Quasi-perfect Lee Codes of Radius 2 and Arbitrarily Large Dimension

postprint version

Cristóbal Camarero[1] and Carmen Martínez[1]

[1]Computer Science and Electronics Department, University of Cantabria

Abstract

A construction of 2-quasi-perfect Lee codes is given over the space $\mathbb{Z}_p^n$ for p prime, $p \equiv \pm 5 \pmod{12}$ and $n = 2[\frac{p}{4}]$. It is known that there are infinitely many such primes. Golomb and Welch conjectured that perfect codes for the Lee-metric do not exist for dimension $n \geq 3$ and radius $r \geq 2$. This conjecture was proved to be true for large radii as well as for low dimensions. The codes found are very close to be perfect, which exhibits the hardness of the conjecture. A series of computations show that related graphs are Ramanujan, which could provide further connections between Coding and Graph Theories.

1 Introduction

Golomb and Welch conjectured in their seminal paper [13] that perfect Lee codes only exist for spheres of radius $r = 1$ or in Lee spaces of dimension $n = 1, 2$. A constructive result for 1-perfect Lee codes was also given in that paper. Moreover, for a radius sufficiently greater than the space dimension, a negative existence result was obtained by approximating the problem to the densest tessellation of $\mathbb{R}^n$ with cross-polytopes. Afterwards, Molnár enumerated all lattice-like 1-perfect codes in [28]. Later, Post in [30] gave a strong negative result. For the cases in which a periodic perfect code exists, Post determined an upper bound for its radius. In this upper bound the radius must fulfill $r < \frac{1}{2}n\sqrt{2} - \frac{3}{4}\sqrt{2} - \frac{1}{2}$ for $n \geq 6$. Later, J. Astola [7] and Lepistö [22] improved the bound given by Post to a quadratic relation between r and n, which can be considered as an Elias-type bound for Lee codes. These negative results suggest that the conjecture is more difficult for radius 2, as was argued by Horak in [16].

Other authors have considered the conjecture for low dimensions. For example, Gravier *et al.* in [14] proved the non-existence of perfect codes in 3-dimensional Lee spaces, even considering spheres of different radii. Dimension 4 was studied by Špacapan in [33], again with the possibility of spheres of different radii and all of them being greater or equal to 2. Also, Horak in [17] and [16] proved the non-existence of perfect Lee codes for $r = 2$ and spaces of dimension $n = 5, 6$. Later, Horak and Grošek in [19] computationally proved the non-existence of perfect Lee codes for dimension $n \leq 12$ and radius $r = 2$ by restricting the problem to linear codes.

In addition, several papers have considered problems involving the conjecture that could provide some insight about it. One approach has been to generalize the Lee metric. Huber in [20] gave 1-perfect codes over Gaussian integers and some non-perfect codes with greater correction. In [9] Costa *et al.* considered a relation between tessellations, graphs and codes over flat tori. In [24, 26, 25] Martinez *et al.* gave a generalization of the Lee distance by means of a family of Cayley graphs over Cayley–Dickson algebras. Also, the existence of perfect codes being ideals of the algebras was considered. Nishimura and Hiramatsu in [29] generalized the Lee distance using a surjective function from $\mathbb{Z}^l$ into a finite field and constructed some non-perfect 2-error correcting codes for this metric.

The existence of Lee codes has also been considered in terms of the size q of the alphabet. AlBdaiwi *et al.* in [3] enumerated all the alphabet sizes q such that there exists a linear 1-perfect Lee code over $\mathbb{Z}_q^n$. In [6] H. Astola and Tabus obtained, for small alphabet size q and dimension n, an upper bound of the number of codewords of error correcting Lee codes.

Recently, a new approach has been taken in terms of *diameter perfect codes*, which were introduced by Ahlswede *et al.* in [1]. A subset $\mathcal{C} \subseteq \mathbb{Z}_q^n$ is a diameter perfect code if there exists an anticode $\mathcal{A}$ such that $|\mathcal{C}||\mathcal{A}| = q^n$. This concept generalizes perfect codes since diameter perfect codes with minimum distance being odd are in fact the perfect codes. Etzion in [11] built diameter perfect codes of minimum distance 4. Later, Horak and AlBdaiwi [18] enumerated the arities q such that there are 4-diameter perfect codes over $\mathbb{Z}_q^n$. Araujo *et al.* in [4] presented a generalization of diameter perfect Lee codes, together with a new conjecture that extends the conjecture by Golomb and Welch. Etzion *et al.* in [12] built Lee codes for large dimension by means of weighing matrices.

Another way of proving the existence of perfect Lee codes has been to relax the condition of being perfect. Thus, although not widely used, quasi-perfect codes for the Lee metric have been considered. AlBdaiwi and Bose in [2] presented some quasi-perfect codes for dimension $n = 2$. Also, in [19] the authors presented some quasi-perfect codes for $n = 3$ and a few radii. Later, Queiroz *et al.* in [31] characterized quasi-perfect codes over Gaussian and Eisenstein–Jacobi integers being linear. As a consequence, linear quasi-perfect Lee codes were obtained for $n = 2$.

In the present paper an explicit construction of linear quasi-perfect Lee codes of radius 2 for arbitrarily large dimensions. It will be shown that these codes are very close to be perfect, since they have half the density of potential perfect codes. By contrast, all other results to this date depend on the dimension of the space. As a consequence, combinatorial arguments may be insufficient to address the conjecture. Nevertheless, the relation with Cayley graphs studied in this paper indicates that the conjecture has also algebraic features. Moreover, in the authors opinion, the existence of these quasi-perfect codes, hints that a perfect code might exist for small radius, although this is contrary to the general believe.

These quasi-perfect 2-error correcting Lee codes will be defined by means of Cayley graphs over Abelian finite groups. The degree of the graph will be the double of the dimension of the Lee space. The order of the graph will be in inverse relation to the density of the quasi-perfect code. Thus, the main contribution of the paper is presented in the next result.

Theorem 1. *For any prime $p \geq 7$ such that $p \equiv \pm 5 \pmod{12}$ there exists a linear 2-quasi-perfect p-ary Lee code over $\mathbb{Z}_p^n$, where $n = 2\left[\frac{p}{4}\right]$ and with p^{n-2} codewords.*

Note that the notation $[a]$ stands for the closest integer to the rational number a. As an example of the codes obtained in previous result, let us consider the following:

Example 1. *Let $n = 4$, $p = 7$. Then, the code over $\mathbb{Z}_7^4$ defined by the parity-check matrix*

$$\begin{pmatrix} 1 & 0 & 2 & -2 \\ 0 & 1 & 2 & 2 \end{pmatrix}$$

results in a 2-quasi-perfect 7-ary Lee code over $\mathbb{Z}_7^4$. This code has $p^{n-2} = 49$ codewords. It is known that perfect codes do not exist in this case since the sphere packing bound is $\frac{7^4}{41} \approx 58.56$.

As a consequence of Dirichlet's theorem on arithmetic progressions, there are infinitely many primes p such that $p \equiv 5 \pmod{12}$ and infinitely many primes such that $p \equiv -5 \pmod{12}$. Thus, for any constant c, there is a prime $p \equiv \pm 5 \pmod{12}$ such that the dimension $n = 2\left[\frac{p}{4}\right]$ is greater than c. As a consequence of this and Theorem 1, it is obtained that:

Corollary 2. *There are infinitely many $n \in \mathbb{N}$ such that there exists a 2-quasi-perfect Lee code over a n-dimensional Lee space.*

As it will be shown later, the result is constructive, and any application that requires the use of Lee-codes could benefit from it. For example, Roth and Siegel in [32] considered BCH Lee codes and their application to constrained and partial-response channels. Using space embeddings, Jiang *et al.* in [21] gave a method to construct Charge-Constrained Rank-Modulation codes (CCRM codes) from Lee error-correcting codes, which could be employed for flash memories. H. Astola and Stankovic in [5] considered Lee codes to build decision diagrams.

The rest of the paper is organized as follows. Since the codes considered in this paper will be defined by means of Cayley graphs, in Section 2 the relation between Lee codes and Cayley graphs over Gaussian integers is stated. Moreover, the family of Cayley graphs under study is defined. Then, in Section 3 the Cayley graphs selected are proved to have error correction capacity 2. In Section 4 those Cayley graphs are shown to attain diameter 3, which implies that they define 2-quasi-perfect codes. Finally, in Section 5 the results presented in this paper are discussed, and some open problems and future lines of research are detailed.

2   Codes and Graphs

Linear 2-quasi-perfect p-ary linear Lee codes are going to be defined by means of Cayley graphs. Therefore, the correspondence between a linear code and a Cayley graph is explained in this section. First, some fundamental definitions are stated here.

Since Lee codes are the target of our study, the natural space to be considered is the finite integer lattice $\mathbb{Z}_p^n$. However, for convenience, also the infinite lattice $\mathbb{Z}^n$ will be considered. Therefore, a *code* $\mathcal{C}$ will be a subset of either $\mathbb{Z}_p^n$ or $\mathbb{Z}^n$. This code is said to be *linear* if it is a subgroup of the corresponding space.

