Groups of Complex Integers Used as QAM Signals

Josep Rifà

Abstract— **Block codes which allow error correction in a two-dimensional QAM signal space are given. The properties of these codes are used to demodulate QAM signals in a differentially coherent detection scheme on a noisy channel. Block codes presented are not group codes; however, their components belong to a group $\mathcal{G}_n$ or $\mathcal{G}'_n$ which is constructed starting from the Gaussian integers $\mathcal{G} = \mathcal{Z}[i]$ modulo a nonprime ideal $(2^n + 2^n i)$ and taking on it the multiplicative group of units. We classify and factor these multiplicative groups and use them to construct the block codes which become optimal and efficient from the point of view of transmission rate and decoding.**

Index Terms—**Gaussian integers, multiplicative groups of units, QAM signals, differentially coherent detection, error-correcting codes.**

I. Introduction

In [1], a multiplicative group of 16 elements is constructed and its application to differentially coherent detection of a 16-QAM signal is given. The authors of [1] ask for the existence, over the complex integers, of other similar and larger groups.

In this correspondence, a positive answer to that question is given. We prove that the 16-element group introduced in [1] is the multiplicative group of units $\mathcal{G}_2 = (\mathcal{Z}[i]/(2^2 + 2^2 i))^*$ and we also show that the operation defined in [1] is the natural multiplication in the quotient ring $\mathcal{Z}[i]/(2^2 + 2^2 i)$.

We construct other larger groups of a similar nature and we prove that the multiplicative group of units in the quotient ring $\mathcal{G}_n = (\mathcal{Z}[i]/2^n + 2^n i)^*$ gives a QAM signal space of $16, 64, 256, \ldots$ and, in general, 2^t points, where $t = 2n$. We also prove in this correspondence that starting with $\mathcal{G}_n$ we can construct a subgroup $\mathcal{G}'_n$ of $8, 32, 128, \ldots$ and, in general, 2^t points, where $t = 2n - 1$. These groups can be used with QAM modulation techniques.

We will take advantage of these constructions to define a code that can correct one additive error. We will see that the proposed codes are optimal taking into account the transmission rate.

Section II is devoted to the study of the multiplicative group of units in the quotient ring $\mathcal{Z}[i]/(2^n + 2^n i)$, where $\mathcal{Z}[i]$ is the ring of Gaussian integers. The most important result of this section is that, independently of the value of n, we can always factor the multiplicative group $(\mathcal{Z}[i]/(2^n + 2^n i))^*$ as a direct product of three cyclic groups of type $(2^{n-1}, 2^{n-1}, 2^2)$. These groups $\mathcal{G}_n$ give us the QAM signal spaces of $16, 64, 256, \ldots$ elements, and we also construct the $\mathcal{G}'_n$ groups of type $(2^{n-1}, 2^{n-1}, 2)$, which give us the QAM signal space of $8, 32, 128, \ldots$ elements.

In Section III we show that $\mathcal{G}_2$ coincides with the group constructed in [1].

Section IV is devoted to the construction of block codes based on the groups $\mathcal{G}_n$ and $\mathcal{G}'_n$. We compute the transmission rate of these codes and their performance when used in an additive Gaussian channel and we also give some examples. Finally, we use these codes in a differentially coherent detection scheme on a noisy channel and we prove error correction is possible under the assumption that there exists at most one error in each block of signals.

An Appendix contains several mathematical lemmas we need in the correspondence.

Manuscript received July 25, 1994; revised February 25, 1995. This work was partially supported by Spanish Grant TIC94-0331. The material in this correspondence was presented in part at the ICT'95 Conference, Indonesia, Apr. 3–7, 1995.

The author is with the Departament d'Informàtica, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain.

IEEE Log Number 9413874.

II. The Multiplicative Group of Units in the $\mathcal{Z}[i]/(2^n + 2^n i)$ Ring

The reader interested in the well-known properties of Gaussian integers $\mathcal{G} = \mathcal{Z}[i]$ can consult [2].

Let $\mathcal{G}$ be the Gaussian integers ring, $\mathcal{G} = \mathcal{Z}[i]$. The elements are of the form $a + bi$, where $a, b \in \mathcal{Z}$ and $i^2 = -1$. The element $\bar{\alpha} = a - bi$ is called the *conjugate* of $\alpha = a + bi \in \mathcal{G}$. The *norm* of the element $\alpha = a + bi \in \mathcal{Z}[i]$ is defined by

$$\|a + bi\| = a^2 + b^2 = \alpha \cdot \bar{\alpha}.$$

The units of $\mathcal{G}$ (elements which have multiplicative inverses) are $1, -1, i, -i$. The irreducible elements (Gaussian primes) in $\mathcal{G}$, up to unitary factors, are

- The elements whose norm is a prime integer p (i.e., $1 + i$, $2 + i$, etc.). The norm must, in fact, take the value $p = 2$, or $p = 1 \bmod 4$.
- The elements $\alpha = p$, where $p = 3 \bmod 4$ is a prime integer.

The factorization in $\mathcal{G}$ is unique, except for a unit factor.

