On coded modulation based on finite rings of integers

Hristo KOSTADINOV
Graduate School of Inf. Systems
Univ. of Electro-Comm.
1-5-1 Chofugaoka, Chofu-shi
Tokyo 182-8585, Japan
e-mail: hristo@math-sys.is.uec.ac.jp

Hiroyoshi MORITA
Graduate School of Inf. Systems
Univ. of Electro-Comm.
1-5-1 Chofugaoka, Chofu-shi
Tokyo 182-8585, Japan
e-mail: morita@is.uec.ac.jp

Nikolai MANEV
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
8 Acad. G Bonchev Str.
1113 Sofia, Bulgaria
e-mail: nlmanev@moi.math.bas.bg

Abstract — **In this paper, we investigate the problem how to use codes over $\mathbb{Z}_A$ to correct any single error which belongs to the set $\{\pm e_1, \pm e_2, \dots, \pm e_s\}$, where e_i's are different elements in $\mathbb{Z}_A$. We present some classes of such codes and describe how they can be applied to M-QAM.**

Codes over finite rings and in particular codes over finite rings of integers have been studied in numerous papers. The earliest papers are due to Varshamov and Tenengolz [1]. Later many authors have investigated these codes and proposed numerous applications. Some of the authors are I. Blake, Spiegel, Calderbank and Sloane, Nilsson, Baldini and Farrell, etc.

In this paper we restrict ourselves only with the case of codes generated by a matrix of rank 1, namely with codes, which are defined as follows:

Definition. [2] *An integer code of length n with weight sequence* $w = (w_1, w_2, \dots, w_n) \in \mathbb{Z}_A^n$, such that $w_j \neq 0$ for $1 \leq j \leq n$, is given as a subset of $\mathbb{Z}_A^n$ defined by

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

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

If the signal points of the constellation implemented in a given communication system are indexed by elements of $\mathbb{Z}_A$, the integer codes can be used to improved its performance. The aim of this paper is to give some examples of such an use.

It is well known that signal points are not equally probable as a result of the decision process. The probability that the signal point s_j appears at the output of the detector depends on the Euclidean distance between s_j and really-sent signal s_i. Therefore, the indexing of signal points by the elements of $\mathbb{Z}_A$ make these elements not equal probable as a value of a position in the error vector. Thus, the aforesaid justifies the next definition.

Definition. [2] The code $C(w,d)$ is said to be a *single* $\{\pm e_1, \pm e_2, \dots, \pm e_s\}$*-error correctable* if it can correct any single error vector $(0, \dots, 0, e_i, 0, \dots, 0)$ with value $\pm e_i$ in position k, where $1 \leq i \leq s$, $1 \leq k \leq n$.

We present several general constructions of single error correctable codes. The next theorem gives an idea for the obtained results.

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

$$\left| \begin{array}{rcl} 0 & \leq a_0 \leq & \lfloor \frac{t-2}{2} \rfloor \\ a_0 & \leq a_1 \leq & t-2-a_0 \\ \min\{1+a_0, a_1\} & \leq a_2 \leq & t-1-a_0 \\ \cdot & \cdot & \cdot \\ \min\{1+a_0, a_{k-3}\} & \leq a_{k-2} \leq & t-1-a_0 \\ 1+a_0 & \leq a_{k-1} \leq & t-1-a_0 \end{array} \right.$$

is single $\{\pm 1, \pm t, \dots, \pm t^{k-1}\}$-error correctable.

These general results enable numerous classes of codes to be constructed. The complexity of the decoding procedure is linear with respect to the codeword length.

We calculate the BER for M-QAM scheme where an integer block code capable to correct up to t errors of given type is applied. Based on the results given above many concrete QAM schemes and codes are considered. In all cases, the improvement of the performance is not worse than one when trellis coded modulation is used. Simultaneously, the decoding algorithm is relatively simple for implementation. For example, a 32-QAM constellation indexed by the elements of $\mathbb{Z}_{32}$ is shown in Fig. 1. The code used in this case is with the weight sequence $w = (1, 15)$, which is $\{\pm 1, \pm 3, \pm 5, \pm 7\}$-error correctable.

Fig. 2 shows the coding gain in the case of 256-QAM when we map any signal point into a pair of elements of $\mathbb{Z}_{16}$ and use a code over $\mathbb{Z}_{16}$.

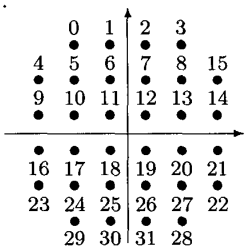

Fig. 1: A 32-QAM signal space constellation

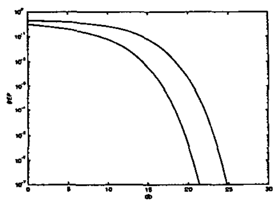

Fig. 2: A comparison of the bit error probability (BEP) versus signal-to-noise ratio (db) between uncoded (upper curve) and coded 256-QAM with a code with length $n = 2$.

[2]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] A.J. Han Vink and Hiroyoshi Morita, "Codes over rings of integer modulo m," *IEICE Trans. Fundamentals*, vol.E81-A, No. 10, Oct. 1998.