Abstract—Motivated by applications in reliable and secure communication, we address the problem of tiling (or partitioning) a finite constellation in $\mathbb{Z}_n^L$ by subsets, in the case that the constellation does not possess an abelian group structure. The property that we do require is that the constellation is generated by a linear code through an injective mapping. The intrinsic relation between the code and the constellation provides a sufficient condition for a tiling to exist. We also present a necessary condition. Inspired by a result in group theory, we discuss results on tiling for the particular case when the finer constellation is an abelian group as well.

I. INTRODUCTION

The problem of tiling consists of factorizing (or partitioning) a group into sets such that their intersection is just the identity element of the group. This problem attracted a lot of attention since Hajós [6] reduced the Minkowski study of filling $\mathbb{R}^n$ by congruent cubes to the factorization of finite groups. Since then, several authors [10], [13], [15], [17] contributed towards this solution, but many circumstances are still unsolved.

Besides the mathematical interest around tiling, including the estimation of Ramsey number of graphs [17], applications in coding theory are also well established. Connections between tilings and perfect codes were addressed in [2], for tilings of $\mathbb{F}_2^n$ with the Hamming metric and in [16], for tilings of general lattices by their sublattices with the Euclidean metric. Tilings of finite abelian groups were also explored in [13] in the context of public key cryptography.

The motivation to our study comes from the wiretap channel, which is a model of communication that concerns both reliability and security. First introduced by Wyner [19], the assumption is that the transmitter aims to send a message to a receiver through a main channel, which is connected to an eavesdropper. The general idea is to construct an encoder and decoder to jointly optimize the data transmission and the equivocation seen by the illegitimate receiver. This tradeoff, denoted by secrecy capacity, was proved to be achieved with random coding arguments and an encoding scheme called coset encoding, where the transmitter encodes the message in terms of the corresponding syndrome. Several papers addressed this problem considering a variety of communication channels and coding schemes, including [9], [12], [18].

Tiling a vector space is always possible. For that reason, linear codes make for a natural alternative for coset encoding through their cosets. On the other hand, lattices with their group structure also admit such characterization and they have been used to demonstrate security properties on the wiretap Gaussian channel, as discussed in [8], [11]. Nevertheless, the receiver is supposed to perform a lattice decoding, which is known to be a hard problem. One approach to the lattice decoding problem is to select a constellation that allows an efficient decoding on the main channel, for example, Construction C (or multilevel code formula [4]), denoted by $\Gamma_C$. Asymptotically, Construction C achieves capacity at high SNR on the AWGN channel with multistage decoding [5].

Contributions: In general, $\Gamma_C$ produces a nonlattice constellation, generated by a finite set in $\mathbb{Z}_n^L$. Recently a subset $\Gamma_C \subseteq \Gamma_C$ was introduced [1], by associating the linear codes underlying both constructions. In this work, we discuss conditions for the existence of a tiling of $\Gamma_C$ by classes of $\Gamma_C$. One condition emerges from the linear code generating such constellations, as we can always tile a code with its cosets, but the second approach involves solving a pure mathematical tiling problem and taking into account the particular case where $\Gamma_C$ is an abelian group (or a lattice). While motivated by the potential application to the wiretap channel, the theoretical problem itself is the emphasis of this paper.

This paper is organized as follows: Sec. II presents preliminary definitions of codes, lattices, and also a way to map codes to constellations such as $\Gamma_C$. Sec. III recalls tiling properties of linear codes. Sec. IV explores a condition inherited from the linear code that guarantees the tiling for the most general form of $\Gamma_C$ (lattice and nonlattice). Sec. V focuses on the case where $\Gamma_C$ is an abelian group (lattice). Finally, Sec. VI concludes the paper.

II. MAPPING LINEAR CODES TO A CONSTELLATION

There are two essential mathematical concepts that underlie our work, which are linear codes and lattices.