$\mathcal{G}$ is a Euclidean ring. Therefore, given $\alpha, \beta \in \mathcal{G}$, there exist $q, r \in \mathcal{G}$, such that $\alpha = \beta \cdot q + r$ and $\|r\| < \|\beta\|$. The quotient q can be computed as

$$q = \left[\frac{\alpha\bar{\beta}}{\|\beta\|}\right]$$

where $[\cdot]$ denotes the Gaussian integer with real and imaginary parts closest to the real and imaginary parts of the argument, respectively. Define the function σ by $\sigma(a) = 1$ if $a \in \mathcal{Z}$ is even and $\sigma(a) = -1$ if $a \in \mathcal{Z}$ is odd.

$\mathcal{G}$ is a principal ring. The ideal generated by $\alpha = 2^n + 2^n i$ is a principal, nonprime ideal and we are interested in the multiplicative group of units $\mathcal{G}_n = (\mathcal{G}/\alpha)^*$. The elements of $\mathcal{G}_n = (\mathcal{G}/\alpha)^*$ are the residues of those in $\mathcal{G}$ which have a multiplicative inverse modulo α, that is, those with no common factor with α. But $(1 - i) = (1 + i)i^3$, so

$$\begin{aligned}\alpha &= 2^n + 2^n i = 2^n(1 + i) \\ &= (1 - i)^n(1 + i)^n(1 + i) = i^3(1 + i)^{2n+1}.\end{aligned}$$

Hence, the elements of $\mathcal{G}_n = (\mathcal{G}/\alpha)^*$ are those with no common factor with $(1 + i)$ and by, Lemma 4 of the Appendix, these elements are of the form $a + bi$ where $\sigma(a)\sigma(b) = -1$. Moreover, we can take as a complete system of incongruent residues in $\mathcal{G}_n$ the classes represented by $a + bi$, where $\sigma(a)\sigma(b) = -1$ and $|a| + |b| < 2^n$.

To illustrate these representatives, take $\mathcal{G}_2 = (\mathcal{G}/\alpha)^*$, where $\alpha = 2^2 + 2^2 i = 4 + 4i$. The complete system in $\mathcal{G}_2$ is the set of all complex integers marked with circles in Fig. 1.

We summarize in the following proposition

Proposition 1: $|\mathcal{G}_n| = |(\mathcal{G}/\alpha)^*| = 2^{2n}$. We can choose, as a canonical representative of each class in $(\mathcal{G}/\alpha)^*$ the elements $a + bi$, where $\sigma(a)\sigma(b) = -1$ and $|a| + |b| < 2^n$.

The next proposition is the main result in this correspondence. Here we prove that all the complex integers in $\mathcal{G}_n$ can be factored in the form

$$(1 + 2i)^a(1 - 2i)^b i^c \bmod 2^n + 2^n i$$

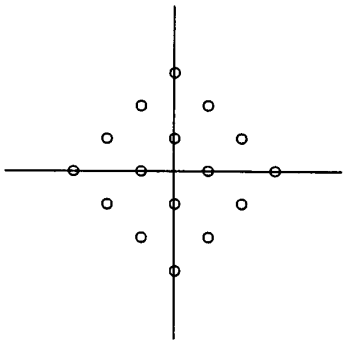

Fig. 1. The group $\mathcal{G}_2$ of 16-QAM signals.

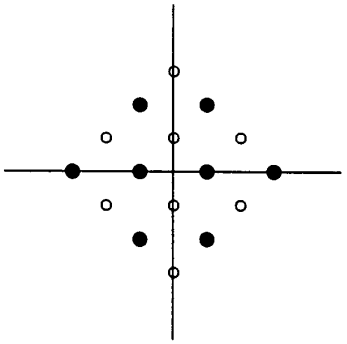

Fig. 2. The group $\mathcal{G}_2'$ group of 8-QAM signals.

where $0 \le a \le 2^{n-1}$, $0 \le b \le 2^{n-1}$, $0 \le c \le 2^2$, and this representation is unique. In other words, if we use $\odot$ for the direct product of commutative, multiplicative groups, we have the following proposition.

Proposition 2: $\mathcal{G}_n$ is a commutative multiplicative finite group of type $(2^{n-1}, 2^{n-1}, 2^2)$ and we can factor $\mathcal{G}_n$ as the direct product

$$\mathcal{G}_n = \langle 1+2i \rangle \odot \langle 1-2i \rangle \odot \langle i \rangle$$

where $\langle x \rangle$ means the cyclic subgroup generated by x.

Proof: The technique to factor a given finite abelian 2-group as a product of cyclic 2-groups is described in many books of basic algebra, for example see [3]. This technique consists of finding an element of maximal period, which allows us to construct the quotient group of the initial group modulo the cyclic subgroup generated by this element, and so on.

- Let $f = 1+2i \in \mathcal{Z}[i]$ and $g = \bar{f} = 1-2i \in \mathcal{Z}[i]$.
  We know (see Lemma 7 and Lemma 10 of the Appendix) the order of $f \in \mathcal{Z}[i]$ is maximal in $\mathcal{G}_n$, so we can factorize $\mathcal{G}_n$ as a direct product, a component of which will be $\langle 1+2i \rangle$.
- The order of
  $$g = \bar{f} = 1-2i \in \mathcal{G}_n / \langle f \rangle$$
  is also the maximum 2^{n-1}.
  In fact, if it were $g^e \in \langle f \rangle$ we would have $g^e = f^j \in \mathcal{G}_n$ with $e, j < 2^{n-1}$, but this is not possible by Lemma 11 of the Appendix.
- At this point of the proof we can assure that
  $$\mathcal{G}_n = \langle 1+2i \rangle \odot \langle 1-2i \rangle \odot G$$
  where the size of G is 4.

