Construction of Barnes-Wall Lattices from Linear Codes over Rings

J. Harshan
Dept. of ECSE,
Monash University
Clayton, Australia
Email:harshan.jagadeesh@monash.edu

Emanuele Viterbo
Dept. of ECSE,
Monash University
Clayton, Australia
Email:emanuele.viterbo@monash.edu

J.-C. Belfiore
Dept. of Communications and Electronics,
Telecom ParisTech
Paris, France
Email:belfiore@enst.fr

***Abstract*— Dense lattice packings can be obtained via the well-known Construction A from *binary* linear codes. In this paper, we use an extension of Construction A called Construction A' to obtain Barnes-Wall lattices from linear codes over polynomials rings. To obtain the Barnes-Wall lattice BW_{2^m} in $\mathbb{C}^{2^m}$ for any $m \geq 1$, we first identify a linear code $\mathcal{C}_{2^m}$ over the quotient ring $\mathcal{U}_m = \mathbb{F}_2[u]/u^m$ and then propose a mapping $\psi : \mathcal{U}_m \to \mathbb{Z}[i]$ such that the code $\mathcal{L}_{2^m} = \psi(\mathcal{C}_{2^m})$ is a lattice constellation. Further, we show that $\mathcal{L}_{2^m}$ has the cubic shaping property when m is even. Finally, we show that BW_{2^m} can be obtained through Construction A' as $BW_{2^m} = (1+i)^m\mathbb{Z}[i]^{2^m} \oplus \mathcal{L}_{2^m}$.**

I. Introduction

This paper addresses the construction of dense lattice packings [1] using linear block codes [2]. Towards explaining the problem statement, we present a series of definitions used in this paper. A complex lattice Λ is a discrete subgroup of $\mathbb{C}^n$ [1]. Alternatively, Λ is a $\mathbb{Z}[i]$-module generated by the vectors $\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n \mid \mathbf{v}_j \in \mathbb{C}^n\}$ as

$$\Lambda = \left\{ \sum_{j=1}^{n} q_j \mathbf{v}_j \mid \forall q_j \in \mathbb{Z}[i] \right\}.$$

We refer to a set $\mathcal{L}$ as a *lattice Euclidean code* (or lattice constellation) in $\mathbb{C}^n$ if $\mathcal{L}$ is a *finite* subset of lattice Λ.

It is well known that any set $\mathcal{S}$ in $\mathbb{C}^n$ has a one-one correspondence to a set (denoted by $\bar{\mathcal{S}}$) in $\mathbb{R}^{2n}$ as $\bar{\mathcal{S}} = \{[\Re(\mathbf{x})\ \Im(\mathbf{x})] \mid \forall \mathbf{x} \in \mathcal{S}\}$. Using the above equivalence from $\mathbb{C}$ to $\mathbb{R}$, we make the following definition on a lattice Euclidean code.

Definition 1: A lattice Euclidean code $\mathcal{L} \subset \Lambda$ is said to have the *cubic shaping* property if the corresponding set $\bar{\mathcal{L}}$ can be written as $\bar{\mathcal{L}} = \bar{\Lambda}/a\mathbb{Z}^{2n}$, for some $a \in \mathbb{Z}$.

The above definition implies that a lattice Euclidean code $\mathcal{L}$ with cubic shaping property is a subset of $\mathbb{Z}_a[i]^n$ for some $a \in \mathbb{Z}$, where $\mathbb{Z}_a$ is the ring of integers modulo a. Henceforth, throughout the paper, a Euclidean code refers to a lattice Euclidean code.

Definition 2: (Chapter 4 in [2]) We define the polynomial quotient ring $\mathcal{U}_m = \mathbb{F}_2[u]/u^m$ in variable u for any $m \geq 1$ as

$$\mathcal{U}_m = \left\{ \sum_{k=0}^{m-1} b_k u^k \mid b_k \in \mathbb{F}_2 \right\},$$

with regular polynomial addition and multiplication over $\mathbb{F}_2$ coefficients along with the quotient operation $u^m = 0$, which is equivalent to cancelling all the terms of degree greater than or equal to m.

Definition 3: A subset of $\mathcal{U}_m^n$ denoted by $\mathcal{C}$ is called a linear code over $\mathcal{U}_m$ if $\mathcal{C}$ can be obtained through a generator matrix $\mathbf{G} \in \mathcal{U}_m^{k \times n}$ as

$$\mathcal{C} = \left\{ \mathbf{zG} \mid \forall \mathbf{z} \in \mathcal{U}_m^k \right\},$$

for some $k \leq n$ and the matrix multiplication is over the ring $\mathcal{U}_m$.