The *Manhattan distance* will be used in the space $\mathbb{Z}^n$. For any two words $v, w \in \mathbb{Z}^n$ its Manhattan distance is defined as:

$$d(v, w) = \sum_{j=1}^{n} |v_i - w_i|.$$

On the other hand, the *Lee distance* will be the metric used when considering $\mathbb{Z}_p^n$. For $v, w \in \mathbb{Z}_p^n$ its Lee distance is defined as

$$d(v, w) = \sum_{j=1}^{n} \min\{|s| \mid s \equiv v_j - w_j \pmod{p}, \ s \in \mathbb{Z}\}.$$

Since the Lee distance becomes the Manhattan distance for $p = \infty$, there will be no opportunity for confusion. In both cases the weight of a word v is defined as its distance to the origin, which will be denoted as $|v| = d(v, O)$. For any positive integer r, the *Lee sphere* of radius r is defined as all the points whose weight is less or equal to r, that is:

$$B_r^n = \{v \mid |v| \le r\}.$$

Note that, for any dimension $n \ge 1$, the cardinal $|B_2^n| = 2n^2 + 2n + 1$, [13].

A code $\mathcal{C}$ is said to be *t-error correcting* if t is the greatest integer such that for any word w there is at the most one codeword $c \in \mathcal{C}$ with $d(w, c) \le t$. Thus, t is called the *error correction* of $\mathcal{C}$. A code $\mathcal{C}$ is said *r-covering* if r is the smallest integer such that for any word w there is at least one codeword $c \in \mathcal{C}$ with $d(w, c) \le r$. Thus, r denotes the covering radius of $\mathcal{C}$. Then, a code that is both t-error correcting and t-covering, or equivalently with error correction equal to its covering radius, is said to be *perfect*. Golomb and Welch in [13] conjectured that there only exist perfect Lee codes for $t = 1$ or $n = 2$. Therefore, the existence of quasi-perfect codes must be studied since they are the best alternative to the perfect codes. Thus, a code that is t-error correcting and $(t+1)$-covering is said to be *t-quasi-perfect*. In this work 2-quasi-perfect Lee codes are found for arbitrarily large dimensions. This is done by the construction of a family of Cayley graphs that leads to the codes definition. The remainder of this section is devoted to define this relation between codes and graphs. For simplicity, the infinite lattice $\mathbb{Z}^n$ will be considered and an equivalent relation can be stated in the case of $\mathbb{Z}_p^n$.

Given a group Γ and a set of generators $H = \{\beta_1, \ldots, \beta_s\} \subset \Gamma$, the *Cayley graph* over Γ generated by H is defined as the graph with set of vertices the elements of Γ, and adjacencies $(u, u + \beta_i)$, for every $u \in \Gamma$ and $i = 1, \ldots, s$. H must satisfy $H = -H$ and $0 \notin H$ in order to be a simple undirected graph. Since only Abelian groups will be considered, the operation of the group will be denoted by $+$ and the neutral element by 0. Now, given a linear code $\mathcal{C} \subset \mathbb{Z}^n$ the associated graph is

$$G = Cay(\mathbb{Z}^n/\mathcal{C}; \{\pm e_1, \ldots, \pm e_n\}).$$

Reciprocally, given a Cayley graph $Cay(\Gamma; \{\pm a_1, \ldots, \pm a_n\})$ a linear code can be built. First, let us consider the homomorphism $\phi : \mathbb{Z}^n \longrightarrow \Gamma$ such that $\phi(e_j) = a_j$. Then, the code is given by

$$\mathcal{C} = \{x \in \mathbb{Z}^n \mid \phi(x) = 0\} = \ker \phi.$$

Next, distance and correction parameters of both the code and the graph are related as Theorem 4 states. Now, let us recall some basic definitions. The *distance* $d_G(v, w)$ between two vertices v, w in a graph G is defined as the number of edges in the shortest path from v to w. Then, the *diameter* of a graph G is the maximum among distances between every pair of vertices. Since Cayley graphs are vertex-transitive, this can also be calculated as the maximum distance to one particular vertex, usually $0 \in \Gamma$.

Definition 3. *Given a Cayley graph $Cay(\Gamma; \{\pm a_1, \ldots, \pm a_n\})$ over an Abelian group Γ, its error correction capacity is defined as the greatest integer t such that for every vertex $v \in \Gamma$ there are $|B_t^n|$ vertices at distance t or less from v.*

Note that since G is a Cayley graph, it is vertex-transitive and therefore it is enough to count the number of vertices around one vertex to determine its error correction capacity. Thus, the equivalence between distance and covering properties of a linear Lee code and its associated Cayley graph over an Abelian group is proved in the following theorem:

Theorem 4. *Let Γ be a finite Abelian group that is generated by $\{a_1, \ldots, a_n\}$ and let $G = Cay(\Gamma; \{\pm a_1, \ldots, \pm a_n\})$. Let ϕ be the homomorphism from $\mathbb{Z}^n$ into Γ defined by $\phi(e_j) = a_j$ and let $\mathcal{C} = \ker \phi$. Then,*

1. the diameter of G equals the covering radius of $\mathcal{C}$ and

2. the error correction capacity of G equals the error correction of $\mathcal{C}$.

But first of all, let us prove the following technical result.

Lemma 5. *In the hypothesis of Theorem 4, for every $x \in \mathbb{Z}^n$ it is obtained that $d_G(\phi(x), 0) = d(x, \mathcal{C})$.*

Proof. Let x be an arbitrary element of $\mathbb{Z}^n$. Let us prove first that $d_G(\phi(x), 0) \leq d(x, \mathcal{C})$. Let c be the closest codeword to x, so $d(x, \mathcal{C}) = d(x, c)$. By the definition of Manhattan distance, $d(x, c) = \sum_{j=1}^n |x_j - c_j|$. As $\mathcal{C}$ is the kernel of ϕ, $\phi(x) = \phi(x - c) = \sum_{j=1}^n (x_j - c_j) a_j$. The distance in a Cayley graph over an Abelian group of a vertex v to 0 is given by $d_G(v, 0) = \min\{\sum_{j=1}^n |y_j| \mid \sum_{j=1}^n y_j a_j = v\}$. Hence, taking $v = \phi(x)$ and $y = x - c$ in the previous expression, $d_G(\phi(x), 0) \leq \sum_{j=1}^n |x_j - c_j| = d(x, \mathcal{C})$.

For the second inequality, $d_G(\phi(x), 0) \geq d(x, \mathcal{C})$, let $y \in \mathbb{Z}^n$ be the vector such that $d_G(\phi(x), 0) = \sum_{j=1}^n |y_j|$ and $\phi(x) = \sum_{j=1}^n y_j a_j$. By definition of y, $\phi(x) = \phi(y)$, so the difference $c = x - y \in \mathcal{C}$ is a codeword. Thus, as $\mathcal{C}$ is a linear code, $d(x, \mathcal{C}) \leq d(x, c) = d(x - c, O) = d(y, O)$, and by the definition of Manhattan distance $d(x, \mathcal{C}) \leq d(y, O) = \sum_{j=1}^n |y_j| = d_G(\phi(x), 0)$. □

Proof. (of Theorem 4). For the first item in the theorem note that $\text{diam}(G) = \max\{d_G(v, 0) \mid v \in \Gamma\} = \max\{d_G(\phi(x), 0) \mid x \in \mathbb{Z}^n\}$, since ϕ is surjective. Then, by Lemma 5 it is obtained that $\max\{d_G(\phi(x), 0) \mid x \in \mathbb{Z}^n\} = \max\{d(x, \mathcal{C}) \mid x \in \mathbb{Z}^n\} = \text{covering radius}(\mathcal{C})$.

For the second item let us proof that for every integer $s > 0$, $\phi(B_s^n) = \{v \in \Gamma \mid d_G(v, 0) \leq s\}$. If x belongs to B_s^n then $d(x, O) \leq s$ and, by Lemma 5, $\phi(x)$ is at distance at most s from 0. Reciprocally, if there is a vertex $v \in \Gamma$ such that $d_G(v, 0) \leq s$ then, there exists x such that $\phi(x) = v$ and $x \in B_s^n$.

Now, let t be the error correction of $\mathcal{C}$, that is, the greatest integer such that all the words in B_t^n are closer to O than to any other codeword. If $x, y \in B_t^n$ are such that $\phi(x) = \phi(y)$ then $\phi(x - y) = 0$. Hence, $x - y \in \ker \phi = \mathcal{C}$. Since $d(x, y) \leq 2t$ it is obtained that $x = y$. Therefore, the cardinal numbers $|B_t^n| = |\phi(B_t^n)|$ are equal. Thus, by previous step $|\{v \in \Gamma \mid d_G(v, 0) \leq t\}| = |B_t^n|$, which implies that the error correction capacity of G is at least t.