The element i is a generator of G because there is no power of i equal to $f^a g^b$. In fact, it is not possible to have

$$f^a g^b = i^c \bmod 2^n + 2^n i$$

where $a, b < 2^{n-1}$ and $0 \le c < 4$ because this would lead to $f^a = g^{2^{n-1}-b} \cdot i^c \in \mathcal{G}_n$, which contradicts Lemma 11 of the Appendix. □

III. QAM Signals

$\mathcal{G}_2$ is the group constructed in [1]. That construction of the 16-QAM signal group can be seen below. The first column in the listing that follows shows the notation used in [1] and the last column is our notation using factorization $\mathcal{G}_2 = \langle f \rangle \odot \langle g \rangle \odot \langle i \rangle$, where $f = 1+2i$ and $g = 1-2i$.

$$\begin{aligned}
\epsilon &= (1,0) = f^0 g^0 i^0 & g_8 &= (-1,0) = f^0 g^0 i^2 \\
g_1 &= (3,0) = f^1 g^1 i^2 & g_9 &= (-3,0) = f^1 g^1 i^0 \\
g_2 &= (2,1) = f^0 g^1 i^1 & g_A &= (-2,1) = f^1 g^0 i^1 \\
g_3 &= (2,-1) = f^1 g^0 i^3 & g_B &= (-2,-1) = f^0 g^1 i^3 \\
g_4 &= (0,1) = f^0 g^0 i^1 & g_C &= (0,-1) = f^0 g^0 i^3 \\
g_5 &= (0,3) = f^1 g^1 i^3 & g_D &= (0,-3) = f^1 g^1 i^1 \\
g_6 &= (-1,2) = f^0 g^1 i^2 & g_E &= (1,-2) = f^0 g^1 i^0 \\
g_7 &= (1,2) = f^1 g^0 i^0 & g_F &= (-1,-2) = f^1 g^0 i^2
\end{aligned}$$

This group can be used as a 16-QAM signal. The group $\mathcal{G}_3$ can be used as a 64-QAM signal and, in general, the group $\mathcal{G}_n$ can be used as a 2^{2n}-QAM signal.

The elements of the $\mathcal{G}_n$ group form a diamond shape in the complex plane, centered at the origin but with the origin not belonging to $\mathcal{G}_n$. The points of $\mathcal{G}_n$ are $a+bi$ with $|a|+|b| < 2^n$ and $\sigma(a)\sigma(b) = -1$ (the real and imaginary values are neither both even, nor both odd). See Fig. 1 for the case of $\mathcal{G}_2$, the group of 16 QAM signals.

The case of signal sets of 2^{2n-1} elements is not covered by $\mathcal{G}_n$ groups, but we can consider the groups $\mathcal{G}_n' \subset \mathcal{G}_n$ defined by

$$\mathcal{G}_n' = \langle 1+2i \rangle \odot \langle 1-2i \rangle \odot \langle -1 \rangle.$$

It is easy to see that $|\mathcal{G}_n'| = 2^{2n-1}$

$\mathcal{G}_n'$ forms a diamond shape in the complex plane like $\mathcal{G}_n$ but without the points $a+bi$ with b odd. See the group $\mathcal{G}_2'$ of the 8-QAM signals marked with filled circles in Fig. 2. The $\mathcal{G}_n$ or $\mathcal{G}_n'$ groups can be used in the differentially coherent detection of QAM signals, as in [1].

IV. One-Error-Correcting Codes

Complex integers have seldom been used in error correction. The interested reader can find a very good introduction to this subject in [4]. There, Huber considers linear codes over the finite field $\mathcal{G}_\pi$ of complex integers modulo a Gaussian prime but, in this correspondence, we are interested in block codes whose codewords are sequences of elements that belong to the group structure $\mathcal{G}_n$, so these codes are not linear codes over a finite field.

If we assume a noiseless channel, the groups $\mathcal{G}_n$ and $\mathcal{G}_n'$ can be successfully used in differentially coherent detection of QAM signals as in [1], but when noise is added to the signal we are interested in constructing error-correcting codes using the groups $\mathcal{G}_n$ or $\mathcal{G}_n'$ to represent the QAM signal space.

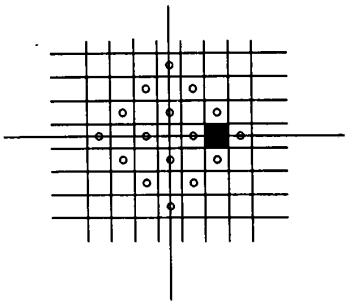

Fig. 3. Quantization of 16-QAM signals.

In the following we will use the group $\mathcal{G}_n$, but the results can be extended to the $\mathcal{G}'_n$ case.