Using the above definitions, we now discuss the subject matter of this paper. Systematic use of binary error-correcting codes to construct some structured lattices is well known in the literature [1]. For example, the checkerboard lattice $\mathcal{D}_2 \subset \mathbb{R}^2$ can be constructed as (Chapter 4, Section 7, [1])

$$\mathcal{D}_2 = 2\mathbb{Z}^2 \oplus \mathcal{L},$$

where $\mathcal{L} = \{\psi(\mathbf{c}) \mid \forall \mathbf{c} \in \mathcal{C}\}$ is an Euclidean code obtained by embedding the codewords of $\mathcal{C}$ the repetition code **(2, 1, 2)** over $\mathbb{F}_2 = \{\mathbf{0}, \mathbf{1}\}$ into the Euclidean space using the mapping $\psi : \mathbb{F}_2 \to \mathbb{Z}$ such that $\psi(\mathbf{0}) = 0$ and $\psi(\mathbf{1}) = 1$. Depending on the structure of the underlying linear error correcting codes, lattice construction can be categorized into different types [1]. In this paper, we consider a special class of constructions called *Construction A* which is defined formally as follows:

Definition 4: (Sec. 2, Chapter 5, [1]) A lattice Λ over $\mathbb{Z}$ is obtained as Construction A from the binary linear code $\mathcal{C}$ if Λ can be represented as

$$\Lambda = 2\mathbb{Z}^n \oplus \mathcal{L}, \tag{1}$$

where $\mathcal{L} = \{\psi(\mathbf{c}) \mid \forall \mathbf{c} \in \mathcal{C}\} \subset \mathbb{Z}^n$ is an Euclidean code obtained by the component-wise mapping $\psi : \mathbb{F}_2 \to \mathbb{Z}$ given by $\psi(\mathbf{0}) = 0$ and $\psi(\mathbf{1}) = 1$ on the alphabet of $\mathcal{C}$.

In the above definition, the linear code $\mathcal{C}$ is restricted to be over $\mathbb{F}_2$ and Λ is viewed as a lattice over $\mathbb{Z}$. However, in general, we could also view Λ as a complex lattice, i.e., as a lattice over $\mathbb{Z}[i]$, and construct Λ using linear code $\mathcal{C}$ over *finite rings*. We introduce a new construction of lattices by relaxing the constraint on the alphabet of the linear code $\mathcal{C}$. Our construction is an extension of Construction A and hence, we refer it as Construction A'. For the most generalized

978-1-4673-2579-0/12/$31.00 ©2012 IEEE

definition of Construction A, we refer the reader to [3]. We use an abstract ring $\mathcal{R}$ to denote either $\mathbb{Z}$ - the ring of integers or $\mathbb{Z}[i]$ - the ring of Gaussian integers.

Definition 5: A lattice Λ over $\mathcal{R}$ is obtained through Construction A' from the linear code $\mathcal{C}$ over the alphabet $\mathcal{U}_m = \mathbb{F}_2[u]/u^m$ for some $m \geq 1$ if Λ can be represented as

$$\Lambda = u^m \mathcal{R}^n \oplus \mathcal{L}, \tag{2}$$

where $\mathcal{L} = \{\psi(\mathbf{c}) \mid \forall \mathbf{c} \in \mathcal{C}\} \subset \mathcal{R}^n$ is an Euclidean code obtained by using an appropriate mapping $\psi : \mathcal{U}_m \to \mathcal{R}$, and

$$u = \begin{cases} 2, \text{ if } \mathcal{R} = \mathbb{Z}, \\ 1+i, \text{ if } \mathcal{R} = \mathbb{Z}[i]. \end{cases}$$

Note that Construction A can be obtained as a special case from Construction A' when $m = 1$ and $\mathcal{R} = \mathbb{Z}$, wherein the embedding operation ψ coincides with the one in Definition 4.

In this paper, we provide Construction A' of Barnes-Wall lattice [1], [4], [5], [6], [7] of dimension 2^m for $m \geq 1$ by viewing it as a lattice over $\mathbb{Z}[i]$. In other words, we present the following key ingredients needed for Construction A' of Barnes-Wall lattices for every $m \geq 1$:

1) An appropriate linear code $\mathcal{C}_{2^m}$ over the alphabet $\mathcal{U}_m$.
2) A suitable mapping $\psi : \mathcal{U}_m \to \mathbb{Z}[i]$ in order to obtain the Euclidean code $\mathcal{L}_{2^m}$ with cubic shaping property.

Throughout the paper, unless specified, the dimension of the Barnes-Wall lattice refers to its rank as a lattice over $\mathbb{Z}[i]$.