Finally, let us denote by t' the error correction capacity of G. Again, there are $|B_{t'}^n|$ words at a distance less of equal to t' from 0. Let $x \in \mathbb{Z}^n$ and let $c_1, c_2 \in \mathcal{C}$ be such that $d(x, c_1), d(x, c_2) \leq t'$. Then, note that $c_1 - x, c_2 - x \in B_{t'}^n$ and $\phi(-x) = \phi(c_1) + \phi(-x) = \phi(c_1 - x) = \phi(c_2 - x)$. From $|B_{t'}^n| = |\phi(B_{t'}^n)|$, it is obtained that ϕ restricted to this set is a bijection, which implies that $c_1 - x = c_2 - x$, that is, $c_1 = c_2$, which concludes the proof. □

Remark 6. *Note that $Cay(\Gamma; \{\pm a_1, \ldots, \pm a_n\}) \cong Cay(\mathbb{Z}^n / \ker \phi; \{\pm e_1, \ldots, \pm e_n\})$. Thus, applying the previous procedure to obtain a code from a graph and applying it again to obtain a graph from a code, then an isomorphic graph is obtained.*

Remark 7. *Theorem 4 can be graphically interpreted by means of tessellations, as illustrated in Figure 1. Subfigure a) shows $\mathcal{C} = \langle (4, 4), (-4, 4) \rangle$, a 3-quasi-perfect linear Lee code over $\mathbb{Z}_{16}^2$. This is, the code has error correction 3 and covering radius 4. Subfigure b) shows a Voronoi tessellation induced by $\mathcal{C}$, in which every tile has as center a codeword. Subfigure c) shows in detail one of these tiles. As it can be observed, it contains the Lee sphere B_3^2 and it is contained in the Lee sphere B_4^2. Subfigure d) shows the Cayley graph $Cay(\frac{\mathbb{Z}_{16}^2}{\mathcal{C}}; \{\pm e_1, \pm e_2\})$. This graph is induced by tessellation as follows. The vertices are the words in the tile and two vertices are adjacent if they are at a distance 1, modulo the tessellation. Finally, observe that the graph has diameter 4 since there are 7 vertices at distance 4 from the center. Also, it has error correction capacity 3 since there are $25 = |B_3^2|$ vertices at a distance less or equal to 3.*

The remainder of the paper describes a family of Cayley graphs over Gaussian integers. Let us denote by $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ the ring of the Gaussian integers. In [15] the fundamentals on this ring can be found. Given an integer prime p, let us denote by $\mathbb{Z}[i]/p\mathbb{Z}[i]$ the quotient additive group of the Gaussian integers over the group generated by $(p) \subset \mathbb{Z}[i]$. Thus, the graph is defined as follows.

Definition 8. *Given an integer prime p, let us define the Cayley graph $\mathcal{G}_p = Cay(\mathbb{Z}[i]/p\mathbb{Z}[i], H)$, where*

$$H = \{\beta \in \mathbb{Z}[i]/p\mathbb{Z}[i] \mid \mathcal{N}(\beta) = 1\}.$$

Note that in the previous definition $\mathcal{N}(\beta) = \mathcal{N}(b_1 + b_2 i) = b_1^2 + b_2^2$ denotes the norm of β. Moreover, the adjacency in the graph is determined by the elements with unitary norm. In the subsequent sections, it will be proved that $\mathcal{G}_p$ induces a 2-quasi-perfect Lee code over $\mathbb{Z}_p^n$ under some conditions. Therefore, it must be determined which primes p are such that $\mathcal{G}_p$ has error correction capacity 2 and diameter 3, as proved in Theorem 4.

3 Error Correction Capacity of $\mathcal{G}_p$

As explained in previous section, 2-quasi-perfect Lee codes will be obtained by means of Cayley graphs. In particular, it will be determined under which conditions the Cayley graph $\mathcal{G}_p$ over the additive group $\mathbb{Z}[i]/p\mathbb{Z}[i]$ and generating set the elements with unitary norm, induces a 2-quasi-perfect code. In this section it will be proved that $p \equiv \pm 5$ (mod 12) implies that $\mathcal{G}_p$ has error correction capacity 2 over $\mathbb{Z}_p^n$ for $n = 2[\frac{p}{4}]$. Hence, in the remainder of the paper, let us assume that $p > 2$ is a prime integer. Therefore, the natural number $n = 2[\frac{p}{4}]$ fulfills $p = 2n \pm 1$.
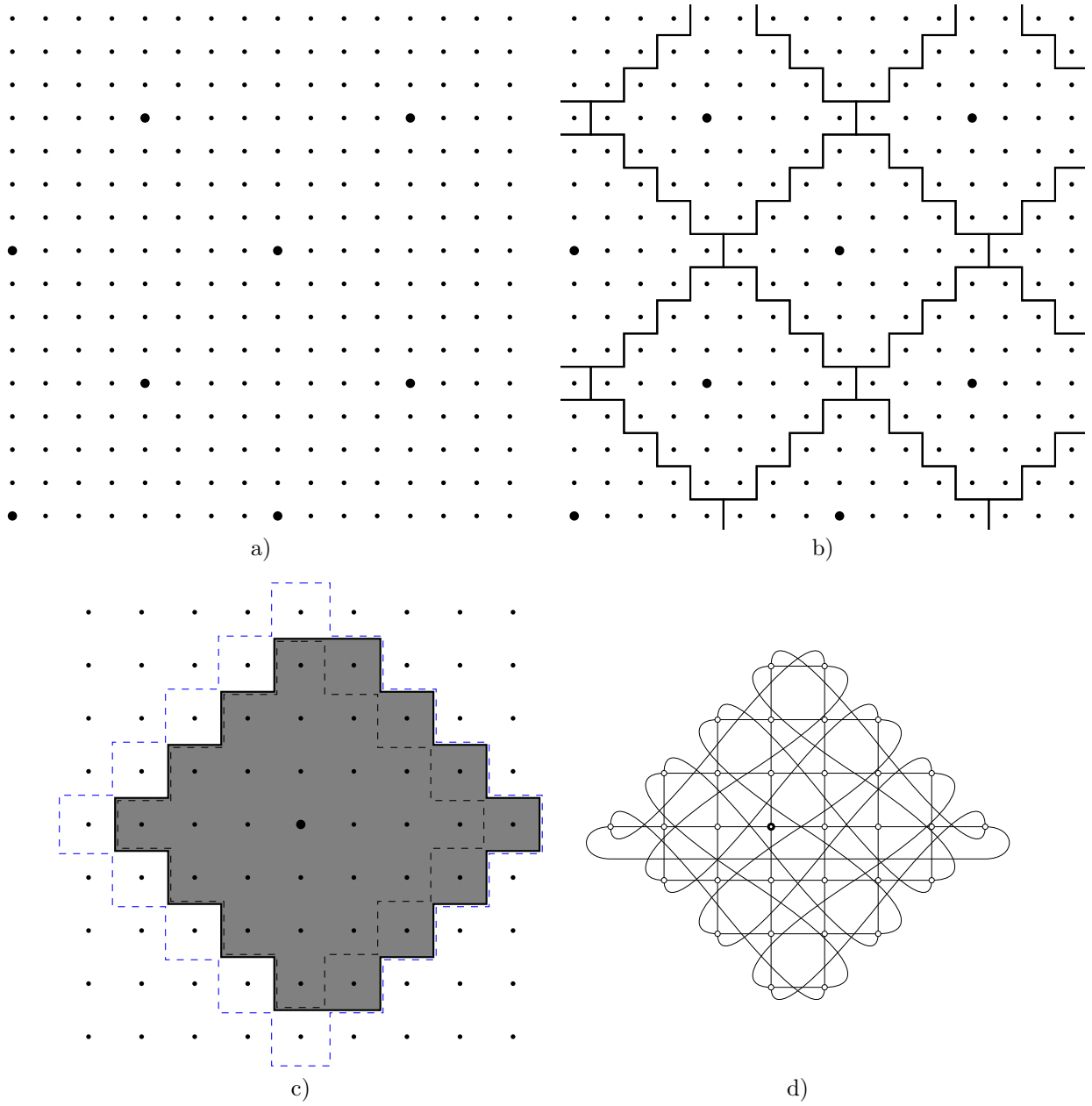
Figure 1: a) A 3-correcting and 4-covering linear Lee code over $\mathbb{Z}_{16}^2$. b) A Voronoi tessellation of the code. c) The tile associated to a codeword. d) The associated graph $Cay(\frac{\mathbb{Z}_{16}^2}{\mathcal{C}}; \{\pm e_1, \pm e_2\})$ in minimum distance representation.

First, let us introduce some notation. Given a Gaussian integer $\beta = b_1 + b_2 i \in \mathbb{Z}[i]$, β^* will denote its conjugate, that is $\beta^* = b_1 - b_2 i$. Also, $\Re(\beta) = b_1$ will stand for its real part and $\Im(\beta) = b_2$ for its imaginary part. Then, the following formula about the norm of a sum of Gaussian integers will be useful in several points of this paper.