Definition 1. A set $\mathcal{C} \subseteq \mathbb{F}_2^n$ is a binary linear $[n,k]$-code if it is a $k$-dimensional subspace of $\mathbb{F}_2^n$.

Definition 2. A lattice $\Lambda \subseteq \mathbb{R}^n$ is a discrete abelian subgroup of $\mathbb{R}^n$.

From now on, we will admit a linear code $\mathcal{C} \subseteq \mathbb{F}_2^n$ and split it into $L$ projection codes $\mathcal{C}_1, \ldots, \mathcal{C}_L$, where each $\mathcal{C}_i \subseteq \mathbb{F}_2^n$ is the restriction of $\mathcal{C}$ to coordinate positions $(i-1)n+1, \ldots, in$, where $i = 1, \ldots, L$. Accordingly, each codeword $c \in \mathcal{C}$ can be written as $c = (c_1, \ldots, c_L)$ with $c_i \in \mathcal{C}_i$.

The mapping $\psi : \mathbb{F}_2^n \rightarrow \mathbb{Z}_2^L$ defined as

$$\psi(c_1, \ldots, c_L) = c_1 + 2c_2 + \cdots + 2^{L-1}c_L,$$

associates a code $\mathcal{C} \subseteq \mathbb{F}_2^n$ to a finite constellation (not necessarily an abelian group), where each $c_i \in \mathbb{F}_2^n$. 

Tiling of Constellations

Maiara F. Bollauf and Øyvind Ytrehus

Simula UiB, N-5008, Bergen, Norway
Email: {maiara, oyvindy}@simula.no
Definition 3. Consider a linear code \( C \subset \mathbb{F}^{nL}_2 \). The infinite constellation defined by \( \Gamma_C \cdot \psi((C) + 2^LZ^n = Y + 2^LZ^n \) is called Construction \( \Psi'^* \).

Definition 4. Let \( \mathcal{C} = C_1 \times \cdots \times C_L \), where each \( C_i \subset \mathbb{F}^n_2 \) is the respective projection code of a linear code \( C \subset \mathbb{F}^{nL}_2 \), for \( i = 1, \ldots, L \). We denote by Construction \( C \) the set \( \Gamma_C = \psi(\mathcal{C}) + 2^LZ^n = X + 2^LZ^n \).

Throughout the paper, the subsets \( X \) and \( Y \) would always refer to \( X = \psi(\mathcal{C}) \) and \( Y = \psi(C) \), for \( \mathcal{C}, \mathcal{C} \subset \mathbb{F}^{nL}_2 \) as in Definitions 3 and 4.

Example 1. Consider \( C \subset \mathbb{F}^2_2 \), with \( n = 2, L = 3 \), given by

\[
C = \{(0, 0, 0, 0, 0, 0), (0, 0, 1, 0, 1, 0), (1, 1, 0, 0, 0, 0), (1, 1, 0, 1, 0, 0), (0, 0, 0, 1, 1, 1), (0, 0, 1, 1, 1, 1)\}.
\]

Here, generator matrices of the codes \( C, \mathcal{C}, C_1, C_2, \) and \( C_3 \) are given (respectively) by

\[
G = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}, \quad \mathcal{G} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad G_1 = (1 & 1), \quad G_2 = (0 & 1), \quad G_3 = (1 & 0).
\]

Observe that if \( C = \mathcal{C} \), then \( \Gamma_C = \Gamma_C \cdot \), however for any other case \( \Gamma_C \cdot \subset \Gamma_C \). Under general assumptions, both \( \Gamma_C \cdot \) and \( \Gamma_C \cdot \) are not lattice constellations. To discuss necessary and sufficient conditions such that \( \Gamma_C \cdot \) is a lattice, we need to define the Schur (or coordinate-wise) product.

Definition 5. The Schur product of \( x = (x_1, \ldots, x_n) \), \( y = (y_1, \ldots, y_n) \in \mathbb{F}^2_2 \) is \( x \circ y = (x_1y_1, \ldots, x_ny_n) \in \mathbb{F}^2_2 \).