We list the contributions and the organisation of the paper as given below:

- We introduce Construction A' of lattices (as in Definition 5) which facilitates us to generate some well structured lattices from linear codes over *finite rings*. As an immediate application, we apply Construction A' to obtain Barnes-Wall lattices of dimension 2^m by embedding a linear code $\mathcal{C}_{2^m}$ over the quotient ring $\mathcal{U}_m$ to a Euclidean code in $\mathbb{Z}[i]^{2^m}$ for any $m \geq 1$ (Section II)
- First, we identify the structure of the linear code $\mathcal{C}_{2^m}$ by using Construction D of Barnes-Wall lattices. Subsequently, we provide a linear encoder to map the information bits onto the codewords of $\mathcal{C}_{2^m}$. We identify that the generator matrix for $\mathcal{C}_{2^m}$ is given by
$$\mathbf{G}_{2^m} = \begin{bmatrix} 1 & 1 \\ 0 & u \end{bmatrix}^{\otimes m},$$
where the tensor operation is over $\mathcal{U}_m$ (Section II). We also prove the equivalence of our encoding technique to Construction D (Section III).
- To find out ψ and $\mathcal{L}_{2^m}$, we first obtain the Euclidean code
$$\mathcal{EC}_{2^m} = \{\Phi(\mathbf{c}) \mid \forall \mathbf{c} \in \mathcal{C}_{2^m}\} \subset \mathbb{Z}[i]^{2^m},$$
through the mapping $\Phi : \mathcal{U}_m \to \mathbb{Z}[i]$ as
$$\Phi\left(\sum_{j=0}^{m-1} b_j u^j\right) = \sum_{j=0}^{m-1} b_j \left(\Phi(u)\right)^j,$$
with $\Phi(u) = 1 + i$. At this stage, we point out that $\mathcal{EC}_{2^m}$ is an arbitrary subset of BW_{2^m} and does not have cubic shaping. To fix this problem, we provide a one-one mapping $\phi : \mathcal{EC}_{2^m} \to \mathcal{L}_{2^m} \subset BW_{2^m}$ such that $\mathcal{L}_{2^m}$ has cubic shaping property for even values of m (Section IV). With this, the mapping ψ (as in Definition 5) is the composition mapping $\phi(\Phi(\cdot))$ on $\mathcal{U}_m$, and we show that BW_{2^m} is obtained as
$$BW_{2^m} = (1+i)^m \mathbb{Z}[i]^{2^m} \oplus \mathcal{L}_{2^m}.$$

More details on this work can be found in [8]. Apart from providing further details on Construction A' of Barnes-Wall lattices, a thorough study on the performance of Euclidean codes from Barnes-Wall lattice constellations is also reported in [8].

Notations: Throughout the paper, boldface letters and capital boldface letters are used to represent vectors and matrices, respectively. For a complex matrix $\mathbf{X}$, the matrices $\mathbf{X}^T$, $\Re(\mathbf{X})$ and $\Im(\mathbf{X})$ denote, respectively, the transpose, real part and imaginary part of $\mathbf{X}$. For a vector $\mathbf{x}$, we use $\mathbf{x}_j$ to represent the j-th component of $\mathbf{x}$. The set of all integers, the real numbers, and the complex numbers are, respectively, denoted by $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$, and $i = \sqrt{-1}$. Cardinality of a set $\mathcal{S}$ is denoted by $|\mathcal{S}|$. Absolute value of a complex number x is denoted by $|x|$. The number of ways of picking n objects out of m objects is denoted by C_n^m. The n-length zero vector is denoted by $\mathbf{0}_n$

II. Construction A' of Barnes-Wall lattice

First, we recall Construction D of Barnes-Wall lattices, and subsequently propose its Construction A' from a suitable code.

A. Construction D of Barnes-Wall lattice

Barnes-Wall lattice can be obtained via Construction D [4] as a $\mathbb{Z}[i]$ lattice as follows: Suppose we want to construct the lattice BW_{2^m} of dimension 2^m where $m \geq 1$, let $\mathcal{RM}(r, m)$ be the binary Reed-Muller (RM) code (Sec. 3.7, Chapter 3, [2]) of length 2^m and of order $0 \leq r \leq m$. With this, BW_{2^m} can be constructed as in (3) given at the top of next page, where $\psi(\cdot)$ is as given in Definition 4. For notational convenience, we also write (3) as

$$BW_{2^m} = (1+i)^m \mathbb{Z}[i]^{2^m} \oplus \bigoplus_{r=0}^{m-1} (1+i)^r \mathcal{RM}(r, m). \tag{4}$$

This method generates BW_{2^m} as a multi-level structure of nested RM codes and hence it falls under Construction D [1].

Example 1: BW_4 (which is also known as E_8 over $\mathbb{Z}$) is constructed as

$$BW_4 = (1+i)^2 \mathbb{Z}[i]^4 \oplus (1+i)\mathcal{RM}(1,2) \oplus \mathcal{RM}(0,2),$$

where the code $\mathcal{RM}(1,2) =$ **(4, 3, 2)** and the code $\mathcal{RM}(0,2) =$ **(4, 1, 4)** in the classical $(\mathbf{n}, \mathbf{k}, \mathbf{d_{min}})$ format.