Lemma 9. *For any pair of Gaussian integers $\beta, \gamma \in \mathbb{Z}[i]$,*

$$\mathcal{N}(\beta + \gamma) = \mathcal{N}(\beta) + \mathcal{N}(\gamma) + 2\Re(\beta\gamma^*).$$

Then, the previous result can be used to prove the following technical lemma:

Lemma 10. *For any $\gamma_1, \gamma_2 \in \mathbb{Z}[i]/p\mathbb{Z}[i]$, if $\mathcal{N}(\gamma_1) = \mathcal{N}(\gamma_2)$ and $\mathcal{N}(1 + \gamma_1) = \mathcal{N}(1 + \gamma_2)$ then $\gamma_1 \in \{\gamma_2, \gamma_2^*\}$.*

Proof. Since $\mathcal{N}(1+\gamma_1) = \mathcal{N}(1+\gamma_2)$, by Lemma 9 it is obtained that $\Re(\gamma_1) = \Re(\gamma_2)$. Therefore, there are $x, y, z \in \mathbb{Z}/p\mathbb{Z}$ such that $\gamma_1 = x + yi$ and $\gamma_2 = x + zi$. Now, $\mathcal{N}(\gamma_1) = \mathcal{N}(\gamma_2)$ implies that $x^2 + y^2 = x^2 + z^2$. As a consequence, $y^2 = z^2$ and therefore $y \in \{\pm z\}$, which means $\gamma_1 \in \{\gamma_2, \gamma_2^*\}$. $\square$

Corollary 11. *Let $\beta \in \mathbb{Z}[i]/p\mathbb{Z}[i]$ be such that $\mathcal{N}(\beta) = 1$. Then, $1 + \beta$ is not a proper zero divisor.*

Proof. If $1 + \beta$ is a zero divisor then $\mathcal{N}(1 + \beta) = 0 = \mathcal{N}(1 + (-1))$. By Lemma 10, $\beta \in \{-1, -1^*\} = \{-1\}$ and $1 + \beta = 0$. $\square$

Let us denote by $G = \mathcal{U}(\mathbb{Z}[i]/p\mathbb{Z}[i])$ the multiplicative group formed by the units of the ring. Then, the set

$$H = \{\beta \in G \mid \mathcal{N}(\beta) = 1\}$$

is clearly a multiplicative normal subgroup of G. It is actually a cyclic group, although this fact will not be used in the proofs. Note that H is the set of adjacencies of $\mathcal{G}_p$, that is, $\mathcal{G}_p = Cay(\mathbb{Z}[i]/p\mathbb{Z}[i], H)$. For any $\gamma \in \mathbb{Z}[i]/p\mathbb{Z}[i]$, the following notation is introduced:

$$\gamma H = \{\gamma\beta \mid \beta \in H\}.$$

Notice that if $\gamma \in G$, then γH is the *coset* of H in G with respect to γ. Nevertheless, this notation is also defined for elements outside G, i.e., for zero divisors of $\mathbb{Z}[i]/p\mathbb{Z}[i]$.

The following lemma tells us that cosets can be identified by the norms of its elements.

Lemma 12. *For any $\gamma \in G$,*

$$\gamma H = \{\beta \in \mathbb{Z}[i]/p\mathbb{Z}[i] \mid \mathcal{N}(\beta) = \mathcal{N}(\gamma)\}.$$

Proof. In order to prove the sets equality, it will be first proved that $\gamma H \subseteq \{\beta \in G \mid \mathcal{N}(\beta) = \mathcal{N}(\gamma)\}$. Thus, let us consider $\beta \in \gamma H$ and it has to be proved that $\mathcal{N}(\beta) = \mathcal{N}(\gamma)$. Since $\beta \in \gamma H$, then there exists $\eta \in H$ such that $\beta = \gamma\eta$. Hence $\mathcal{N}(\beta) = \mathcal{N}(\gamma)\mathcal{N}(\eta) = \mathcal{N}(\gamma)$.

Now, let us consider the other inclusion, that is, $\gamma H \supseteq \{\beta \in G \mid \mathcal{N}(\beta) = \mathcal{N}(\gamma)\}$. Therefore, let $\beta \in G$ be such that $\mathcal{N}(\beta) = \mathcal{N}(\gamma)$. Since γ is invertible, $\beta = \gamma(\beta\gamma^{-1})$. Now, as $\mathcal{N}(\beta\gamma^{-1}) = 1$ it is obtained that $\beta \in \gamma H$. $\square$

Theorem 14 states that the degree of the graph $\mathcal{G}_p$ is $2n$. To prove it some particular cases of the Quadratic Reciprocity Law will be necessary, which are recalled in the following theorem for self-containedness.

Theorem 13 (Quadratic Reciprocity)**.** *If p is an integer prime, then:*

1. *The number of solutions to $-1 = x^2$ in $\mathbb{Z}/p\mathbb{Z}$ is:*

   - *2 if $p \equiv 1 \pmod 4$,*
   - *1 if $p = 2$ and*
   - *0 if $p \equiv 3 \pmod 4$.*

2. *The number of solutions to $3 = x^2$ in $\mathbb{Z}/p\mathbb{Z}$ is:*

   - *2 if $p \equiv \pm 1 \pmod{12}$,*
   - *1 if $p = 3$ or $p = 2$ and*
   - *0 otherwise.*

Theorem 14. *For any odd prime integer p, let $n = 2[\frac{p}{4}]$. Then,*

$$|H| = |\{\beta \in \mathbb{Z}[i]/p\mathbb{Z}[i] \mid \mathcal{N}(\beta) = 1\}| = 2n.$$

Proof. It is clear that
$$|H| = |\{(x, y) \mid x, y \in \mathbb{Z}/p\mathbb{Z}, \ x^2 + y^2 = 1\}|.$$

Therefore, let us consider the solutions of $x, y \in \mathbb{Z}/p\mathbb{Z}$ of equation $x^2 + y^2 = 1$. First, if $x = 1$ then $y^2 = 0$ whose unique solution is $y = 0$. Let us assume $x \neq 1$ to find the rest of the solutions. Since $x \neq 1$, $x - 1$ has inverse and it is possible to define $s = y/(x - 1) \in \mathbb{Z}/p\mathbb{Z}$. By considering the intersection of the straight line $y = s(x - 1)$ with the curve $x^2 + y^2 = 1$ it is obtained that $x^2 + (s(x - 1))^2 = 1$. The only solutions of this equation are $x = 1$ (which has already been considered) and $x = \frac{s^2 - 1}{s^2 + 1}$. This second solution for x equals 1 if and only if $p = 2$. Thus, the only solutions with $x \neq 1$ are $x = \frac{s^2 - 1}{s^2 + 1}$ and $y = \frac{-2s}{s^2 + 1}$.

Now, for each possible value of s, there is one solution with this form, that is, p minus the number of solutions of $s^2 + 1 = 0$. By the Quadratic Reciprocity Law (first item of Theorem 13) there are $p + 1$ solutions if $p \equiv 3 \pmod 4$ and $p - 1$ if $p \equiv 1 \pmod 4$. Thus, for primes of the form $p = 1 + 4k$, there are $p - 1 = 4k = 2n$ solutions and for primes $p = -1 + 4k$ there are $p + 1 = 4k = 2n$ solutions, where $k \in \mathbb{N}$.

Finally, just to ensure that the counted solutions are all different, note that if for a pair s_1, s_2 the same solution (x, y) is obtained, then $s_1 = s_2 = y/(x - 1)$. $\qquad\square$

Next, it is easy to obtain the following consequence of previous theorem, which will be used in Section 4 to determine the diameter of the graph $\mathcal{G}_p$.

Corollary 15. *For any odd prime integer p, let $n = 2[\frac{p}{4}]$. If $0 \neq \gamma \in \mathbb{Z}[i]/p\mathbb{Z}[i]$ then $|\gamma H| = 2n$.*

Proof. Firstly, note that if $\gamma \in G$, then γH is a coset, which is widely known to have the same cardinal. Thus, the non-immediate part of the proof lies on the zero divisors. By Theorem 14, it is straightforward that $|\gamma H| \leq 2n$. Proceeding by *reductio ad absurdum*, let us assume $|\gamma H| < 2n$. Then, there exist $\beta_1 \neq \beta_2$ such that $\gamma\beta_1 = \gamma\beta_2$, thus $\gamma(\beta_1 - \beta_2) = 0$. Since $\gamma \neq 0$ then $\beta_1 - \beta_2$ must be a zero divisor. Now, multiplying by β_1^{-1}, $1 - \beta_2\beta_1^{-1}$ is also a zero divisor. By Corollary 11, $1 - \beta_2\beta_1^{-1} = 0$ and hence $\beta_1 = \beta_2$, which is a contradiction. $\qquad\square$

Before stating the conditions under which $\mathcal{G}_p$ has error correction capacity 2, the following lemma is going to be proved. This lemma determines the number of possible norms among the neighbours of a vertex with a given norm.

