes of integer codes capable of correcting single error with an example. The first one is with using a look-up table. The second one follows from the construction of the integer code given by Theorem 3.1. Both decoding schemes need linear complexity with respect to the codeword length.

The construction of integer codes capable of correcting multiple errors of given types is much more complicated. Here, the weight sequence $\boldsymbol{w}$ will have a matrix form (not a vector as it is in case of a single error) and it is difficult to give its exact form. The number of all possible error vectors of a given type is a polynomial function as well. Examples of integer codes capable of correcting more than one error are given in [9]. Our next step in this study will be to construct integer codes capable of correcting multiple errors.

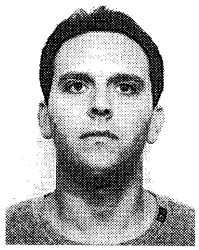
Acknowledgement

This work was partially supported by Grant I-803/98 of the Bulgarian NSF.

References

[1] 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.
[2] I. Blake, "Codes over certain rings," Inf. Control, vol.20, pp.396–404, 1972.
[3] I. Blake, "Codes over integer residue rings," Inf. Control, vol.29, pp.295–300, 1975.
[4] 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.
[5] A. Geyser and H. Morita, "Performance of integer coded modulation over Rayleigh fading channels," Proc. 22nd SITA, pp.745–748, Yuzawa, Japan, Nov./Dec. 1999.
[6] 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.
[7] M. Nilsson, Linear block codes over rings for phase shift keying, Thesis no.331, Linköping University, 1993.
[8] E. Spiegel, "Codes over Z_m," Inf. Control, vol.35, pp.48–51, 1977.

[9] A.J. Han Vink and Hiroyoshi Morita, "Codes over rings of integer modulo m," IEICE Trans. Fundamentals, vol.E81-A, no.10, pp.2013–2018, Oct. 1998.



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. Since April 2002, he is a Ph.D. student at the University of Electro-Communications, Tokyo, Japan. 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 Associate 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

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.