Example 2: BW_{16} is obtained as

$$BW_{16} = (1+i)^4 \mathbb{Z}[i]^{16} \oplus (1+i)^3 \mathbf{(16,\ 15,\ 2)} \oplus (1+i)^2 \mathbf{(16,\ 11,\ 4)} \oplus (1+i) \mathbf{(16,\ 5,\ 8)} \oplus \mathbf{(16,\ 1,\ 6)}.$$

$$BW_{2^m} = \left\{ (1+i)^m \mathbf{a} + \sum_{r=0}^{m-1} (1+i)^r \psi(\mathbf{c}_r) \mid \forall \mathbf{c}_r \in \mathcal{RM}(r,m), \forall \mathbf{a} \in \mathbb{Z}[i]^{2^m} \right\} \quad (3)$$

B. Construction A'

In order to obtain BW_{2^m} as Construction A', we first need to find a suitable linear code $\mathcal{C}_{2^m}$ over an appropriate ring. To find such a code, we are interested in understanding the following expression in (4),

$$\mathcal{EC}_{2^m} = \bigoplus_{r=0}^{m-1} (1+i)^r \mathcal{RM}(r,m), \quad (5)$$

as a single code. If we denote $u = 1+i$ and consider u as a *symbol*, then the expression

$$\sum_{r=0}^{m-1} u^r \mathcal{RM}(r,m), \quad (6)$$

can be viewed as a code denoted by $\mathcal{C}_{2^m}$ over the ring $\mathcal{U}_m$.

Example 3: For BW_4, the code $\mathcal{C}_4$ is given by u**(4, 3, 2)**$+$**(4, 1, 4)**, which can be viewed as a code over the quotient ring $\mathcal{U}_2$.

Example 4: Another example is $\mathcal{C}_{16}$, which is obtained from BW_{16} and is given by

$\mathcal{C}_{16} =$ **(16, 1, 6)**$+u$**(16, 5, 8)**$+u^2$**(16, 11, 4)**$+u^3$**(16, 15, 2)**,

where $\mathcal{C}_{16}$ is defined over $\mathcal{U}_4$.

In general, the ring on which the code

$$\mathcal{C}_{2^m} = \sum_{r=0}^{m-1} u^r \mathcal{RM}(r,m) \quad (7)$$

is defined is the quotient ring $\mathcal{U}_m$. With this, we have identified the linear code $\mathcal{C}_{2^m}$ to be useful for Construction A' of BW_{2^m}.

In the rest of this subsection, we provide a linear encoder to generate the codewords of $\mathcal{C}_{2^m}$. It is known that the 2^m-dimensional Barnes-Wall lattice BW_{2^m} over $\mathbb{Z}[i]$ is generated by the rows of the m-fold Kronecker product [6]

$$\mathbf{G} = \begin{bmatrix} 1 & 1 \\ 0 & (1+i) \end{bmatrix}^{\otimes m}.$$

Replacing $u = 1+i$ as a *symbol* and making $u^m = 0$ in $\mathbf{G}$, we obtain the generator matrix $\mathbf{G}_{2^m}$ which can be viewed as a matrix over $\mathcal{U}_m$.

Example 5: The generator matrix $\mathbf{G}_4$ is given by

$$\mathbf{G}_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & u & 0 & u \\ 0 & 0 & u & u \\ 0 & 0 & 0 & 0 \end{bmatrix} \in \mathcal{U}_2^{4\times 4}.$$

By using $\mathbf{G}_{2^m}$ as a matrix over $\mathcal{U}_m$, the code $\mathcal{C}_{2^m}$ is obtained as below:

Encoding of $\mathcal{C}_{2^m}$: Let $\mathbf{z} \in \mathcal{U}_m^{2^m}$, i.e., the j-th component of $\mathbf{z}$ is given by

$$\mathbf{z}_j = \sum_{k=0}^{m-1} b_{k,j} u^k, \quad (8)$$

where $b_{k,j} \in \mathbb{F}_2$ for all k, j. Using $\mathbf{z}$ and $\mathbf{G}_{2^m}$, the code $\mathcal{C}_{2^m} \subset \mathcal{U}_m^{2^m}$ can be obtained as

$$\mathcal{C}_{2^m} = \left\{ \mathbf{x} = \mathbf{z}\mathbf{G}_{2^m} \mid \forall \mathbf{z} \in \mathcal{U}_m^{2^m} \right\}, \quad (9)$$

where the matrix multiplication is over $\mathcal{U}_m$.

Proposition 1: The rate of the code $\mathcal{C}_{2^m}$ in bits per codeword is $(\frac{m}{2})2^m$.