Consider the set W of all the sequences $\{s_i\}_{i\in I}$, where each $s_i \in \mathcal{G}_n$ and the index set I is one among the following

$$I_1 = \{f^a g^b \mid f \equiv 1 + 2i;\, g \equiv 1 - 2i;\, 0 \le a < 2^{n-1};\, 0 \le b < 2^{n-1}\} \tag{1}$$

$$I_2 = \{f^a g^b \mid f \equiv 1 + 2i;\, g \equiv 1 - 2i;\, 0 \le a < 2^{n-2};\, 0 \le b < 2^{n-2}\} \tag{2}$$

$$I_3 = \{f^a \mid f \equiv 1 + 2i;\, 0 \le a < 2^{n-1}\}. \tag{3}$$

We will have sequences of length either $N = 2^{2n-2}$ or $N = 2^{2n-4}$ or $N = 2^{n-1}$, depending on the index set used.

We define the code $C_I \subset W$ by taking the subset of all the sequences $\{w_m\}_{m\in I}$ such that

$$w_{f^0 g^0} \equiv - \sum_{m \in I - \{f^0 g^0\}} w_m \cdot m.$$

All components w_m are free except for the index $m = f^0 g^0$. The symbol w_m indexed by $m = f^0 g^0$ is a redundant symbol and can be used for error correction.

Code C_I is a block code of length N over $\mathcal{G}_n$. The transmission rate of code C_I is

$$R = \frac{N-1}{N}$$

and it is not difficult to see that the minimum Hamming distance between codewords is 2. Because there is only one redundant component these codes fulfill the Singleton bound with equality and are optimal (see [5, p. 317]).

The smallest Euclidean distance d_E^2 between two uncoded vectors is 2 and between two codewords in code C_I is either $d_E'^2 = 4$, $d_E'^2 = 8$, or $d_E'^2 = 8$ depending whether the index set I is I_1, I_2, or I_3, so if we compute the asymptotic coding gain defined in [6, p. 238] we obtain

$$G \le 10 \log_{10} (R \cdot d_E'^2 / d_E^2) \text{ dB}$$

so $G \approx 3.01$ dB or $G \approx 6.02$ dB depending on the code used.

Any component of the sequence we receive through the channel is a point in the complex plane. We will use a quantization that will associate these points in the complex plane to a complex integer. An easy way to do that is to associate all the points in the black zone of Fig. 3 to the central point.

Suppose that, after quantization, there is only one error $\epsilon \in \mathcal{G}$ added to the component indexed by $j \in I$. The received sequence is $v = \{v_m\}_{m\in I}$, where

$$\begin{cases} v_m \equiv w_m & \forall m \in I \text{ with } m \ne j \\ v_j \equiv w_j + \epsilon. \end{cases}$$

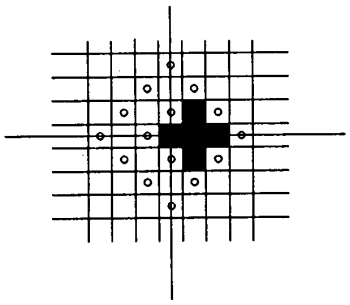

Fig. 4. Zone where error correction is possible when the true signal is the point $(1, 0)$ and we use code C_{I_1} or C_{I_3}.

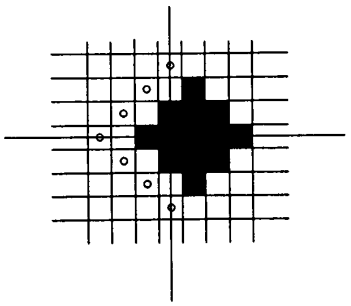

Fig. 5. Zone where error correction is possible when the true signal is the point $(1, 0)$ and we use code C_{I_2}.

Now we can compute the syndrome

$$S(v) \equiv \sum_{m\in I} v_m \cdot m = j \cdot \epsilon.$$

So the computed syndrome coincides with $S(v) = j \cdot \epsilon$ and we can correct the error if we can deduce the position j of the error and its value ϵ from $j \cdot \epsilon$.

Proposition 3: If either $I = I_1$ or $I = I_3$, code C_I allows error correction of one error of type

$$\{1, -1, i, -i\}$$

added by the channel. If $I = I_2$, code C_I allows error correction of one error of type

$$\{1, -1, i, -i, 1 + i, 1 - i, -1 + i, -1 - i, 2, -2, 2i, -2i\}$$

added by the channel.

Proof: From Proposition 2 we know that $\forall\, j \in I = I_1$ and $\forall 0 \le c < 4$ the elements $i^c \cdot j \in \mathcal{G}_n$ are all different; therefore, if the error is $\epsilon \in \{1, -1, i, -i\}$ and we are using code C_I, where $I = I_1$ or $I = I_3$, from $S(v) = i^c \cdot j$, we can compute the position j of the error and its value i^c $(0 \le c < 4)$. This kind of error correction (see Fig. 4) is the so-called *one Mannheim error correction* in [4].

From Proposition 12 of the Appendix we know that $\forall\, j \in I = I_2$, $\forall 0 \le c < 4$, and $\forall 0 \le d \le 2$, the elements $i^c(1 + i)^d \cdot j$ are all different. Therefore, if the error is

$$\epsilon \in \{1, -1, i, -i, 1 + i, -1 + i, 1 - i, -1 - i, 2, -2, 2i, -2i\}$$

and we are using code C_I, where $I = I_2$, from $S(v) = i^c(1+i)^d \cdot j$ we can compute the position j of the error and its value $i^c(1 + i)^d$, where $0 \le c < 4$ and $0 \le d \le 2$ (see Fig. 5).

