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

Cristóbal Camarero and Carmen Martínez *

December 19, 2014

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 $n = 2^{[4]}$. It is known that there are infinite such primes. Perfect codes for the Lee-metric were conjectured by Golomb and Welch not to exist, which has been proved for large radii and also for low dimension. The codes found are very close to be perfect, which tells about the nature of the conjecture. Some computations show that related graphs are Ramanujan, which could provide further connections between the fields.

1 Introduction

Golomb and Welch conjectured in their seminal paper [13] that perfect Lee codes do 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 given by approximating the problem to the densest tilling 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. If a perfect code exists, Post determined an upper bound for its radius, in terms of the dimension, specifically, the radius must fulfill $r < \frac{1}{2} \sqrt{2} - \frac{3}{2} \sqrt{2} - \frac{1}{4}$ 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. Those negative results in [30, 7, 22], suggest that the conjecture is more difficult for radius $2$, as argued by Horak in [16].

Other authors have considered the conjecture for small 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 considered by Špacapan in [34], again with the possibility of spheres of different radii but at least 2. Also, Horak in [17] and [16] proved the non-existence of perfect Lee codes in spaces of dimension up to $n \leq 6$. Later, to achieve higher dimensions, Horak and Grošek in [19] restricted the problem to linear codes and verified computationally the non-existence of perfect Lee codes for dimension $n \leq 12$ and radius $r = 2$.

On the other hand, several papers have considered problems around the conjecture that could give some insight. 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 $C \subseteq \mathbb{Z}_q^n$ is a diameter perfect code if there exists an anticode $A$ such that $|C||A| = q^n$. 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 $\mathbb{Z}_q$. 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.

A different approach to the existence of perfect Lee codes has been to relax the condition of being perfect. Thus, quasi-perfect codes for the Lee metric have been considered just in a small number of papers. 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 are obtained for $n = 2$.

In the present paper a explicit construction of linear quasi-perfect Lee codes of radius 2 for arbitrarily large dimension is given. As it will be shown, these codes are very close to be perfect since they have half of the density of potential perfect codes. In the authors' opinion, the existence of these quasi-perfect codes, hints that maybe a perfect code could exist for low radius; and if they do not exist then the proof must be of a very different nature than the proofs in previous papers dealing with the conjecture.

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 $p \equiv \pm 5$ (mod 12) there exists a linear 2-quasi-perfect $p$-ary Lee code over $\mathbb{Z}_p^n$, where $n = 2 \left\lceil \frac{p}{4} \right\rceil$ and with $p^{n-2}$ codewords.

Note that the notation $\lceil a \rceil$ 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 $\frac{1}{7} \approx 58.56$.

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

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

As it will be seen later, the result is constructive, and any application that requires the use of Lee-codes can 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 concludes 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. Moreover, 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-like

\[ \mathbb{Z}^n \] .

This code is said to be linear or lattice-like if it is a subgroup of the corresponding space.

In the space \( \mathbb{Z}^n \) it will be used the Manhattan distance. 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 when considering \( \mathbb{Z}_p^n \). For \( v, w \in \mathbb{Z}_p^n \) its Lee distance is defined as

\[
    d(v, w) = \sum_{j=1}^{n} \min\{|s| \mid s \equiv v_i - w_i \pmod{p}, s \in \mathbb{Z}\}.
\]

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 zero vector, which will be denoted as \( |v| = d(v, 0) \). For any positive integer \( r \), the Lee sphere of radius \( r \) is defined as all the points with weight less or equal to \( r \), that is:

\[
    B^n_r = \{ v \mid |v| \leq r \}.
\]

Note that, for any dimension \( n \geq 1 \), the cardinal \( |B^n_r| = 2n^2 + 2n + 1 \).

A code \( C \) is said t-error correcting if \( t \) is the greatest integer such that for any word \( w \) there is at most one codeword \( c \in C \) with \( d(w, c) \leq t \). A code \( C \) is said \( r \)-covering if \( r \) is the smallest integer such that for any word \( w \) there is at least one codeword \( c \in C \) with \( d(w, c) \leq r \). Then, a code that is both \( t \)-error correcting and \( r \)-covering 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 ones. 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 dimension. This is done by the construction of a family of Cayley graphs that leads to the codes definition. In the remaining section the infinite lattice \( \mathbb{Z}^n \) will be considered. An equivalent relation can be stated in the case of \( \mathbb{Z}_p^n \).

Codes and tilings are closely related as it is manifested in many papers. Given a linear code \( C \), the tessellation induced by the Voronoi regions of the codewords can be considered. The Voronoi region of a codeword is composed by the words that are closer to it than to other codewords. Since the code is linear, the tessellation is congruent, that is, all the tiles have the same shape and size. If \( C \) is a \( t \)-perfect error correcting code then the tiles obtained are translations of the Lee sphere of radius \( t \). Otherwise, for a \( t \)-correcting and \( r \)-covering code, each induced tile contains a Lee sphere of radius \( t \) and it is contained in a Lee sphere of radius \( r \). Reciprocally, the centers
of the congruent tiles of a lattice-like tessellation can be used to define a linear code.