Proof: Each component of $\mathbf{z}$ carries m information bits in the variables $b_{k,j}$ as shown in (8). This amounts to a total of $m2^m$ bits carried by $\mathbf{z}$. However, since the matrix multiplication is over $\mathcal{U}_m$, not all the information bits $b_{k,j}$ are encoded as codewords of $\mathcal{C}_{2^m}$ (due to $u^m = 0$). Using the structure of $\mathbf{G}_{2^m}$ it is possible to identify the indices (k, j) of information bits $b_{k,j}$ which get encoded into the codewords of $\mathcal{C}_{2^m}$ as follows: Let the set $\mathcal{I}_q$ denote the indices of the rows of $\mathbf{G}_{2^m}$ whose components take values from the binary set $\{0, u^q\}$ for $q = 0, 1, \cdots m-1$. Due to the quotient operation $u^m = 0$, the components of $\mathbf{z}$ which are in the index set $\mathcal{I}_q$ are restricted to be of the form, $\mathbf{z}_j = \sum_{k=0}^{m-1-q} b_{k,j} u^k \ \forall j \in \mathcal{I}_q$. For example, $\mathbf{z}_1 = \sum_{k=0}^{m-1} b_{k,1} u^k$ and $\mathbf{z}_{2^m} = 0$. Using the structure of $\mathbf{G}_{2^m}$ we observe that $|\mathcal{I}_q| = C_q^m$, and hence find the total number of information bits on a codeword of $\mathcal{C}_{2^m}$ as $\sum_{k=0}^{m} (m-k) C_k^m$. Therefore, the rate of $\mathcal{C}_{2^m}$ in bits per codeword is $\sum_{i=0}^{m-1} C_i^m (m-i) = \frac{m}{2} 2^m$. ■

We now provide an example for the proposed encoding technique, showcasing the positions of the information bits that get encoded to the codewords of $\mathcal{C}_{2^m}$.

Example 6: For $m = 3$, the input vector $\mathbf{z}$ and $\mathbf{G}_8$ are of the form,

$$\mathbf{z}^T = \begin{bmatrix} b_{0,1} + b_{1,1}u + b_{2,1}u^2 \\ b_{0,2} + b_{1,2}u \\ b_{0,3} + b_{1,3}u \\ b_{0,4} \\ b_{0,5} + b_{1,5}u \\ b_{0,6} \\ b_{0,7} \\ 0 \end{bmatrix} \text{ and}$$

$$\mathbf{G}_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & u & 0 & u & 0 & u & 0 & u \\ 0 & 0 & u & u & 0 & 0 & u & u \\ 0 & 0 & 0 & u^2 & 0 & 0 & 0 & u^2 \\ 0 & 0 & 0 & 0 & u & u & u & u \\ 0 & 0 & 0 & 0 & 0 & u^2 & 0 & u^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & u^2 & u^2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

III. On Equivalence of Construction A' to Construction D

In this subsection, we prove the equivalence of our encoding technique to Construction D. In other words, the following theorem shows that the codewords generated in (9) can be uniquely represented as vectors of a multi-level code of nested RM codes as in (7).

Theorem 1: The codewords generated in (9) can be uniquely represented as codewords obtained through Construction D.

Proof: The entries of $\mathbf{G}_{2^m}$ take values from the set $\{0, 1, u, u^2, \cdots u^{m-1}\}$. After suitable row permutations, $\mathbf{G}_{2^m}$ can be written as

$$\mathbf{G}_{2^m} = \begin{bmatrix} \mathbf{R}_0 \\ u\mathbf{R}_1 \\ \vdots \\ u^{m-1}\mathbf{R}_{m-1} \\ u^m\mathbf{R}_m \end{bmatrix}, \tag{10}$$

where $\mathbf{R}_k \in \mathbb{F}_2^{C_k^m \times 2^m}$. Note that $[\mathbf{R}_0^T \ \mathbf{R}_1^T \ \cdots \ \mathbf{R}_r^T]^T$ is a generator matrix of the r-th order RM code for $r \leq m$. Recalling the encoding technique, the code $\mathcal{C}_{2^m}$ is obtained as

$$\mathcal{C}_{2^m} = \{\mathbf{x} = \mathbf{z}\mathbf{G}_{2^m} \mid \forall \ \mathbf{z} \in \mathcal{U}_m^{2^m}\}$$

where the matrix multiplication is over $\mathcal{U}_m$. The vector $\mathbf{z}$ can be written as $\mathbf{z} = \mathbf{u}\mathbf{B}$, where

$$\mathbf{u} = \begin{bmatrix} 1 & u & u^2 & \cdots & u^{m-2} & u^{m-1} \end{bmatrix} \in \mathcal{U}_m^{1\times m}$$

and

$$\mathbf{B} = \begin{bmatrix} b_{0,0} & b_{0,1} & \cdots & b_{0,2^m-2} & b_{0,2^m-1} \\ b_{1,0} & b_{1,1} & \cdots & b_{1,2^m-2} & b_{1,2^m-1} \\ b_{2,0} & b_{2,1} & \cdots & b_{2,2^m-2} & b_{2,2^m-1} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ b_{m-2,0} & b_{m-2,1} & \cdots & b_{m-2,2^m-2} & b_{m-2,2^m-1} \\ b_{m-1,0} & b_{m-1,1} & \cdots & b_{m-1,2^m-2} & b_{m-1,2^m-1} \end{bmatrix} \in \mathbb{F}_2^{m\times 2^m}.$$