A. Example

Suppose $\mathcal{G}_n = \mathcal{G}_2$ and we use the index set

$$I = I_1 = \{f^0g^0, f^0g^1, f^1g^0, f^1g^1\}.$$

The sequences of C_I have four components from $\mathcal{G}_2$. Three of them are unconstrained and the fourth, which corresponds to the index f^0g^0 can be computed from the others by

$$w_{f^0g^0} = -\sum_{m \in I - \{f^0g^0\}} w_m \cdot m.$$

For example, to transmit the information given by the QAM signals

$$(3,0), (2,-1), (2,1)$$

we will construct the following sequence: $w_{f^0g^1} = (3,0)$, $w_{f^1g^0} = (2,-1)$, $w_{f^1g^1} = (2,1)$ and we will compute

$$\begin{aligned} w_{f^0g^0} &= -(3,0)f^0g^1 - (2,-1)f^1g^0 - (2,1)f^1g^1 \\ &= (1,2) + (0,1) + (2,-1) = (3,2) = (-1,-2). \end{aligned}$$

Now we will send through the channel the four signals

$$\{w_{f^0g^0}, w_{f^0g^1}, w_{f^1g^0}, w_{f^1g^1}\} = \{(-1,-2), (3,0), (2,-1), (2,1)\}.$$

Suppose that, after quantization, one error $\epsilon = i$ is added to the second component of the received sequence which will be

$$(-1,-2)\ (3,1)\ (2,-1)\ (2,1).$$

The receiver will compute the syndrome

$$\begin{aligned} S(v) &= (-3,0)f^0g^0 + (3,1)f^0g^1 + (2,-1)f^1g^0 + (2,1)f^1g^1 \\ &= (-1,-2) + (1,-1) + (0,-1) + (-2,1) = (2,1) \end{aligned}$$

and, according to the listing in Section III, we will have

$$S(v) = (2,1) = f^0g^1 i.$$

The conclusion will be that there was one error of type i in the component indexed by f^0g^1.

B. The Differentially Coherent Detection Scheme in a Noisy Channel

In a noiseless channel the differentially coherent detection scheme of QAM signals works in the following way (see [1] for further details):

Suppose the signals we want to send are $d_0, d_1, \cdots, d_n, \cdots, \in \mathcal{G}_n$.

- The transmitter computes $s_i = d_i(\overline{s_{i-1}})^{-1}$.
- In the receiver, the symbols arrive as $\rho_0, \rho_1, \cdots$, with only a phase shift ϕ. We have $\rho_n = s_n e^{i\phi}$.
- The receiver computes the original signals $d_i = \rho_i \overline{\rho_{i-1}}$.

Now suppose a noisy channel. In the receiver, the symbols will arrive as $\rho'_i = s'_i e^{i\phi}$, where there is a phase shift ϕ and $s'_i = s_i + \epsilon_i$, where ϵ_i is an error added by the channel. Assume there is only one error in each block and, moreover, the error after quantization is in the set $\{1,-1,i,-i\}$.

The code C_I, where $I = I_3$ (see (3)), performs very well in this situation and we will modify the differentially coherent detection scheme above for error correction.

- The transmitter computes $s_i = d_i(\overline{s_{i-1}})^{-1}$.
- Before sending the symbol s_i the transmitter uses the block error-correction code C_{I_3} by adding a redundant symbol to each $N - 1 = 2^{n-1} - 1$ symbols.
- In the receiver, the symbols arrive as $\rho'_i = s'_i e^{i\phi}$, where there is a phase shift ϕ and $s'_i = s_i + \epsilon_i$, where ϵ_i is an error added by the channel.
- For each received block $\rho'_t, \rho'_{t+1}, \cdots, \rho'_{t+N-1}$, the receiver computes the syndrome

$$S = \sum_{i=0}^{N-1} \rho'_{t+i} f^i = e^{i\phi}\epsilon_a f^a$$

where ϵ_a is the only error added by the channel just in the f^a component of the block.

We know that $\|e^{i\phi}\epsilon_a\| = 1$, so it is possible to compute the position f^a of the error because $\|S\| = \|f^a\| = \|5^a\|$ and this value identifies f^a (see Lemma 8).

Now it is possible to compute the correct $\rho_a = \rho'_a - e^{i\phi}\epsilon_a$, which is only affected by the phase shift.

- The receiver computes the original signals $d_i = \rho_i \overline{\rho_{i-1}}$.

V. Conclusion

We have constructed, classified, and characterized the groups $\mathcal{G}_n$ and $\mathcal{G}'_n$ that can be used for differentially coherent detection of a QAM signal. In fact, we have generalized the construction of the finite group given in [1].

These groups can be used, in general, in the design of block codes for QAM signal constellations.

We have focused on the problem of channel coding by using an additive Gaussian channel and we have constructed error-correcting codes which allow us to correct one error in the two-dimensional signal. This error, after quantization, can belong to the set

$$\{1,-1,i,-i,1+i,1-i,-1+i,-1-i,2,-2,2i,-2i\}.$$

The transmission rate of these codes is very high because there is only one redundant symbol, and their decoding is very efficient.

We have used these codes as a solution in a noisy channel when we are interested in the differentially coherent detection scheme.