Lemma 16. *For any $c \in \mathbb{Z}/p\mathbb{Z}$, $c \neq 0$, let us consider the set $N_p(c) = \{\mathcal{N}(1 + \beta) \mid \mathcal{N}(\beta) = c\} \subset \mathbb{Z}/p\mathbb{Z}$. Then, it is obtained that:*
$$|N_p(c)| = \begin{cases} n + 1 & \text{if } c \text{ is a square residue mod } p, \\ n & \text{if } c \text{ is not a square residue mod } p. \end{cases}$$

Proof. In the first case, that is c being a square residue, there must exists $s \in \mathbb{Z}/p\mathbb{Z}$ such that $c = s^2$. By Lemma 12 and Corollary 15 there are $2n$ elements with norm c, which are:

$$\{\beta \mid \mathcal{N}(\beta) = c\}$$
$$= \{s, -s, \beta_1, \beta_2, \ldots, \beta_{n-1}, \beta_1^*, \beta_2^*, \ldots, \beta_{n-1}^*\},$$

for some $\beta_1, \ldots, \beta_{n-1} \in \mathbb{Z}[i]/p\mathbb{Z}[i]$. Then,

$$N_p(c) = \{\mathcal{N}(1 + \beta) \mid \mathcal{N}(\beta) = c\} =$$
$$\{\mathcal{N}(1 + s), \mathcal{N}(1 - s), \mathcal{N}(1 + \beta_1), \mathcal{N}(1 + \beta_2), \ldots, \mathcal{N}(1 + \beta_{n-1})\},$$

which are different by Lemma 10. Hence $|N_p(c)| = 2 + (n - 1) = n + 1$.

For the case of c being a square non-residue let us proceed in a similar way. It is obtained that

$$\{\beta \mid \mathcal{N}(\beta) = c\}$$
$$= \{\beta_0, \beta_1, \beta_2, \ldots, \beta_{n-1}, \beta_0^*, \beta_1^*, \beta_2^*, \ldots, \beta_{n-1}^*\}.$$

Then

$$N_p(c) = \{\mathcal{N}(1 + \beta) \mid \mathcal{N}(\beta) = c\} =$$
$$\{\mathcal{N}(1 + \beta_0), \mathcal{N}(1 + \beta_1), \mathcal{N}(1 + \beta_2), \ldots, \mathcal{N}(1 + \beta_{n-1})\},$$

which are different by Lemma 10. Hence $|N_p(c)| = n$. $\qquad\square$

As it is noted afterwards, the case $c = 1$ in previous lemma will be used to prove the error correction capacity. Later, the fact that n is a lower bound of $|N_p(c)|$ will be considered to determine the graph diameter.

To finish the section, next theorem establishes the conditions for p such that $\mathcal{G}_p$ has error correction capacity 2.

Theorem 17. *Let p be a prime integer satisfying $p \equiv \pm 5 \pmod{12}$. Then, the Cayley graph $\mathcal{G}_p$ has error correction capacity 2.*

Proof. Let $n = 2\left\lceil \frac{p}{4} \right\rceil$. As it was explained in previous section, it has to be proved that $\mathcal{G}_p$ contains $|B_2^n| = 2n^2 + 2n + 1$ vertices at distance 2 or less from 0. Clearly, 0 is the unique vertex at distance 0. Now, the set H contains all the vertices at distance 1 and $|H| = 2n$ by Theorem 14.

The vertices at distance 2 is the set $A = \{\beta_a + \beta_b \mid \beta_a, \beta_b \in H\} \setminus (H \cup \{0\})$. Thus, let us prove that $|A| = 2n^2$. By Lemma 12 and Corollary 15, $|A| = 2n \cdot |N_p(1) \setminus \{0, 1\}|$. Since 1 is always a square residue for any p, hence by Lemma 16, $|N_p(1) \setminus \{0\}| = n$. It remains to be proved that 1 does not belong to $N_p(1)$.

Suppose that there is β with $\mathcal{N}(\beta) = 1$ and $\mathcal{N}(1 + \beta) = 1$. Then, by Lemma 9, $1 = 2 + 2\Re(\beta)$ and hence $\Re(\beta) = -2^{-1}$. Let $\beta = -2^{-1} + yi$, which implies $1 = \mathcal{N}(\beta) = 2^{-2} + y^2$. Then, $3 = (2y)^2$, which only has solutions for $p = 3$ or $p \equiv \pm 1 \pmod{12}$ by the second item of Theorem 13. Thus, $|N_p(1) \setminus \{0, 1\}| = |N_p(1) \setminus \{0\}| = n$ and $|A| = 2n \cdot n$, which concludes the proof. $\qquad\square$

Remark 18. *If p is a prime greater than 3 that does not satisfy $p \equiv \pm 5 \pmod{12}$, then $p \equiv \pm 1 \pmod{12}$. In this case, $\mathcal{G}_p$ only contains $2n^2 + 1$ vertices at distance 2 or less from vertex 0. Although it is not a 2-error correcting code, it is very close to it, since only $2n$ syndromes cannot be corrected.*

4 Diameter of $\mathcal{G}_p$

In this section it will be proved that $\mathcal{G}_p$ has diameter 3 for any prime $p > 5$. The proof will be divided into two subsections. The first considers the case $p \equiv 3 \pmod{4}$ and the second the case $p \equiv 1 \pmod{4}$. Also, from here onwards it will be assumed again that $n = 2\lceil \frac{p}{4} \rceil$. Note that, since $|\mathbb{Z}[i]/p\mathbb{Z}[i]| = p^2 > |B_2^n|$, there are vertices outside the sphere of radius 2, which means that the diameter of the graph is at least 3. As it will be seen next, the proofs proceed by *reductio ad absurdum* by the assumption of the existence of a vertex at a distance 4 from vertex 0, thus reaching a contradiction.

4.1 Case $p \equiv 3 \pmod{4}$

In this case the proof of the diameter can be easily obtained by using a counting argument. Note that in this case $p = 2n - 1$ and therefore $\mathbb{Z}[i]/p\mathbb{Z}[i]$ is a field.

Theorem 19. *For any prime p such that $p \equiv 3 \pmod{4}$ the graph $\mathcal{G}_p$ has diameter 3.*

Proof. By *reductio ad absurdum* let us assume that there exists a vertex $\gamma \in \mathbb{Z}[i]/p\mathbb{Z}[i]$ at distance 4 from vertex 0. Let $c = \mathcal{N}(\gamma)$. Since γ is so far, it is obtained that $N_p(1) \cap N_p(c) = \emptyset$.

Let us denote by $W_t(0)$ the number of vertices at a distance t from vertex 0. Then, $\{W_t(0) \mid t = 0, \dots, 4\}$ is the distance distribution of the graph $\mathcal{G}_p$. Now, the cardinals $W_1(0) = |H|$ and $W_4(0) \geq |\gamma H|$ can be calculated by Corollary 15. Also, by Lemma 16 it can be computed that $|N_p(1)| = n + 1$ and $|N_p(c)| \geq n$. Thus, the obtained bounds for the distance distribution are summarized as follows:

$$
\begin{aligned}
W_0(0) &= |\{0\}| & &= 1 \\
W_1(0) &= |H| & &= 1 \cdot 2n \\
W_2(0) &= 2n \cdot |N_p(1) \setminus \{0, 1\}| & &\geq (n-1) \cdot 2n \\
W_3(0) &\geq 2n \cdot |N_p(c) \setminus \{c\}| & &\geq (n-1) \cdot 2n \\
W_4(0) &\geq |\gamma H| & &= 1 \cdot 2n
\end{aligned}
$$

As a consequence, the total number of vertices satisfies $|\mathbb{Z}[i]/p\mathbb{Z}[i]| \geq 1 + 2n(1 + (n-1) + (n-1) + 1) = 4n^2 + 1 > 4n^2 - 4n + 1 = p^2 = |\mathbb{Z}[i]/p\mathbb{Z}[i]|$, which is a contradiction. $\qquad\square$

4.2 Case $p \equiv 1 \pmod{4}$

Unfortunately, the reasoning made in the previous case fails to give us a contradiction if $p \equiv 1 \pmod{4}$. Therefore, it will be needed to resort to the tight bound from algebraic geometry obtained in the Hasse–Weil Theorem. Note that, in this case, $p = 2n + 1$ and the ring $\mathbb{Z}[i]/p\mathbb{Z}[i]$ contains zero divisors.

First, let us prove two technical lemmas that analyze what happens with the zero divisors of the ring.

Lemma 20. *For any proper zero divisor $\zeta \in \mathbb{Z}[i]/p\mathbb{Z}[i]$,*

$$\zeta H = \{x\zeta \mid x \in \mathbb{Z}/p\mathbb{Z}, \ x \neq 0\}.$$

Proof. On the one hand, by Corollary 15, the cardinal $|\zeta H|$ is $2n$. On the other hand, $|\{x\zeta \mid x \in \mathbb{Z}/p\mathbb{Z},\ x \neq 0\}|$ has $p - 1 = 2n$ elements. Since both sets have the same size, it is enough to prove one inclusion to show the sets equality. Therefore, let us prove the left to right inclusion.

Let $\beta = a + bi$ be an element of norm 1 and $\zeta = u + vi$ a proper zero divisor, hence of norm 0. As $\zeta \neq 0$ and $\mathbb{Z}/p\mathbb{Z}$ is a field, both u and v are nonzero. Let us define $x = a - b\frac{v}{u} \in \mathbb{Z}/p\mathbb{Z}$. Therefore,

$$x\zeta = (a - b\frac{v}{u})(u + vi) = (au - bv) + (av - b\frac{v^2}{u})i$$

$$= (au - bv) + (av - b\frac{-u^2}{u})i = (au - bv) + (av + bu)i$$

$$= (a + bi)(u + vi) = \beta\zeta.$$

Finally, note that if x were zero, then β would be a zero divisor, contradicting $\mathcal{N}(\beta) = 1$. $\qquad\square$

The following lemma has its inspiration in Lemma 16, but with the intention of generalizing to the case of zero divisors.