A chain of linear codes \( C_1 \subseteq \cdots \subseteq C_L \) is said to be closed under Schur product if for any two elements \( c_i, \tilde{c}_i \in C_i \), it is valid that \( c_i \circ \tilde{c}_i \in C_{i+1} \), for all \( i = 1, \ldots, L - 1 \). In Definition 4, \( \Gamma_C \cdot \) is a lattice if and only \( C_1 \subseteq \cdots \subseteq C_L \) and this chain is closed under Schur product 0.

Next, we are going to express operations in \( \mathbb{Z}^n_2 \) in terms of operations in \( \mathbb{F}^n_2 \).

If \( \phi : \mathbb{F}^2_2 \rightarrow \mathbb{Z}^n \) is the natural embedding, then \( \phi(x) + \phi(y) = \phi(x \circ y + 2\phi(x \circ y)) \), where \( \circ \) denotes the addition in \( \mathbb{F}^n_2 \) and \( + \) denotes the addition in \( \mathbb{Z}^n \). We will write \( x + y = x \circ y + 2(x \circ y) \) to simplify the notation.

Proposition 1. Consider \( C \subset \mathbb{F}^2_2 \) a linear code and the mapping \( \psi \) defined as in 1. Then, for \( c, \tilde{c} \in C \),

\[
\psi(c) + \psi(\tilde{c}) = \psi(c \circ \tilde{c}) + 2\psi(c \circ \tilde{c}),
\]

Proof. We have by definition that

\[
\psi(c + \tilde{c}) = (c_1 \circ \tilde{c}_1) + \cdots + 2^{L-1}(c_{L-1} \circ \tilde{c}_{L-1})
\]

\[
= (c_1 + \tilde{c}_1 - 2(c_1 \circ \tilde{c}_1)) + \cdots + 2^{L-1}(c_{L-1} + \tilde{c}_{L-1} - 2(c_{L-1} \circ \tilde{c}_{L-1}))
\]

\[
= (c_1 + \cdots + 2^{L-1}c_{L-1}) + (c_1 + \cdots + 2^{L-1}c_{L-1}) - 2((c_1 \circ \tilde{c}_1) + \cdots + 2^{L-1}(c_{L-1} \circ \tilde{c}_{L-1}))
\]

\[
= \psi(c) + \psi(\tilde{c}) - 2\psi(c \circ \tilde{c}).
\]

Besides this operation, it will be helpful to establish the notion of level shift.

Definition 6. Given a codeword \( c = (c_1, \ldots, c_L) \in C \subset \mathbb{F}^n_2 \), we define

\[
c(i) = (0, 0, \ldots, 0, c_1, \ldots, c_{L-i-1}, c_{L-i})
\]

as the \((i\text{-th})\) level shift of the codeword \( c \), for any \( i = 1, \ldots, L - 1 \).

For example, \( c(1) = (0, c_1, \ldots, c_{L-1}) \) and \( c^{(L-1)} = (0, 0, \ldots, c_1) \). From this definition, it is clearly valid that \( \psi(c) = \psi(c^{(1)}) \). Throughout the paper, we will also refer to the Schur level shift, which means that, given \( c \circ \tilde{c} = (c_1 \circ \tilde{c}_1, \ldots, c_{L-1} \circ \tilde{c}_{L-1}) \), then \( c \circ \tilde{c}^{(1)} = (0, c_1 \circ \tilde{c}_1, \ldots, c_{L-1} \circ \tilde{c}_{L-1}) \), for \( c, \tilde{c} \in \mathbb{F}^2_2 \).