Note that $b_{k,j}$ are the information bits to be encoded into codewords of $\mathcal{C}_{2^m}$. We split the information matrix $\mathbf{B}$ as $[\mathbf{B}_0 \ \mathbf{B}_1 \ \cdots \ \mathbf{B}_m]$ where $\mathbf{B}_k \in \mathbb{F}_2^{m\times C_k^m}$ for $k = 0, 1, \cdots m$. After the above split, the BW lattice vector $\mathbf{x}$ is obtained as

$$\mathbf{x} = \mathbf{u}[\mathbf{B}_0 \ \mathbf{B}_1 \ \cdots \ \mathbf{B}_m] \begin{bmatrix} \mathbf{R}_0 \\ u\mathbf{R}_1 \\ \vdots \\ u^{m-1}\mathbf{R}_{m-1} \\ u^m\mathbf{R}_m \end{bmatrix}.$$

The R.H.S of the above operation can be alternately written as

$$\mathbf{x} = \mathbf{u}[\bar{\mathbf{B}}_0 \ \bar{\mathbf{B}}_1 \ \cdots \ \bar{\mathbf{B}}_m] \underbrace{\begin{bmatrix} \mathbf{R}_0 \\ \mathbf{R}_1 \\ \vdots \\ \mathbf{R}_{m-1} \\ \mathbf{R}_m \end{bmatrix}}_{\mathbf{G}_{RM}},$$

where $\bar{\mathbf{B}}_k = \begin{bmatrix} \mathbf{0}_{k\times C_k^m} \\ \mathbf{B}_k([1:m-k],:) \end{bmatrix}$. Note that $\mathbf{G}_{RM}$ is the nested RM generator matrix. We use the notation $\bar{\mathbf{B}} = [\bar{\mathbf{B}}_0 \ \bar{\mathbf{B}}_1 \ \cdots \ \bar{\mathbf{B}}_m]$. We also point out that the informations bits in each row of $\bar{\mathbf{B}}$ are encoded to RM codewords of appropriate order by the matrix multiplication $\bar{\mathbf{B}}\mathbf{G}_{RM}$. Due to zero entries in $\bar{\mathbf{B}}$, the matrix $\bar{\mathbf{B}}$ has only $\sum_{n=0}^{k-1} C_n^m$ information bits in the k-th row of $\bar{\mathbf{B}}$ for $k = 1, 2, \cdots m$. Since, these $\sum_{n=0}^{k-1} C_n^m$ bits are placed in the first as many columns of $\bar{\mathbf{B}}$, the information bits in the k-th row of $\bar{\mathbf{B}}$ are encoded into a RM codeword of $(k-1)$-th order. Finally, on the multiplication of $\mathbf{u}$ from left, the generated RM codewords are appropriately weighed by powers of u and added. This proves the equivalence of our construction to Construction D. ■

Till now, we have identified the linear code $\mathcal{C}_{2^m}$ and its encoding technique over the quotient ring $\mathcal{U}_m$. In the next subsection, we discuss embedding of $\mathcal{C}_{2^m}$ into the Euclidean space $\mathbb{Z}[i]^{2^m}$.

IV. Embedding to Barnes-Wall Lattice and Cubic Shaping

By using the map $\Phi(u) = 1 + i$ on $\mathcal{C}_{2^m}$, we get a Euclidean code given by

$$\begin{aligned} \mathcal{EC}_{2^m} &= \{\Phi(\mathbf{c}) \mid \forall \mathbf{c} \in \mathcal{C}_{2^m}\} \in \mathbb{Z}[i]^{2^m}, \\ &= \bigoplus_{r=0}^{m-1} (1+i)^r \mathcal{RM}(r, m), \end{aligned} \tag{11}$$

where Φ maps the symbols of $\mathcal{U}_m$ into $\mathbb{Z}[i]$ as

$$\Phi\left(\sum_{j=0}^{m-1} b_j u^j\right) = \sum_{j=0}^{m-1} b_j \left(\Phi(u)\right)^j. \tag{12}$$

It is to be noted that $\mathcal{EC}_{2^m}$ is an arbitrary subset of BW_{2^m} and does not have cubic shaping. To fix this problem, we propose a one-one mapping ϕ on $\mathcal{EC}_{2^m}$ to obtain a new Euclidean code denoted by $\mathcal{L}_{2^m}$ such that $\mathcal{L}_{2^m}$ has cubic shaping when m is even. For any $\mathbf{x} = [x_1, x_2, x_3, \cdots, x_{2^m}] \in \mathcal{EC}_{2^m}$, the mapping ϕ operates on each component of $\mathbf{x}$ as,

$$\phi(x_j) = \begin{cases} x_j \bmod 2^{\frac{m}{2}}, \text{ when } m \text{ is even;} \\ \varphi\left(x_j \bmod 2^{\frac{m+1}{2}}\right), \text{ when } m \text{ is odd,} \end{cases} \tag{13}$$