Lemma 21. *For any proper zero divisor $\zeta \in \mathbb{Z}[i]/p\mathbb{Z}[i]$,*

$$\{\mathcal{N}(\beta + \zeta) \mid \mathcal{N}(\beta) = 1\} = \mathbb{Z}/p\mathbb{Z} \setminus \{1\}.$$

Proof. Let $\zeta = u + vi$ be a proper zero divisor. By Lemma 20,

$$\{\mathcal{N}(\beta + \zeta) \mid \mathcal{N}(\beta) = 1\} = \{\mathcal{N}(1 + \beta\zeta) \mid \mathcal{N}(\beta) = 1\}$$
$$= \{\mathcal{N}(1 + x\zeta) \mid x \in \mathbb{Z}/p\mathbb{Z},\ x \neq 0\}$$
$$= \{1 + 2xu \mid x \in \mathbb{Z}/p\mathbb{Z},\ x \neq 0\}.$$

To finish, note that $y = 1 + 2xu$ with $x \neq 0$ has solution for every value of y except 1. $\qquad\square$

The previous lemma indicates that proper zero divisors are neighbours of every vertex at distance 2 from 0, and hence they are at distance 3 from 0. Then, the following lemma gives a polynomial description of the sets $N_p(t)$.

Lemma 22. *Let $p \equiv 1 \pmod 4$ be a prime in $\mathbb{Z}$. For any $t \in \mathbb{Z}/p\mathbb{Z}$, $t \neq 0$, it is obtained that*

$$N_p(t) = \{x^{-1}(x + 1)(x + t) \mid x \in \mathbb{Z}/p\mathbb{Z},\ x \neq 0\}.$$

Proof. By the first item of Theorem 13, there exists $r \in \mathbb{Z}/p\mathbb{Z}$ such that $r^2 = -1$. Note that $x^{-1}(x + 1)(x + t) = x + tx^{-1} + t + 1$. First, let us prove the left to right inclusion of the sets. In this aim, let $\beta = a + bi$, $\mathcal{N}(\beta) = a^2 + b^2 = t$ for a generic element $\mathcal{N}(1 + \beta)$ in $N_p(t)$. Thus, let us check that $x = a + rb$ satisfies $\mathcal{N}(1 + \beta) = x + tx^{-1} + t + 1$. By Lemma 9, $x\mathcal{N}(1 + \beta) = x(\mathcal{N}(1) + \mathcal{N}(\beta) + 2\Re(\beta)) = x(t + 1) + 2ax$. Hence,

$$x(x + tx^{-1} + t + 1) - x\mathcal{N}(1 + \beta)$$
$$= x^2 + t - 2ax$$
$$= t + (a + rb)^2 - 2a(a + rb)$$
$$= t + (a^2 + 2rab + r^2b^2) - (2a^2 + 2rab)$$
$$= t - a^2 + r^2b^2$$
$$= t - a^2 - b^2$$
$$= 0.$$

For the right to left inclusion, let $x \neq 0$ and $y = x^{-1}(x + 1)(x + t)$ being an element of $\{x^{-1}(x + 1)(x + t) \mid x \in \mathbb{Z}/p\mathbb{Z},\ x \neq 0\}$. Now, define $\beta = x + x^{-1}(t - x^2) + 2^{-1}x^{-1}(t - x^2)ri$. Then, by calculation $\mathcal{N}(\beta) = (x + x^{-1}(t - x^2))^2 + (2^{-1}x^{-1}(t - x^2)r)^2 = t$. Moreover, $\mathcal{N}(1 + \beta) = 1 + t + 2\Re(\beta) = 1 + t + 2x + x^{-1}(t - x^2) = y$, which ends the proof. $\qquad\square$

The intersection between $N_p(1)$ and $N_p(t)$ will be given by the roots of the polynomial $P_t(x, y) = y(x + 1)^2 - x(y + 1)(y + t)$. In order to apply the Hasse–Weil bound, the polynomial must be irreducible. Therefore, let us introduce the following definition and two useful results in Lemma 24 and Corollary 25.

Definition 23. *Given a field $\mathbb{F}$, a polynomial $P \in \mathbb{F}[x, y]$ is called absolutely irreducible if it is irreducible in the algebraic closure of $\mathbb{F}$.*

Lemma 24. *For any prime p, the polynomial $P_t(x, y) = y(x + 1)^2 - x(y + 1)(y + t) \in \mathbb{Z}_p[x, y]$ is absolutely irreducible for $t \neq 0, 1$.*

Proof. The polynomial $P_t(x, y) = xy(x - y) + (1 - t)xy + y - tx$ has degree 3. If $P_t(x, y)$ is not absolute irreducible, then there exist polynomials $A(x, y)$, $B(x, y)$ with coefficients in the algebraic closure of $\mathbb{Z}/p\mathbb{Z}$ such that $P_t(x, y) = AB$ with $\deg A(x, y) = 2$ and $\deg B(x, y) = 1$. Furthermore, the product of the leading terms of $A(x, y)$ and $B(x, y)$ must be $xy(x - y)$. Let us consider the following three mutually exclusive cases, depending on polynomials $A(x, y)$ and $B(x, y)$

1. Case $A(x, y) = (xy + ax + by + c)$, $B(x, y) = (x - y + d)$. The coefficient of x^2 in $A(x, y) \cdot B(x, y)$ is a and the one of y^2 is $-b$. By hypothesis, both are 0 in $P_t(x, y)$. Then, the coefficient of xy is $d = 1 - t$, the coefficient of x is $c = -t$ and the coefficient of y is $-c = t = 1$. Hence, for $t = 1$ there exists the factorization $P_1(x, y) = (xy - 1)(x - y)$.

2. Case $A(x, y) = (x(x - y) + ax + by + c)$, $B(x, y) = (y + d)$. Now, the coefficient of x^2 in $A(x, y) \cdot B(x, y)$ is $d = 0$ and the coefficient of y^2 is $b = 0$. Then, the coefficient of xy is $a = 1 - t$, the coefficient of x is $0 = -t$ and the coefficient of y is $c = 1$. Hence, for $t = 0$ there exists the factorization $P_0(x, y) = (x^2 - xy + x + 1)y$.

3. Case $A(x, y) = (y(x - y) + ax + by + c)$, $B(x, y) = (x + d)$. The coefficient of x^2 is $a = 0$ and the coefficient of y^2 is $-d = 0$. Then, the coefficient of y would be $0 = 1$, which implies that there exists no factorization.

Finally, there are factorizations of $P_t(x, y)$ only for $t = 0$ and $t = 1$, which proves the result. $\square$

Corollary 25. *The homogeneous polynomial*

$$^h P_t(x, y, z) = xy(x - y) + (1 - t)xyz + (y - tx)z^2$$

is absolutely irreducible for $t \neq 0, 1$.

Proof. If $^h P_t(x, y, z)$ had a factorization, then its evaluation at $z = 1$ would be a factorization of $P_t(x, y)$, contradicting Lemma 24. $\square$

Finally, let us conclude the section by proving the main result.

Theorem 26. *If p is a prime such that $p \equiv 1 \pmod 4$ and $p > 5$, then the diameter of $\mathcal{G}_p$ is 3.*

Proof. Let us proceed again by *reductio ad absurdum*. First, let us assume the existence of a vertex γ at distance 4 from 0 in $\mathcal{G}_p$, with p fulfilling the hypothesis of the statement. Let $t = \mathcal{N}(\gamma)$. Note that $t \neq 1$ since the vertices with norm equal to 1 are at distance 1. Also, $t \neq 0$ by Lemma 21. Hence, by Lemma 12, the vertices with norm in the set $N_p(t) \setminus \{0\}$ are at distance at least 3. Meanwhile, the vertices with norm in $N_p(1) \setminus \{0\}$ are at distance at most 2 from 0. Therefore, the intersection of previous two sets is $N_p(1) \cap N_p(t) = \{0\}$.

Now, using polynomial notation, previous sets equality is equivalent, by Lemma 22, to the non-existence of solutions to $x^{-1}(x + 1)^2 = y^{-1}(y + 1)(y + t)$ other than $x = -1$. Let us highlight that the solution $x = -1$ corresponds with norm 0. Thus, vertices in H have vertex 0 as their neighbour, while vertices in γH have as some of their neighbours vertices that are proper zero divisors.

The contradiction will be obtained when proving the existence of a solution to $P_t(x, y) = 0$ other than the trivial ones $(x, y) \in \{(0, 0), (-1, -1), (-1, -t)\}$. To this aim, let us define the varieties

$$V_t = \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid P_t(x, y) = 0\},$$

$$X_t = \{(x : y : z) \in \mathbb{P}^2_{\mathbb{Z}/p\mathbb{Z}} \mid {}^h P_t(x, y, z) = 0\},$$

where $\mathbb{P}^2_{\mathbb{Z}/p\mathbb{Z}}$ denotes the projective space of dimension 2 over $\mathbb{Z}/p\mathbb{Z}$. The notation $(x : y : z)$ indicates a projective point, which is the same point as $(\lambda x : \lambda y : \lambda z)$ for any $\lambda \neq 0$. Thus, affine solutions can be recovered by taking $\lambda = z^{-1}$; except for solutions $(x : y : 0)$, which are the points at the infinite.