From Proposition 1 it might also be necessary to work with the representation of a negative number in \( \mathbb{Z}^n_2 \). For this reason, we use the two’s complement as follows

\[
-\psi(c) = \psi((1, 1, \ldots, 1) \circ c) + \psi(1, 0, \ldots, 0)
\]

\[
= \psi((1, 1, \ldots, 1) \circ c \circ (1, 0, \ldots, 0)) + 2\psi((1, 1, \ldots, 1) \circ c) \circ (1, 0, \ldots, 0)).
\]

Then, \( u = 0 \) or \( u = (1, 0, \ldots, 0) \) and

\[
\psi(u)(0, 1, 0, \ldots, 1) \circ c, \quad \text{if} \quad u = 0
\]

\[
\psi((0, 1, 0, \ldots, 1) \circ c) + \psi(0, 1, 0, \ldots, 0), \quad \text{otherwise.}
\]

The overall idea is to write \( -\psi(c) = \psi(c') \), for a given \( c \in C \) and \( c' \in \mathcal{C} \). If the first case of 1 holds, then immediately \( c' = (0, 1, \ldots, 1) \circ c \). Otherwise, one needs to apply recursively the result of Proposition 1 to \( \psi((0, 1, \ldots, 1) \circ c) + \psi(0, 1, 0, \ldots, 0) \), until the Schur product vanishes and the value of \( c' \) is found.

III. TILING OF \( \mathcal{C} \) WITH COSETS OF \( C \)

We start by defining formally tiling of finite abelian groups.

Definition 7. A tiling of a finite abelian group \( G \subset \mathbb{R}^n \) is a pair \( (A, B) \) of subsets of \( G \) such that \( A \cap B = \{0\} \) and every \( g \in G \) can be uniquely written as \( g = a + b, a \in A, b \in B \). Then say that \( (A, B) \) is a tiling of \( G \).

Let \( |C| = 2^n \) and \( |\mathcal{C}| = |C_1 \times \cdots \times C_L| = 2^n \), where \( m < m = \sum_{i=1}^L \dim(C_i) \).
Due to the fact that $C$ is an abelian subgroup of the additive
group $\mathbb{C}$, we can consider cosets of $C$ to lie in $\mathbb{C}$
disjoint sets of cardinality $2^m$ each. It allows us to write $\mathbb{C} =
C \oplus \mathbb{D}$, where $C \cap \mathbb{D} = \{0\}$, $C \subset (\mathbb{C} \setminus C) \cup \{0\}$, and the elements \(d_i \in D\) are
called coset representatives, for $i = 1, \ldots, 2^m - m$.
Each coset will have only one representative $d_i \in D$.

Observe that any choice of coset representative can be
considered, however, for practical reasons, it is usually taken as
the minimum weight codeword among the coset and denoted
by coset leader. The next theorem summarizes these properties
and it is a well known result in linear algebra.

**Theorem 1.** Let $C \subset \mathbb{C} = C_1 \times \cdots \times C_L \subseteq \mathbb{F}_2^L$ be linear
codes. Then, the following properties hold:

1. Every coset of $C$ contains exactly $2^m$ codewords.
2. If $x \in (C \oplus y)$, then $(C \oplus x) = (C \oplus y)$.
3. Every codeword in $\mathbb{C}$ is contained in one and only one
coset of $C$.
4. There are exactly $2^{m - m}$ cosets of $C$.

**Proof.** For item iii), observe that $x \in (C \oplus x)$, since $x =
(0 \oplus x)$, $0 \in C$, and every codeword of $\mathbb{C}$ is contained in
some coset of $C$. Moreover, suppose $x \in (C \oplus y) \cap (C \oplus z)$,
then $x = c \oplus y = c' \oplus z$ and $y = (c' \oplus c) \oplus z \in (C \oplus z)$
and by item ii) $(C \oplus y) = (C \oplus z)$. □

**IV. Tiling of Irregular Constellations**

Unlike codes and lattices, which have the regular structure
of vector space and group, respectively, we will now consider
constellations that do not possess such a structure, but which
are derived from linear codes. The idea is to analyze characteristics
of such constellations inherited from the linear code.