where $\varphi(\cdot)$ is defined on $\mathbb{Z}_{2^{\frac{m+1}{2}}}[i]$ as,

$$\varphi(z) = \begin{cases} z, \text{ when } \Im(z) < 2^{\frac{m-1}{2}}; \\ z + \left(2^{\frac{m-1}{2}} - i2^{\frac{m-1}{2}}\right), \text{ when } \Re(z) < 2^{\frac{m-1}{2}} \\ \quad \text{and } \Im(z) \geq 2^{\frac{m-1}{2}}; \\ z - \left(2^{\frac{m-1}{2}} + i2^{\frac{m-1}{2}}\right), \text{ when } \Re(z) \geq 2^{\frac{m-1}{2}} \\ \quad \text{and } \Im(z) \geq 2^{\frac{m-1}{2}}. \end{cases} \tag{14}$$

The mapping ϕ guarantees the following property on $\mathcal{L}_{2^m}$:

$$\mathcal{L}_{2^m} \subset \begin{cases} \left\{\mathbb{Z}_{2^{\frac{m}{2}}}[i]\right\}^{2^m}, \text{ if } m \text{ is even;} \\ \{\mathbb{Z}_{2^{\frac{m+1}{2}}}\}^{2^m} + i\{\mathbb{Z}_{2^{\frac{m-1}{2}}}\}^{2^m}, \text{ if } m \text{ is odd.} \end{cases} \tag{15}$$

From (15), note that each component of the vector in $\mathcal{L}_{2^m}$ is in a cubic box and a rectangular box, when m is even and odd, respectively. With this, the mapping ψ (given in Definition 5) needed to obtain the Euclidean code $\mathcal{L}_{2^m}$ from $\mathcal{C}_{2^m}$ can be written as

$$\psi = \phi(\Phi(\cdot)), \tag{16}$$

where Φ and ϕ are given in (12) and (13) respectively.

Proposition 2: The rate of the Euclidean code $\mathcal{L}_{2^m}$ in bits per complex dimension is $\frac{m}{2}$.

Proof: The proof follows from the one-one nature of ψ and the result of Proposition 1. For the proof on the one-one nature of ψ, we refer the reader to Proposition 2 of [8]. ■

Remark 1: We point out that Construction A' does not qualify to be the generalized Construction A of [3] since the proposed embedding operation ψ is not a linear map.

The following theorem shows that ψ retains the Barnes-Wall lattice structure on $\mathcal{L}_{2^m}$ and proves Construction A' of BW_{2^m}.

Theorem 2: The Euclidean code $\mathcal{L}_{2^m}$ and the lattice BW_{2^m} are related as $BW_{2^m} = (1+i)^m\mathbb{Z}[i]^{2^m} \oplus \mathcal{L}_{2^m}$.

Proof: Consider the case when m is even. From (3) and (11), any $\mathbf{z} \in BW_{2^m}$ can be written as

$$\mathbf{z} = (1+i)^m\mathbf{a} + \mathbf{x}, \tag{17}$$

where $\mathbf{a} \in \mathbb{Z}[i]^{2^m}$ and $\mathbf{x} \in \mathcal{EC}_{2^m}$. Further, upon the modulo operation in (13), $\mathbf{x}$ satisfies $\mathbf{x} = 2^{\frac{m}{2}}\mathbf{r} + \phi(\mathbf{x})$, where $\phi(\mathbf{x}) \in \mathcal{L}_{2^m}$ and $\mathbf{r} \in \mathbb{Z}[i]^{2^m}$. This implies

$$\phi(\mathbf{x}) = \mathbf{x} - 2^{\frac{m}{2}}\mathbf{r} = \mathbf{x} + (1+i)^m\mathbf{r}', \tag{18}$$

for some $\mathbf{r}' \in \mathbb{Z}[i]^{2^m}$. The second equality follows as

$$(1+i)^m = a2^{\frac{m}{2}} \text{ where } a \in \{1, -1, i, -i\}. \tag{19}$$

The R.H.S of (18) is in the form of (3) and hence $\mathcal{L}_{2^m} \subset BW_{2^m}$. Further, combining (17) and (18), we have

$$\mathbf{z} = (1+i)^m\mathbf{a}' + \phi(\mathbf{x}), \tag{20}$$

for some $\mathbf{a}' \in \mathbb{Z}[i]^{2^m}$ and $\phi(\mathbf{x}) \in \mathcal{L}_{2^m}$. From (15), we also observe that

$$(1+i)^m\mathbb{Z}[i]^{2^m} \cap \mathcal{L}_{2^m} = 2^{\frac{m}{2}}\mathbb{Z}[i]^{2^m} \cap \mathcal{L}_{2^m} = \{\mathbf{0}_{2^m}\}. \tag{21}$$

The first equality in the above equation follows from (19). With (20) and (21), the statement of the theorem follows when m is even.