The codewords of the constructed block codes are sequences of elements that belong to group structures $\mathcal{G}_n$ or $\mathcal{G}'_n$. These codes are neither group nor linear codes over a field, so it is not possible to use the standard techniques in these cases.

This correspondence gives rise to several research problems, for instance finding codes that allow us to correct more than one error, and also finding very efficient decoding algorithms for these cases.

Appendix

Lemma 4: The following statements are equivalent:

1) $a + bi$ is a multiple of $1 + i$ (or $1 - i$).
2) $a + b$ and $a - b$ are both even numbers.
3) $\sigma(a)\sigma(b) = 1$.
4) The class $[a + bi]$ is not invertible in $\mathcal{G}/\alpha$.

Proof:

1) The multiples of $1 + i$ and the multiples of $1 - i$ are the same because $1 + i$ differs from $1 - i$ by a unitary factor: $1 + i = (1 - i) \cdot i$. If $a + bi$ is a multiple of $1 + i$ then

$$a + bi = (1 + i) \cdot (c + di) = (c - d) + (c + d)i$$

so $a + b = 2c$ and $b - a = 2d$, are both even numbers.

2) If $a + b = 2c$ and $b - a = 2d$ are both even numbers, then a and b have the same parity, so $\sigma(a)\sigma(b) = 1$.
3) If $\sigma(a)\sigma(b) = 1$ then the parity of a and b is the same. We can take $a + b = 2c$ and $b - a = 2d$ and construct

$$a + bi = \frac{2c - 2d}{2} + \frac{2c + 2d}{2}i = (1 + i)(c + di)$$

so $a + bi$ is a multiple of $1 + i$ and its residue class is not an invertible element in $\mathcal{G}/\alpha$.

All the representatives $a+bi$ and $c+di$, in the same class, satisfy

$$\sigma(a)\sigma(b) = \sigma(c)\sigma(d).$$

In fact

$$a+bi = c+di+(x+yi)\alpha.$$

Then $a = c+(x-y)2^n$ and $b = d+(x+y)2^n$. So $\sigma(a) = \sigma(c)$ and $\sigma(b) = \sigma(d)$.

4) If $[a+bi]$ is not an invertible element in $\mathcal{G}/\alpha$ then $a+bi$ and $\alpha = 2^n + 2^n i$ have common factors, so $a+bi$ is a multiple of $1+i$. □

Lemma 5: If s is an odd integer and $a+bi \in \mathcal{Z}[i]$ then either $a+bi$ or $1+s(a+bi)$ is a multiple of $1+i$.

Proof: If $a+bi$ is not a multiple of $1+i$ then $\sigma(a)\cdot\sigma(b) \neq 1$. If s is an odd number then $\sigma(sa) = \sigma(a)$ and $\sigma(sb) = \sigma(b)$ so $\sigma(sa)\cdot\sigma(sb) \neq 1$.

But $\sigma(1+sa) \neq \sigma(sa)$, hence $\sigma(1+sa)\cdot\sigma(sb) = 1$ and $1+sa+sbi$ is a multiple of $1+i$. □

Lemma 6: If $a+bi \in \mathcal{G}_3$ then the multiplicative order of $a+bi$ is at most 2^2.

Proof: First we can suppose $a = 1+2t$ and $b = 2r$, where $t, r \in \mathcal{Z}$. Then

$$\begin{aligned}(a+bi)^{2^2} &= (1+2t+2ri)^{2^2} = (1+(2t+2ri))^{2^2}\\ &= 1+8(t+ri)+24(t+ri)^2\\ &\quad +32(t+ri)^3+16(t+ri)^4.\end{aligned}$$

But $(1+i)(1-i) \equiv 2$ so

$$\begin{aligned}(a+bi)^{2^2} &\equiv 1+8((t+ri)+3(t+ri)^2))\\ &\quad +16(1+i)(1-i)(t+ri)^3\\ &\quad +8(1+i)(1-i)(t+ri)^4\\ &\equiv 1+8((t+ri)+3(t+ri)^2))\\ &\equiv 1+8(t+ri)(1+3(t+ri)) \bmod 8+8i.\end{aligned}$$

Now by using Lemma 5 for $s=3$ we have $a+bi \equiv 1 \bmod 8+8i$.

The second part of the lemma is exactly the same but assuming $a = 2r$ and $b = 1+2t$. □

Lemma 7: Suppose $n \geq 3$. If $a+bi \in \mathcal{G}_n$ then the multiplicative order of $a+bi$ is a divisor of 2^{n-1}.

Proof: The order of $a+bi$ will be a divisor of 2^{2n}, which is the size of $\mathcal{G}_n$.

Let e be the order of $f \equiv a+bi \in \mathcal{G}_n$.

From

$$f^e \equiv 1+(c+di)(2^n+2^n i)$$

we can write

$$\begin{aligned}f^{2e} &\equiv 1+2(c+di)(2^n+2^n i)+(c+di)^2(2^n+2^n i)^2\\ &\equiv 1 \bmod 2^{n+1}+2^{n+1}i.\end{aligned}$$

By Lemma 6 we can begin with $f^{2^2} \equiv 1 \bmod (2^3+2^3 i)$ and then $f^{2^3} \equiv 1 \bmod (2^4+2^4 i)$ and so on until $f^{2^{n-1}} \equiv 1 \bmod (2^n+2^n i)$. □

Remark: In the case $n < 3$ we have

- When $n=1$ the units, modulo $2+2i$, are $\mathcal{G}_1 = \{1,-1,i,-i\}$.
- When $n=2$ the units, modulo $2^2+2^2 i$ are

$$\mathcal{G}_2 = \{\pm 1, \pm 3, \pm 3i, \pm i, \pm 1 \pm 2i, \pm 2 \pm i\}$$

and, for each one, its order is a divisor of 4.