In this section we will work with the finite representation
of the constellations $\Gamma_C$ and $\Gamma_{C^*}$, given by $X$ and $Y$ respectively
(see Definitions 3 and 4). Observe that $|X| = |\mathbb{C}| = 2^m$ and
$|Y| = |C| = 2^m$. By defining a class of $\Gamma_{C^*}$ as the image
under $\psi$ of a coset representative of the code $C \subseteq \mathbb{F}_2^L$, from
Theorem 1 we can conclude that there are $|X|/|Y| = 2^{m - m}$
distinct classes of $\Gamma_{C^*}$.

For convenience, we will use the notation of tiling defined
for groups as in Definition 7 also for the sets $X$ and $Y$,
which in general do not have group structure, but share the
same operation (addition). We must then demonstrate that the
representation of $X = Y + Z$ as a sum is unique, which is
equivalent to show that $(Y + z_j) \cap (Y + z_k) = \emptyset$, for
$z_j \neq z_k \in Z$, and that $Y \cap Z = \{0\}$. Here also $|Z| = 2^{m - m}$
and the elements of $Z$ will be called class representatives.
Instead of tiling, it might be more appropriate to use the term
partition of sets. However, we aimed for a unique notation
throughout the paper. We apologize for any confusion arising
from this abuse of notation.

In general, $(Y, Z)$ is not a tiling of $X$.

**Example 2.** Consider $C = \{(0, 0, 0, 0), (1, 1, 0, 0), (1, 0, 1, 0),
(1, 1, 1, 0)\} \subseteq \mathbb{F}_2^4$, $n = 1$, $L = 4$. Therefore, $Y = \{0, 3, 5, 6\}$
and $X = \{0, 1, 2, 3, 4, 5, 6, 7\} \subseteq \mathbb{Z}_{16}$. There are four possible
choices for the nonzero remaining element of $Z$, which are
1, 2, 4, 7, but observe that none of them generate the whole
set $X$. This is explained by the distance profile of $Y$, which is
not constant and cannot be obtained by a unique translation.

Based on the tiling of the underlying codes we can derive
the following condition for the tiling of the finite constellations.
From the previous section, we have that $(C, D)$
is a tiling of $\mathbb{C}$, $d_i \in D$ are the coset representatives, for
$i = 1, \ldots, 2^m - m$. Let 
$Z = \{z_i : z_i = \psi(d_i)\}$, for the respective coset representatives $d_i \in D$.

**Theorem 2.** $(Y, Z)$ is a tiling of $X$ if $(c \ast d_i)^{(1)} = 0$, for all $c \in C$, $d_i \in D$.

**Proof.** Consider $x \in X$. By definition, $x = \psi(b)$ for some $b \in \mathbb{C}$. Since $(C, D)$ is a tiling of $\mathbb{C}$, we can write $b = c \oplus d_i$, for $c \in C$, $d_i \in D$, $i = 1, \ldots, 2^m - m$. Hence,

$$x = \psi(c \oplus d_i) = \psi(c) + \psi(d_i) - 2\psi(c \ast d_i)$$

$$= \psi(c) + \psi(d_i) - \psi((c \ast d_i)^{(1)}), \quad \text{for all } c \in C.$$ 

By hypothesis, $(c \ast d_i)^{(1)} = 0$, and therefore, (6) implies

$$\psi(c \oplus d_1) = \psi(c_2 \oplus d_2), \quad \text{for all } c \in C.$$ 

A particular case where the hypothesis of Theorem 2 is
satisfied is when each coset of $\mathbb{C}$ has a representative in the
form $(0, \ldots, c_L) \in D$, for all $c_L \in C_L$. Hence, the level shifts
of all Schur products will be zero. An example follows next.

**Example 3.** Consider the linear code $C$ in Example 7 together
with $X$ and $Y$. Set $d_1 = 0$ and among the nonzero possible
choices for the remaining coset representative in $D$, we select

$$d_2 = (0, 0, 0, 1, 0). \quad \text{Notice that the Schur product between}
$$

$\text{d}_2$ and any element of $C$ is either zero or $d_2$, whose level shift
is zero and the condition of Theorem 2 is satisfied. $(Y, Z)$ is
a tiling of $X$, with $Z = \{(0, 0), (4, 0)\}$.

