Error-Correcting Codes for QAM from Integer Rings of an Euclidean Complex Quadratic Field[1]

Josep Rifà
Dept. of Computer Sciences
Autonomous University of Barcelona
08193 Bellaterra, Spain
Email jrifa@ccd.uab.es

Mercè Villanueva
Dept. of Computer Sciences
Autonomous University of Barcelona
08193 Bellaterra, Spain
Email mvillanueva@ccd.uab.es

Abstract — **New error-correcting block codes for two-dimensional signal constellations such as QAM are given. They can correct one error in each component of the codewords, with only one redundant symbol. We also prove that these new block codes can be constructed for any Euclidean complex quadratic field.**

I. Introduction

In [2], two-dimensional signal sets were constructed over Gaussian integers modulo a non prime ideal $(2^n+2^n i)$, taking the multiplicative group of units. These kinds of constellations are interesting because they allow the use of differentially coherent detection in a QAM signal space.

In this paper we present new error-correcting block codes for two-dimensional signal constellations, such as QAM, constructed from integer rings of a complex algebraic number field. Their special interest is that they can correct one error in each component of the codewords, with only one redundant symbol, when they are sent on an additive noisy channel. Consequently, the transmission rate is $R = \frac{N-1}{N}$, where N is the block code length. We propose a very efficient decoding method based on only one euclidean division for each component.

II. Error-correcting block codes over $\Theta_{\mathbb{K}}/M$

Assume $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ is an Euclidean complex quadratic field and the ring of integers of $\mathbb{K}$ is $\Theta_{\mathbb{K}} = \{a+bw : a,b \in \mathbb{Z}\}$, where $w = \frac{1+\sqrt{d}}{2}$ or $w = \sqrt{d}$ depending on d. (The values for which $\mathbb{Q}(\sqrt{d})$ is an Euclidean complex quadratic field are $d = -1, -2, -3, -7$ and -11.) Using the map $\phi(a+bw) = a+bi$ from $\Theta_{\mathbb{K}}$ into $\mathbb{Z}[i]$, which is a $\mathbb{Z}$–module isomorphism, we can see $\Theta_{\mathbb{K}}$ as an infinite set of points in the complex plane. The quotient ring $G = \Theta_{\mathbb{K}}/M$, where M is a non-zero ideal of $\Theta_{\mathbb{K}}$, is finite and the map ϕ allows us to see it as a finite set of points in the complex plane, that is, as a QAM signal space.

Let $I = \{h^i \mid h \in G,\ 0 \le i \le k\}$ be the index set. We define block codes C_I of length $N = k+1$ over G by taking the subset of all the sequences $c = \{c_j\}_{j\in I}$, where $c_j \in G$ is such that

$$c_{h^0} \equiv -\sum_{j \in I-\{h^0\}} c_j \cdot j \pmod{M} \qquad (1)$$

The codewords in these codes are sequences of elements that belong to the quotient ring G, but they are not group codes. In [1] Forney proved that (N, K, D) group codes over general groups can be no better (in terms of Hamming distance) than conventional linear codes over fields or equivalently, group codes over elementary abelian groups, and are often worse.

Suppose we want to transmit signals of a $|G|$–QAM, using a block code C_I over G. Let $\{c_j\}_{j\in I-\{h^0\}}$ be the information sequence. Then, we compute the unique redundant symbol c_{h^0} by using equation (1).

Using the map ϕ, the components of the sequences are points in the complex integer plane. They are sent through an additive noisy channel and the received sequences are points in the complex plane, too. We will use a quantization that will associate these received points to a complex integer.

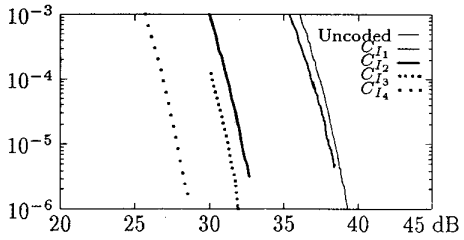
After performing the quantization, let $v = \{v_j\}_{j\in I}$ be the received sequence, where $v_j = c_j + e_j$ and $v_j, e_j \in \Theta_{\mathbb{K}}\ \forall j \in I$. To correct the errors e_j, $\forall j \in I$, added in each one of the codeword component, we compute $S(v) \equiv \sum_{j\in I} v_j \cdot j \equiv e_0 + e_1 h + \cdots + e_k h^k$, where $e_{h^i} = e_i$.

From $S(v) \in G$, dividing by h, we can assure, under certain conditions, that the errors $e_0, e_1, \ldots, e_k$ can be obtained as the division remainders. When the errors $e_0, \ldots, e_k$ are known, the computation $c_j = v_j - e_j$ $(\forall j \in I - \{h^0\})$ is sufficient to recover the information sequence.

III. Examples and Simulations

Over $G_5 = \mathbb{Z}[i]/(32+32i)$ (2048–QAM signal space), we can construct the block codes C_{I_1} with $N = 3$ and C_{I_2}, C_{I_3}, C_{I_4} with $N = 2$, which can correct errors such that their euclidean norm will be less than or equal to 1, 2, 4 and 5 respectively.

The following figure shows the probability of symbol error (P_s) versus signal-to-noise ratio (SNR) in dB for the Gaussian Channel with additive white noise.



References

[1] G.D. Forney, "On the Hamming Distance Properties of Group Codes" *IEEE Trans. Inform. Theory*, vol. 38, no. 6, pp. 1797-1801, 1992.

[2] J. Rifà, "Groups of Complex Integers Used as QAM Signals" *IEEE Trans. Inform. Theory*, vol. IT-41, pp. 1512-1517, 1995.

[1]This work has been partially supported by a Spanish CICYT grant TEL97-0663.