Lemma 8: The multiplicative order of 5, modulo 2^{n+1} and modulo $2^n+2^n i$, is 2^{n-1}.

We also have

$$5^{2^{n-2}} \equiv 1+2^n \bmod 2^{n+1}$$

and

$$5^{2^{n-2}} \equiv 1+2^n \bmod 2^n+2^n i.$$

Proof: It is easy to see that

$$5^{2^0} \equiv 1+2^2 \bmod 2^3$$

and by using induction on n we can suppose

$$5^{2^{n-3}} \equiv 1+2^{n-1} \bmod 2^n$$

so

$$5^{2^{n-3}} \equiv 1+2^{n-1}+\lambda 2^n$$

and squaring each side we get

$$5^{2^{n-2}} \equiv 1+2^n \bmod 2^{n+1}.$$

Squaring again

$$5^{2^{n-1}} \equiv 1 \bmod 2^{n+1}.$$

So the multiplicative order of 5 will be 2^{n-1} modulo 2^{n+1}.

But $2 \equiv (1-i)(1+i)$, so

$$2^{n+1} \equiv (1-i)(2^n+2^n i)$$

and the multiplicative order of 5 modulo $2^n+2^n i$ will be 2^{n-1}. □

Lemma 9: Let $\alpha, \beta \in \mathcal{G}_n$. We have

- $\alpha \equiv \beta \bmod 2^n \Longrightarrow \alpha \equiv \beta \bmod 2^{n-1}+2^{n-1}i$.
- $\alpha \equiv \beta \bmod 2^n+2^n i \Longrightarrow \alpha \equiv \beta \bmod 2^n$.
- $\alpha \equiv \beta \bmod 2^n+2^n i \Longrightarrow \|\alpha\| \equiv \|\beta\| \bmod 2^{n+1}$

Lemma 10: Let f be $f = 1+2i \in \mathcal{Z}[i]$ and $g = \bar{f} = 1-2i$. The multiplicative order of f and g modulo $2^n+2^n i$ is exactly 2^{n-1}.

Proof: Suppose $n \geq 3$.

We know by Lemma 7 that the multiplicative order e of f (or g) modulo $2^n+2^n i$ is a divisor of 2^{n-1} and if it were $e < 2^{n-1}$ then

$$f^e \equiv 1 \bmod 2^n+2^n i$$

so, by using Lemma 9, we would have

$$\|f^e\| \equiv 1 \bmod 2^{n+1}.$$

But $\|f\| = 5$, so $5^e \equiv 1 \bmod 2^{n+1}$ which contradicts Lemma 8.

If $n=2$, the proof is straightforward. □

Lemma 11: Let f be $f = 1+2i \in \mathcal{Z}[i]$ and $g = \bar{f} = 1-2i$. Then $f^a \not\equiv g^b i^c \in \mathcal{G}_n$, where $a, b < 2^{n-1}$ and $0 \leq c < 4$

Proof: If it were

$$f^a \equiv g^b i^c \in \mathcal{G}_n$$

we could use Lemma 9 to write

$$5^a \equiv 5^b \bmod 2^{n+1}$$

but according to Lemma 8 we would have

$$a \equiv b \bmod 2^{n-1}$$

so $a = b \in \mathcal{Z}$.

Now, if it were

$$f^a \equiv g^a i^c \in \mathcal{G}_n$$

where $a < 2^{n-1}$ and $0 \le c < 4$, we could take $a = t2^h$, where $\gcd(t, 2^{n-1}) = 1$ hence for some coefficient A we would have

$$A \cdot t \equiv 1 \bmod 2^{n-1}$$

and

$$(f^{t2^h})^A \equiv (g^{t2^h})^A i^{cA} \bmod 2^n + 2^n i.$$

But $f^{tA} \equiv f \in \mathcal{G}_n$ and $g^{tA} \equiv g \in \mathcal{G}_n$, hence $f^{2^h} \equiv g^{2^h} \cdot i^{c'}$ for some c'

Squaring each side in the equality above we finally get

$$f^{2^{n-2}} \equiv g^{2^{n-2}} \bmod 2^n + 2^n i$$
$$\|f^{2^{n-2}}\| \equiv f^{2^{n-2}} g^{2^{n-2}} \equiv g^{2^{n-1}}$$
$$\equiv 1 \bmod 2^n + 2^n i.$$

But

$$\|f^{2^{n-2}}\| \equiv \|f\|^{2^{n-2}} \equiv 5^{2^{n-2}} \not\equiv 1 \bmod 2^n + 2^n i$$

by using Lemma 8. That contradicts the initial hypothesis. □

Proposition 12: Let $\gamma \not\equiv \beta \in \mathcal{G}_n$ be two elements belonging to $\langle 1 + 2i \rangle \setminus \langle 1 - 2i \rangle$ and suppose $\gamma \equiv f^a g^b$, $\beta \equiv f^{a'} g^{b'}$, where $f \equiv 1 + 2i$, $g \equiv \bar{f} \equiv 1 - 2i$.