The result of Theorem 2 is particularly useful when we are
working with a small number of levels. Theorem 3 gives a
necessary condition for $(Y, Z)$ to be a tiling of $X$.

**Theorem 3.** If $(Y, Z)$ is a tiling of $X$ and at most the second
Schur level shift is vanishing, then the Schur level shift $(c \ast
d_i)^{(1)} \in \overline{C}$, for all $c \in C$ and $d_i \in D$. 


$X$ is a finite abelian group of finite abelian group of $\Gamma$, which is the topic of the next section.

Example 4. Consider $X = \mathbb{Z}_{16}$ and $Y = \{0, 5, 10, 15\}$. Thus, it is true for this setting of points that

$$X = Y + \begin{pmatrix} 0, 4, 8, 12 \end{pmatrix}_Z. \tag{9}$$

and $(Y, Z)$ is a tiling of $X$. The linear codes generating such constellations are, respectively to $X$ and $Y$,

$$C = \{(0, 0, 0, 0), (1, 0, 1, 0), (0, 1, 0, 1), (1, 1, 1, 1)\} \subset \mathbb{F}_2^4$$

$$\mathcal{C} = \mathbb{F}_2^4.$$ The classes in the set $Z$ according to \[9\] are written as $4 = \psi(0, 0, 1, 0), 8 = \psi(0, 0, 0, 1)$, and $12 = \psi(0, 0, 1, 1)$. By easy calculations, we can check that at most the second Schur level shifts between the class representatives and codewords of $C$ are zero. In this particular case, $X$ is an abelian group (and $\Gamma_C = X + 16\mathbb{Z}$ is a lattice). Theorem \[3\] then applies.

We could keep calculating the recursion proposed in Theorem \[3\] and exploiting conditional consequences of the tiling, but that result already implies that there might be significant contributions by considering $X$ to be an abelian group (as in Example \[4\]), which is the topic of the next section.

V. WHEN THE FINER CONSTELLATION IS A LATTICE

From now on, we assume that the finer constellation $\Gamma_C$ is a lattice. Then, since $\Gamma_C = X + 2^L \mathbb{Z}^n$, $X$ will be taken as a finite abelian group of $\mathbb{Z}_{2^n}^L$. The result below is intuitive.

Proposition 2. $\Gamma_C = X + 2^L \mathbb{Z}^n$ is a lattice if and only if $X$ is a finite abelian group of $\mathbb{Z}_{2^n}^L$.

We are interested in finding conditions on the set $Y$ such that it tiles $X$ and consequently, we will be able to conclude that $\Gamma_C$ tiling $\Gamma_C$. In order to explore this algebraic direction, we need the next definition.

Definition 8. If $A$ is a subset of $B$, we define the set

$$A - A = \{b \in B : \exists a_1, a_2 \in A \text{ such that } b = a_1 - a_2\}.$$
Initially, consider the set $S = (\mathbb{C} \setminus C) \cup \{0\}$, where we must select the elements to compose $D$ and $Z = \psi(D)$.

1) For every element $c \in C$, find the correspondent $c' \in \mathbb{C}$ such that $-\psi(c) = \psi(c')$, according to Eqs. (3) and (4). Remove all these elements $c'$ from the set $S$.

2) Consider now the elements $\bar{c} \in \mathbb{C}$ such that $\psi(c) = \psi(\bar{c})$, for all nonzero $c \neq \bar{c} \in C$. Remove all these elements $\bar{c}$ from the set $S$ as well.

3) Thus, $D \subseteq S$. If $D \subseteq S$, then one must select $2^m-m-1$ nonzero elements in $S$ to form $D$, such that for $Z = \psi(D)$ the relation $(Y - Y) \cap (Z - Z) = \{0\}$ holds.

This process is shown with details in the next example.