Hasse–Weil's theorem [8] states that

$$\big| |X_t| - (p + 1) \big| \leq 2\sqrt{p},$$

for absolutely irreducible polynomial curves X_t of degree 3. Note that, by Corollary 25, Hasse–Weil's theorem can be applied to $^h P_t(x, y, z)$. Therefore,

$$|X_t| \geq p + 1 - 2\sqrt{p}.$$

Now, the only 3 projective solutions for $^h P_t(x, y, z) = 0$ with $z = 0$ are $(x : y : z) \in \{(0 : 1 : 0), (1 : 0 : 0), (1 : 1 : 0)\}$. Thus, $|V_t| = |X_t| - 3$, which implies:

$$|V_t| \geq p - 2 - 2\sqrt{p}.$$

As a consequence, those primes p such that $|V_t| \geq 4$ provide the expected contradiction. Clearly, if $p \geq 17$ then,

$$|V_t| \geq p - 2 - 2\sqrt{p} \geq 17 - 2 - 2\sqrt{17} \geq 6.7.$$

Finally, the unique prime $p \equiv 1 \pmod 4$ such that $5 < p < 17$ is 13. In this particular case, it can be computed that $|V_t| \geq 9$ for any t, which concludes the proof. $\square$

Remark 27. $\mathcal{G}_5$ *has diameter 4 since vertex $2 + 2i$ and its associates are at distance 4 from vertex 0.*

n	p	H	p^2	$|B_3^n|$
4	13	$\pm\{1, 3+4i, i, -4+3i\}$	169	129
6	26	$\pm\{1, 4+4i, 9+11i, i, -4+4i, -11+9i\}$	676	377
8	41	$\pm\{1, 2+13i, 6+18i, 11+i, i, -13+2i, -18+6i, -1+11i\}$	1681	833

Table 1: $\mathcal{G}_p$ graphs that generate 3-quasi-perfect Lee codes over $\mathbb{Z}_p^n$.

5 Discussion

In this final section, conclusions of this work and future research will be presented. In the first subsection, the main result is rewritten using parity-check matrices. Besides, a formal proof of the infiniteness of the constructed family of quasi-perfect codes is given. Some considerations on the density of the codes are taken into account. Moreover, other examples of codes presenting greater density and an upper error correction capacity are shown. In the final subsection, the authors exhibit the relations between the graphs considered in the present study with other graph theoretical problems, trying to give a new insight into the perfect Lee codes conjecture formulated by Golomb and Welch more than forty years ago.

5.1 Quasi-perfect Lee codes

As it has been proved in previous Sections 3 and 4, $\mathcal{G}_p$ has error correction capacity 2 and diameter 3, for any prime $p > 5$ and $p \equiv \pm5 \pmod{12}$.

Dirichlet's theorem on arithmetic progressions asserts that, in any arithmetic progression whose initial term is coprime with its increment, there are infinitely many primes. As a natural consequence, congruences can be considered as arithmetic progressions, and therefore it can be obtained:

Corollary 28. *There are infinitely many $n \in \mathbb{N}$ such that $p = 2n \pm 1$, $p \geq 7$ prime in $\mathbb{Z}$, $p \equiv \pm5 \pmod{12}$.*

Then, when applying the previous result it is obtained:

Corollary 29. *The family of graphs $\mathcal{G}_p$ contains infinitely many graphs with error correction capacity 2 and diameter 3.*

Then, as it was discussed in Section 2, each of these graphs induces a 2-quasi-perfect Lee code.

Theorem 30. *Let p be a prime. Let $\{\beta_1, \ldots, \beta_{2n}\} = \{\pm\beta_1, \ldots, \pm\beta_n\}$ be the elements of $\mathbb{Z}[i]/p\mathbb{Z}[i]$ with unitary norm. Let $\mathcal{G}_p = Cay(\mathbb{Z}[i]/p\mathbb{Z}[i], \{\beta_1, \ldots, \beta_{2n}\})$ and $\mathcal{C} \subset \mathbb{Z}_p^n$ be the code associated to $\mathcal{G}_p$ such that $\mathcal{C} = \ker\phi$ and $\phi : \mathbb{Z}_p^n \longrightarrow \mathbb{Z}[i]/p\mathbb{Z}[i]$ such that $\phi(e_j) = \beta_j$. Then,*

$$M = \begin{pmatrix} \Re(\beta_1) & \Re(\beta_2) & \cdots & \Re(\beta_n) \\ \Im(\beta_1) & \Im(\beta_2) & \cdots & \Im(\beta_n) \end{pmatrix}.$$

is the parity-check matrix of $\mathcal{C}$.

Proof. Let us denote by $\psi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}^2$ such that $\psi(\beta) = (\Re(\beta), \Im(\beta))$. Note that the homomorphism defined by the matrix M is equal to the mapping $\psi \circ \phi$. Thus, $\mathcal{C} = \ker(\phi) = \ker(\psi \circ \phi) = \{x \mid Mx = 0\}$. $\square$

Now, let us give some considerations on the quality of the constructed codes. Note that, since the Lee sphere of radius 2 contains $|B_2| = 2n^2 + 2n + 1$ words, the graph induced by any 2-quasi-perfect linear code has at least $2n^2 + 2n + 1$ vertices. The graphs $\mathcal{G}_p$ constructed in this paper have p^2 vertices. Therefore, for the case $p = 2n + 1$, the number of vertices is $p^2 = 4n^2 + 4n + 1 = 2|B_2| - 1$. Also, for the case $p = 2n - 1$, the number of vertices is $p^2 = 4n^2 - 4n + 1 = 2|B_2| - 8n - 1$. Thus, the reached vertices are asymptotically the double of those that would be reached in the graph associated to a perfect code. In other words, the density of the codes presented is $\frac{1}{p^2}$.

Although the obtained density is quite good, for some small cases (low dimensions), graphs with a smaller number of vertices have been computationally found. Let us consider the following examples.

Example 2. *Let $n = 8$ be the dimension and $p = 13$. The set of generators of the Cayley graph will be $H = \{\beta u \mid \beta \in \{1, 4+10i, 8, 7+11i\}, u \in \mathcal{U}(\mathbb{Z}[i])\}$. In this case the Cayley graph $\mathcal{G} = Cay(\mathbb{Z}[i]/p\mathbb{Z}[i], H)$ induces a 2-quasi-perfect code. Note that $\mathcal{G}$ has $p^2 = 169$ vertices, which is just 17% over $|B_2^8| = 145$, the cardinal of the sphere in this dimension.*

Example 3. *Let $n = 16$ be the dimension. In this case, by extending the search into a different ring, a new graph has been found. The graph is built over the Quaternion integers $\mathbb{H}(\mathbb{Z})$ modulo $p = 5$, being the generator set $H = \{\beta u \mid \beta \in \{1, 1+2i+3j, 3i+4j+4k, 3+4i+3j\}, u \in \mathcal{U}(\mathbb{H}(\mathbb{Z}))\}$. In this case, the number of vertices of the graph is $p^4 = 625$, which is 15% over $|B_2^{16}| = 545$.*

These small examples suggest that there exist codes very close to be perfect, although general constructions seem to be difficult to find.

Golomb and Welch in [13] noted that there cannot be perfect codes with correction greater than a constant that depends on the dimension by the use of the maximum density of packing with cross-polytopes. Clearly, this can be applied to quasi-perfect codes. For every n there exists t_n such that there are no t-quasi-perfect codes for $t \geq t_n$. Hence, this might suggest that the radius 2 case is an exceptional one. Nevertheless, some 3-quasi-perfect codes have been found for small dimensions. Note that in this case the n-dimensional sphere of radius 3 has cardinal $|B_3^n| = \frac{1}{3}(1+2n)(3+2n+2n^2)$. The examples that we have found are summarized in Table 1. The codes are obtained from Cayley graphs $Cay(\mathbb{Z}[i]/p\mathbb{Z}[i], H)$, for parameters n, p, H as shown in the table. As it can be seen, the first example is just 31% over the cardinal of the sphere, while the second and third are 79% and 102%, respectively. Any of the three examples can be considered as 3-quasi-perfect codes really near to the perfect code.

In the authors' opinion, the construction of an infinite family of graphs containing these codes or similar ones would have a great practical value. Moreover, it would contribute to a better understanding of the Golomb and Welch conjecture.