Once the tessellation induced by the linear code is obtained, then this tessellation can be used to define a Cayley graph. Given a group $\Gamma$ and a set of generators $H = \{\beta_1, \ldots, \beta_s\} \subset \Gamma$, the Cayley graph over $\Gamma$ generated by $H$ is defined as the graph with set of vertices the elements of $\Gamma$, and adjacencies $(u, u + \beta_i)$, for every $u \in \Gamma$ and $i = 1, \ldots, s$. Now, if $H = -H$ then the Cayley graph is undirected, as the ones considered in this paper. Thus, this graph is denoted by $Cay(\Gamma, H)$. The distance between two vertices in a graph is calculated as the length of a minimum path that joins them. Therefore, the diameter of a graph is the maximum among distances between every pair of vertices.

Now, let us consider a tessellation of congruent tiles by translations. Then, a graph can be defined by considering the words inside the tile centered at codeword 0 as its set of vertices. To define the adjacency, two different situations can be considered. For the vertices inside the tile, two vertices are adjacent if they are at a distance 1. In the case of vertices in the boundary of the tile, two vertices $u$ and $v$ are adjacent if there is a tile center $c$ such that $d(u, c + v) = 1$. Note that, since the tessellation comes from a linear code, the graph is a undirected Cayley graph over the Abelian group $\mathbb{Z}^n/\mathbb{Z}$. Now, if $t$ is the greatest integer such that the Lee sphere $B^t_i$ is contained in the tile, then this graph has $|B^t_i|$ vertices at distance $t$ or less. By analogy to the concept of correction in codes, this value $t$ will be referred as the error correction capacity of the graph. If $r$ is the smallest positive integer such that $B^r_i$ contains the tile, then the graph has diameter $r$. Given a Cayley graph it is straightforward to obtain a lattice-like congruent tiling. The tile can be defined by the representation in minimum distances of the set of vertices. Then, the tiling of the space is induced by the adjacency of the peripheral vertices.

In the rest of the paper a family of Cayley graphs over Gaussian integers will be considered. Let us denote by $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ the ring of the Gaussian integers. In Appendix A there is a summary of some fundamentals on this ring. 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 3.** Given an integer prime $p$, let us define the Cayley graph $G_p = Cay(\mathbb{Z}[i]/p\mathbb{Z}[i], H)$, where

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

Note that in previous definition $N(\beta) = N(b_1 + b_2i) = b_1^2 + b_2^2$ denotes the norm of $\beta$. Moreover, the adjacency in the graph is determined by the elements with unitary norm. In the following sections, it will be proved that $G_p$ induces a 2-quasi-perfect Lee code over $\mathbb{Z}_n^2$ under some conditions. Therefore, it must be determined which primes $p$ are such that $G_p$ has error correction capacity 2 and diameter 3.

### 3 Error Correction Capacity of $G_p$

As explained in previous section, 2-quasi-perfect Lee codes are going to be obtained by means of Cayley graphs. In particular, it will be determined under which conditions the Cayley graph $G_p$ over the additive group $\mathbb{Z}[i]/p\mathbb{Z}[i]$ and generating set those elements with unitary norm induces a 2-quasi-perfect code. In this section it will be proved that $p \equiv \pm 5 \pmod{12}$ implies that $G_p$ has error correction capacity 2 over $\mathbb{Z}_n^2$ for $n = 2\lfloor\frac{p}{2}\rfloor$. Hence, in the remainder of the paper, let us assume that $p > 2$ is a prime integer. Therefore, the natural number $n = 2\lfloor\frac{p}{2}\rfloor$ fulfills $p = 2n \pm 1$.

First, let us introduce some notation. Given a Gaussian integer $\beta = b_1 + b_2i \in \mathbb{Z}[i]$, $\beta^*$ will denote its conjugate, that is $\beta^* = b_1 - b_2i$. Also, $R(\beta) = b_1$ will stand for its real part and $S(\beta) = b_2$ 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 4.** For any pair of Gaussian integers $\beta, \gamma \in \mathbb{Z}[i]$,

$$N(\beta + \gamma) = N(\beta) + N(\gamma) + 2R(\beta^* \gamma).$$
Then, the previous result can be used to prove the following technical lemma:

**Lemma 5.** 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 4 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 \( \gamma_1 \in \{\gamma_2, \gamma_2^*\} \).

**Corollary 6.** 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 5 \( \beta \in \{-1, -1^*\} = \{-1\} \) and \( 1 + \beta = 0 \).

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 \( \mathcal{G}_p \), this is, \( G = \text{Cay}(\mathbb{Z}[i]/p\mathbb{Z}[i], H) \). 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 \( \gamma H \) is the coset of \( H \) in \( G \) with respect to \( \gamma \). 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 7.** 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 \( \gamma \) is invertible, \( \beta = \gamma (\beta \gamma^{-1}) \). Now, as \( \mathcal{N}(\beta \gamma^{-1}) = 1 \) it is obtained that \( \beta \in \gamma H \).