If $0 \le a, a', b, b' < 2^{n-2}$ then $\forall\, 0 \le c, c' < 4$, $\forall\, 0 \le d, d' \le 2$, is

$$i^c (1+i)^d \gamma \not\equiv i^{c'} (1+i)^{d'} \beta \in \mathcal{G}_n.$$

Proof: Suppose

$$i^c (1+i)^d \gamma \equiv i^{c'} (1+i)^{d'} \beta \in \mathcal{G}_n.$$

First of all it is easy to see that $d = d'$, and assuming $d \le 2$ we can write

$$i^c \gamma \equiv i^{c'} \beta \bmod 2^{n-1} + 2^{n-1} i.$$

Thus, by Lemma 11 $a \equiv a' \bmod 2^{n-2}$, $b \equiv b' \bmod 2^{n-2}$, and $c \equiv c' \bmod 2^2$, so $a = a'$, $b = b'$, $c = c'$, and $\gamma = \beta$ □

ACKNOWLEDGMENT

The author wishes to thank the referees for careful reading of the first version of this correspondence and for their very helpful comments.

REFERENCES

[1] R. G. Egri and F. A. Horrigan, "A finite group of complex integers and its application to differentially coherent detection of QAM signals," *IEEE Trans. Inform. Theory*, vol. 40, no. 1, pp. 217–219, Jan. 1994.
[2] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed. London, UK: Clarendon Press, 1989.
[3] S. Lang, *Algebra*. Reading, MA: Addison-Wesley, 1969.
[4] K. Huber, "Codes over gaussian integers," *IEEE Trans. Inform. Theory*, vol. 40, no. 1, pp. 207–216, Jan. 1994.
[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
[6] R. E. Blahut, *Digital Transmission of Information*. Reading, MA: Addison-Wesley, 1990.

New 16-PSK Group Trellis Codes

Francesco Agus, Sergio Benedetto, *Senior Member, IEEE*, and Roberto Garello, *Member IEEE*

***Abstract*—The theory of group codes simplifies the construction of good rotationally invariant trellis codes for the additive white Gaussian noise channel. New geometrically uniform trellis codes, with spectral efficiency 3 bits/2D, based on multidimensional $L \times 16$-PSK constellations in 4, 6, and 8 dimensions, obtained by group trellis codes over nonbinary groups of the kind Z_{16}^L, are presented. Most of the codes improve, in terms of asymptotic gain and rotational invariance, the best codes known so far in the literature.**

I. INTRODUCTION

The construction of "good" Euclidean-space trellis codes for the additive white Gaussian noise channel (where "good" is usually identified with large Euclidean free distance) is made difficult by the lack of algebraic methods to synthesize good codes, that instead may exist for finite-length block codes. Even if the theory of *group codes* [10] has not yet provided these algebraic constructions, it allows more systematic searches into the class of *geometrically uniform (GU) codes* [9]. Most of the best codes known in the literature have been proved to be GU [9], [18]. Moreover, the symmetry properties of GU codes highly simplifies their performance evaluation: since all the Voronoi regions are congruent, the Euclidean distances and error probabilities can be evaluated based on any sample sequence of the codes, which is normally chosen as the all-zero sequence.

In [2] GU trellis codes based on multidimensional $L \times M$-PSK constellations, with $L = 1, 2, 3, 4$, $M = 4, 8, 16$, integer and noninteger rates in bits/2D, obtained using binary linear convolutional codes, i.e., group trellis codes over binary groups of the kind Z_2^k, were presented. Nevertheless, for $M = 8$ and 16, the binary constraint imposes severe limitations in terms of maximum free distance achievable. If the average energy per dimension of the constellation is $\mathcal{E} = 0.5$ (every two-dimensional PSK has unitary radius) then $d_{\text{free}}^2 \le 4$ for $M = 8$ and $d_{\text{free}}^2 \le 2$ for $M = 16$. These limitations can be overcome using codes over nonbinary groups of the kind Z_M^L (Z_M is the group of integers modulo M); in [3] new trellis codes over $L \times M$-PSK, with $L = 2, 3, 4$, $M = 4, 8$, and spectral efficiency of 1 and 2 bits/2D, were obtained in this way. Moreover, the theory of group codes provides efficient methods for the construction of rotationally invariant codes if these kinds of groups are chosen for PSK constellations [3], [4].

In this correspondence we apply the group code approach to the construction of new GU trellis codes over multidimensional $L \times 16$-PSK constellations, with spectral efficiency 3 bits/2D, using group trellis codes over nonbinary groups of the kind Z_{16}^L.

In Section II the essential features of GU codes and group codes are recalled. Section III contains a brief summary of the group codes approach to the construction of rotationally invariant codes. The best trellis codes over $L \times 16$-PSK known so far are reported in Section IV. In Section V we present new GU trellis codes with spectral efficiency of 2 bits/2D, found with the group codes approach. They are always

Manuscript received Sept. 8, 1994; revised Apr. 11, 1995. This work was partially supported by CNR under Progetto Finalizzato Trasporti, subproject "Prometheus."

The authors are with the Dipartimento di Elettronica, Politecnico di Torino, 10129 Torino, Italy.

IEEE Log Number 9413881.