We now consider the case when m is odd. For this case, we first study the mod $2^{\frac{m+1}{2}}$ operation in (13), and subsequently study the effect of φ. With the mod operation, any $\mathbf{x} \in \mathcal{EC}_{2^m}$ satisfies $\mathbf{x} = 2^{\frac{m+1}{2}}\mathbf{r} + \bar{\mathbf{x}}$, where $\bar{\mathbf{x}} \in \mathbb{Z}_{2^{\frac{m+1}{2}}}[i]^{2^m}$ and $\mathbf{r} \in \mathbb{Z}[i]^{2^m}$. This implies

$$\bar{\mathbf{x}} = \mathbf{x} - 2^{\frac{m+1}{2}}\mathbf{r} = \mathbf{x} + (1+i)^m\mathbf{r}', \tag{22}$$

for some $\mathbf{r}' \in \mathbb{Z}[i]^{2^m}$. The second equality follows as $2^{\frac{m+1}{2}} = a\cdot(1+i)^m$ for some $a \in \mathbb{Z}[i]$. We point out that $\bar{\mathbf{x}}$ is already a Barnes-Wall lattice point. Further, the constants added in (14) are such that

$$2^{\frac{m-1}{2}}(1-i) = a\cdot(1+i)^m \text{ and } 2^{\frac{m-1}{2}}(1+i) = b\cdot(1+i)^m$$

for some $a, b \in \mathbb{Z}[i]$. Therefore, $\varphi(\bar{\mathbf{x}})$ continues to be a Barnes-Wall lattice point. We also know that $\mathbf{x} = (1+i)^m\mathbf{r} + \phi(\mathbf{x})$, for some $\mathbf{r} \in \mathbb{Z}[i]^{2^m}$ and $\phi(\mathbf{x}) \in \mathcal{L}_{2^m}$. Finally, from (15), we have

$$(1+i)^m\mathbb{Z}[i]^{2^m} \cap \mathcal{L}_{2^m} = 2^{\frac{m-1}{2}}(1+i)\mathbb{Z}[i]^{2^m} \cap \mathcal{L}_{2^m} = \{\mathbf{0}_{2^m}\}.$$

The first equality in the above equation follows as $(1+i)^m$ is of the form $a2^{\frac{m-1}{2}}$ where $a = \pm 1 \pm i$. This completes the proof when m is odd. ■

Using the results of Theorem 2, the Construction A' of BW_{2^m} is given by $BW_{2^m} = (1+i)^m\mathbb{Z}[i]^{2^m} \oplus \mathcal{L}_{2^m}$, where $\mathcal{L}_{2^m}$ is the Euclidean code obtained from $\mathcal{C}_{2^m}$ through the mapping $\psi = \phi(\Phi(\cdot))$ on $\mathcal{U}_m$.

V. Conclusion

In this paper, we have introduced an extension of Construction A to obtain the class of Barnes-Wall lattices from linear codes over rings. We highlight that the mapping ψ provides the cubic shaping property on the Euclidean code, which in turn facilitates labelling of information bits if the Euclidean code is to be used as a coded modulation scheme.

Acknowledgment

This work was performed within the Monash Software Defined Telecommunications Lab and supported by the Monash Professional Fellowship 2011.

References

[1] J.H. Conway and N.J.A Sloane, *Sphere Packings, Lattices and Groups*, Second Edition, 1993, Springer-Verlag, New York.

[2] R. E. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley Publishing Company, Inc, 1983.

[3] G.D. Forney, and A. Vardy, "Generalized Minimum-Distance Decoding of Euclidean-Space Codes and Lattices", *IEEE Transactions on Information Theory*, vol. 42, no. 6, Nov. 1996, pp. 1992 - 2026.

[4] G.D. Forney, "Coset Codes- Part II: Binary Lattices and Related Codes", *IEEE Transactions on Information Theory*, vol. 34, no. 5, Sept. 1988, pp. 1152 - 1187.

[5] G. Nebe, E. M. Rains and N. J. A. Sloane, "A Simple Construction of the Barnes-Wall Lattices", in *Codes, Graphs, and Systems: A Celebration of the Life and Career of G. David Forney, Jr. on the Occasion of his Sixtieth Birthday*, ed. R. E. Blahut and R. Koetter, Kluwer, 2002, pp. 333-342.

[6] D. Micciancio, and A. Nicolsi, "Efficient Bounded Distance Decoders for Barnes-Wall Lattices", in the Proc. of *IEEE ISIT 2008*, Toronto, Canada, July 6-11, 2008.

[7] A. J. Salomon, and O. Amrani, "Augmented Product Codes and Lattices: Reed-Muller Codes and Barnes-Wall Lattices", *IEEE Transactions on Information Theory*, vol. 51, no. 11, Nov. 2005, pp. 3918 - 3930.

[8] J. Harshan, E. Viterbo, and J.-C. Belfiore, "Practical Encoders and Decoders for Euclidean Codes from Barnes-Wall Lattices," available on arXiv:1203.3282v2 [cs.IT], March 2012.