**Example 5.** Consider $X = \mathbb{Z}_{16}$, $Y = \{0, 3, 12, 15\}$ and $Z = \{0, 2, 8, 10\}$ (colors refer to $X = Y + Z$ in Figure 1). Following Theorem 2 we need to check that for $Y$ and $Z$, $(Y - Y) \cap (Z - Z) = \{0\}$.

Clearly $(Y - Y) \cap (Z - Z) = \{0\}$ and $(Y, Z)$ is a tiling of $X$, illustrated in Figure 1.

**REFERENCES**

[1] M. F. Bollauf, R. Zamir and S. I. R. Costa, “Multilevel constructions: coding, packing and geometric uniformity”, IEEE Trans. on Inf. Th., vol. 65, no. 12, pp. 7669-7681, Dec. 2019.

[2] G. Cohen, S. Litsyn, A. Vardy, and G. Zémor, “Tilings of binary spaces”, SIAM J. Disc. Math., vol. 9, no. 3, pp. 393-412, 1996.

[3] M. Dinitz, “Full rank tilings of finite abelian groups”, SIAM J. Disc. Math., vol. 20, no. 1, pp. 160-170, 2006.

[4] G. D. Forney, “Coset codes-part I: introduction and geometrical classification”, IEEE Trans. Inf. Th., vol. 34, no. 5, pp. 1123-1151, Sep. 1988.

[5] G. D. Forney, M. D. Trott, and S.-Y. Chung, “Sphere bound achieving coset codes and multilevel coset codes”, IEEE Trans. Inf. Th., vol. 46, no. 3, pp. 820-850, May 2000.

[6] G. Hajos, “Sur la factorisation des groupes abeliens”, Časop. Pěst. Math., vol. 74, pp. 147-162, 1949.

[7] W. Kositwatanarerk and F. Oggier, “Connections between Construction D and related constructions of lattices”, Des., Cod. and Crypt., v. 73, pp. 441-455, Nov. 2014.

[8] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, “Semantically secure lattice codes for the Gaussian wiretap channel”, vol. 60, no. 10, pp. 6399-6416, Oct. 2014.

[9] H. Mahdavifar and A. Vardy, “Achieving secrecy capacity of the wiretap channel using polar codes”, IEEE Trans. Inform. Th., vol. 57, no. 10, pp. 6328-6443, Oct. 2011.

[10] D. J. Newman, “Tesselation of integers”, J. of Num. Th., vol. 9, pp. 107-111, 1977.

[11] F. Oggier, P. Solé, and J.-C. Belfiore, “Lattice codes for the Gaussian wiretap channel: construction and analysis”, vol. 62, no. 10, pp. 5690-5708, Oct. 2015.

[12] L. H. Ozarow and A. D. Wyner, “Wire-tap channel II”, Bell. Lab. Tech. J., vol. 63, no. 10, pp. 2135-157, Dec. 1984.

[13] M. Qiu and S. A. Vanstone, “Factorizations in the elementary abelian p-groups and their cryptographic significance”, J. of Crypt., vol. 7, pp. 201-212, 1994.

[14] L. Redéi, “Lacunary polynomials over finite fields”. New York, USA: American Elsevier, 1973.

[15] A. D. Sands, “On Keller’s conjecture for certain cyclic groups”, Proc. of the Edin. Math. Soc., vol. 22, no. 1, pp. 17-21, Feb. 1979.

[16] A. D. Steyr, J. E. Strapasson, and S. I. R. Costa, “Perfect codes in Euclidean lattices”, Comp. Appl. Math., vol. 40, no. 47, Jan. 2021.

[17] S. Szabó and A. D. Sands, “Factoring groups into subsets”, vol. 256. Boca Raton, USA: Chapman & Hall, 2009.

[18] A. Thangaraj, S. Dhiidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, “Applications of LDPC codes to the wiretap channel”, IEEE Trans. Inf. Th., vol. 53, no. 8, pp. 2933-2945, Aug. 2007.

[19] A. D. Wyner, “The wire-tap channel”, Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355-387, Oct. 1975.