5.2 Related Problems

This study could be used to deal with problems from areas of study different from Coding Theory. For example, this graph theoretical study of perfect codes can be seen as the reverse of the degree-diameter problem for Cayley graphs over Abelian finite groups [27]. In this problem, for a given diameter, graphs with the maximum possible number of vertices are searched. Specifically, for a positive integer t, graphs providing t-covering codes but without considering the correction are looked for. Note that in this case, the order of the graphs obtained is lower than the cardinal of the corresponding sphere $|B_t^n|$. Therefore, in the present paper graphs providing t-correcting codes and enforcing additionally $(t + 1)$-covering have been constructed. In our case, the order of the Cayley graphs is always greater than the cardinal of the sphere $|B_t^n|$. The degree-diameter problem for $t = 2$ and $t = 3$ has been considered in [23, 34]. In those papers families of graphs with smaller number of vertices than the sphere cardinal were given. Specifically, one of the graph constructions in Macbeth *et al.* [23] is given for infinitely many degrees $2n$ of graphs of diameter 2 and $\frac{3}{2}(n^2 - 1) = \frac{3}{4}|B_2^n| - \frac{3}{2}n - \frac{9}{4}$ vertices. Then, Vetrík [34] constructs graphs with diameter 3 and $\frac{9}{128}(2n+3)^2(2n-5)$ vertices, which is asymptotically $\frac{27}{64}|B_3^n|$; it is remarkable that these graphs have error correction capacity 1 instead of the expected 2, and thus they do not induce quasi-perfect codes. Note that a Cayley graph attaining the degree-diameter bound will induce a perfect code and *vice versa*.

Furthermore, the graphs considered in this paper seemed to be good expanders. Therefore, the authors computed the spectrum of some of them and the results show that they are Ramanujan graphs. *Ramanujan graphs* are good expander graphs that attain the spectral bound [10]. More specifically, $\mathcal{G}$ is a Ramanujan graph if and only if for every eigenvalue λ of its adjacency matrix it holds either $|\lambda| = \deg(\mathcal{G})$ or $|\lambda| \leq 2\sqrt{\deg(\mathcal{G}) - 1}$. Therefore, the following conjecture is proposed.

Conjecture 31. *$\mathcal{G}_p$ is a Ramanujan graph for any prime $p \equiv 3 \pmod 4$.*

This conjecture has been verified for all primes $p < 1000$; the only primes in that range for which $\mathcal{G}_p$ is not Ramanujan are 17, 53 and 541. Moreover, the authors believe that *most primes* fulfilling $p \equiv 1 \pmod 4$ are such that $\mathcal{G}_p$ is also a Ramanujan graphs. Therefore, the proof of this conjecture and the study of the relation between Golomb and Welch conjecture and spectral analysis will be considered as future work.

Acknowledgments

References

[1] Rudolf Ahlswede, Harout K. Aydinian, and Levon H. Khachatrian. On perfect codes and related concepts. *Designs, Codes and Cryptography*, 22(3):221–237, 2001.

[2] Bader F. AlBdaiwi and Bella Bose. Quasi-perfect Lee distance codes. *Information Theory, IEEE Transactions on*, 49(6):1535–1539, June 2003.

[3] Bader F. AlBdaiwi, Peter Horak, and Lorenzo Milazzo. Enumerating and decoding perfect linear Lee codes. *Designs, Codes and Cryptography*, 52(2):155–162, 2009.

[4] Carlos Araújo, Italo J. Dejter, and Peter Horak. A generalization of Lee codes. *Designs, Codes and Cryptography*, 70(1-2):77–90, 2014.

[5] Helena Astola and Stanislav Stankovic. On the use of Lee-codes for constructing multiple-valued error-correcting decision diagrams. In *Communications Control and Signal Processing (ISCCSP), 2012 5th International Symposium on*, pages 1–6. IEEE, 2012.

[6] Helena Astola and Ioan Tabus. Bounds on the size of Lee-codes. In *Image and Signal Processing and Analysis (ISPA), 2013 8th International Symposium on*, pages 471–476, September 2013.

[7] Jaakko Astola. An Elias-type bound for Lee codes over large alphabets and its application to perfect codes (corresp.). *Information Theory, IEEE Transactions on*, 28(1):111–113, January 1982.

[8] Henri Cohen. *Number Theory: Volume I: Tools and Diophantine Equations*, volume 1. Springer, 2007.

[9] Sueli I. R. Costa, Marcelo Muniz, Edson Agustini, and Reginaldo Palazzo Jr. Graphs, tessellations, and perfect codes on flat tori. *Information Theory, IEEE Transactions on*, 50(10):2363–2377, October 2004.

[10] Giuliana Davidoff, Peter Sarnak, and Alain Valette. *Elementary number theory, group theory and Ramanujan graphs*, volume 55. Cambridge University Press, 2003.

[11] Tuvi Etzion. Product constructions for perfect Lee codes. *Information Theory, IEEE Transactions on*, 57(11):7473–7481, November 2011.

[12] Tuvi Etzion, Alexander Vardy, and Eitan Yaakobi. Coding for the Lee and Manhattan metrics with weighing matrices. *Information Theory, IEEE Transactions on*, 59(10):6712–6723, October 2013.

[13] Solomon W. Golomb and Lloyd R. Welch. Perfect codes in the Lee metric and the packing of polyominoes. *SIAM Journal on Applied Mathematics*, 18(2):302–317, 1970.

[14] Sylvain Gravier, Michel Mollard, and Charles Payan. On the non-existence of 3-dimensional tiling in the Lee metric. *European Journal of Combinatorics*, 19(5):567–572, 1998.

[15] Godfrey Harold Hardy and Edward Maitland Wright. *An introduction to the theory of numbers*, volume 4. Oxford University Press, fourth edition, 1979.

[16] Peter Horak. On perfect Lee codes. *Discrete Mathematics*, 309(18):5551–5561, 2009. Combinatorics 2006, A Meeting in Celebration of Pavol Hell's 60th Birthday (May 1–5, 2006).

[17] Peter Horak. Tilings in Lee metric. *European Journal of Combinatorics*, 30(2):480–489, 2009.

[18] Peter Horak and Bader F. AlBdaiwi. Diameter perfect Lee codes. *Information Theory, IEEE Transactions on*, 58(8):5490–5499, August 2012.

[19] Peter Horak and Otokar Grošek. A new approach towards the Golomb–Welch conjecture. *European Journal of Combinatorics*, 38:12–22, 2014.

[20] Klaus Huber. Codes over Gaussian integers. *Information Theory, IEEE Transactions on*, 40(1):207–216, January 1994.

[21] Anxiao Jiang, Moshe Schwartz, and Jehoshua Bruck. Correcting charge-constrained errors in the rank-modulation scheme. *Information Theory, IEEE Transactions on*, 56(5):2112–2120, 2010.

[22] Timo Lepistö. A modification of the Elias-bound and nonexistence theorems for perfect codes in the Lee-metric. *Information and Control*, 49(2):109–124, 1981.

[23] Heather Macbeth, Jana Šiagiová, and Jozef Širáň. Cayley graphs of given degree and diameter for cyclic, Abelian, and metacyclic groups. *Discrete Mathematics*, 312(1):94–99, 2012. Algebraic Graph Theory – A Volume Dedicated to Gert Sabidussi on the Occasion of His 80th Birthday.

[24] Carmen Martínez, Ramón Beivide, and Ernst M. Gabidulin. Perfect codes for metrics induced by circulant graphs. *Information Theory, IEEE Transactions on*, 53(9):3042–3052, 2007.

[25] Carmen Martínez, Ramón Beivide, and Ernst M. Gabidulin. Perfect codes from Cayley graphs over Lipschitz integers. *Information Theory, IEEE Transactions on*, 55(8):3552–3562, August 2009.

[26] Carmen Martínez, Esteban Stafford, Ramón Beivide, Cristóbal Camarero, Fernando Vallejo, and Ernst Gabidulin. Graph-base metrics over QAM constellations. In *2008 IEEE International Symposium on Information Theory*, pages 2494–2498, July 2008.

[27] Mirka Miller and Jozef Sirán. Moore graphs and beyond: A survey of the degree/diameter problem (2nd ed). *The Electronic Journal of Combinatorics*, 5 2013.

[28] Emil Molnár. Sui mosaici dello spazio di dimensionen. *Atti Accad. Naz. Lincei, VIII. Ser., Rend., Cl. Sci. Fis. Mat. Nat*, 51:177–185, 1971.

[29] Shigeto Nishimura and Toyokazu Hiramatsu. A generalization of the Lee distance and error correcting codes. *Discrete Applied Mathematics*, 156(5):588–595, 2008.

[30] Karel A. Post. Nonexistence theorems on perfect Lee codes over large alphabets. *Information and Control*, 29(4):369–380, 1975.

[31] Cátia Quilles Queiroz, Cristóbal Camarero, Carmen Martínez, and Reginaldo Palazzo Jr. Quasi-perfect codes from Cayley graphs over integer rings. *Information Theory, IEEE Transactions on*, 59(9):5905–5916, September 2013.

[32] Ron M. Roth and Paul H. Siegel. Lee-metric BCH codes and their application to constrained and partial-response channels. *Information Theory, IEEE Transactions on*, 40(4):1083–1096, July 1994.

[33] Simon Špacapan. Nonexistence of face-to-face four-dimensional tilings in the Lee metric. *European Journal of Combinatorics*, 28(1):127–133, 2007.

[34] Tomáš Vetrík. Abelian Cayley graphs of given degree and diameter 2 and 3. *Graphs and Combinatorics*, pages 1–5, 2013.