Theorem 8 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 8 (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 \( p = 2 \) or \( p = 3 \) and
   - \( 0 \) otherwise.

**Theorem 9.** For any odd prime integer \( p \), let \( n = 2[\frac{p}{4}] \). Then,

\[
|H| = |\{(x, y) \mid x, y \in \mathbb{Z}/p\mathbb{Z}, \ x^2 + y^2 = 1\}| = 2n.
\]

**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 look for the rest of 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 \( x = \frac{2s}{s^2 + 1} \). This second solution for \( x \) equals 1 if and only if \( p = 2 \). Thus, the only solutions with \( x \neq 1 \) are \( x = \frac{2s}{s^2 + 1} \) 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 9) 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 $s_1 = s_2 = y/(x - 1)$.

Next, it can be easily obtained the following consequence of previous theorem, which will be used in Section 4 to determine the diameter of the graph $G_p$.

**Corollary 10.** For any odd prime integer $p$, let $n = 2[\frac{p}{4}]$. If $0 \neq \gamma \in \mathbb{Z}[i]/\mathbb{Z}[i]$ then $|\gamma H| = 2n$.

**Proof.** Firstly, note that if $\gamma \in G$, then $\gamma H$ is a coset, which are widely known to have the same cardinal. Thus, the non-immediate part of the proof lies on the zero divisors. By Theorem 9 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 $\beta_1^{-1}$, $1 - \beta_2 \beta_1^{-1}$ is also a zero divisor. By Corollary 9, $1 - \beta_2 \beta_1^{-1} = 0$ and hence $\beta_1 = \beta_2$, which is a contradiction.

Before stating the conditions under which $G_p$ 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 11.** For any $c \in \mathbb{Z}/p\mathbb{Z}$, $c \neq 0$, let us consider the set $N_p(c) = \{N(1 + \beta) \mid N(\beta) = c\} \subset \mathbb{Z}/p\mathbb{Z}$. 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 7 and Corollary 10 there are $2n$ elements with norm $c$, which are:

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

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

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

which are different by Lemma 9. 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

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

Then

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

which are different by Lemma 9. Hence $|N_p(c)| = n$.

As it will be noted afterwards, the case $c = 1$ in previous lemma is going to 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 $G_p$ has error correction capacity 2.

**Theorem 12.** Let $p$ be a prime integer satisfying $p \equiv \pm 5 \pmod{12}$. Let $n = 2[\frac{p}{4}]$. Then, the Cayley graph $G_p$ has error correction capacity 2.

**Proof.** As it was explained in previous section, it has to be proved that $G_p$ contains $|B_2^p| = 2n^2 + 2n + 1$ 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 9.
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 7 and Corollary 10 \(|A| = 2n \cdot |N_p(1) \setminus \{0\}|\). Since 1 is always a square residue for any \( p \), hence by Lemma 11 \(|N_p(1) \setminus \{0\}| = n\). It remains to be proved that 1 does not belong to \( N_p(1) \).

Suppose that there is \( \beta \) with \( \mathcal{N}(\beta) = 1 \) and \( \mathcal{N}(1 + \beta) = 1 \). Then, by Lemma 4 \( 1 = 2 + 2 \mathcal{N}(\beta) \) and hence \( \mathcal{N}(\beta) = -2^{-1} \). 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 \( p \equiv \pm 1 \) (mod 12) by the second item of Theorem 8. Thus, \(|N_p(1) \setminus \{0,1\}| = |N_p(1) \setminus \{0\}| = n \) and \(|A| = 2n \cdot n\), which concludes the proof. \( \square \)

**Remark 13.** If \( p \) is a prime greater than 3 that does not satisfy \( p \equiv \pm 5 \) (mod 12), then \( p \equiv \pm 1 \) (mod 12). In this case, \( G_p \) 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 since only 2n syndromes cannot be corrected.

## 4 Diameter of \( G_p \)

In this section it will be proved that \( G_p \) has diameter 3 for any prime \( p > 5 \). The proof will be separated into two subsections, the first one considering the case \( p \equiv 3 \) (mod 4) and the second one the case \( p \equiv 1 \) (mod 4). Also, from here onwards it will be assumed again that \( n = 2[\mathbb{F}_p^2] \). Note that, since \(|\mathbb{Z}[i]/p\mathbb{Z}[i]| = p^2 > |B_2^3|\), 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 \( p \equiv 3 \) (mod 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 14.** For any prime \( p \) such that \( p \equiv 3 \) (mod 4) the graph \( G_p \) 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 of vertex 0. Let \( c = \mathcal{N}(\gamma) \). Since \( \gamma \) 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, \( \{W_t(0) \mid t = 0, \ldots, 4\} \) is the distance distribution of the graph \( G_p \). Now, the cardinals \( W_1(0) = |H| \) and \( W_4(0) \geq |\gamma H| \) can be calculated by Corollary 10. Also, by Lemma 11 it can be computed that \( |N_p(1)| = n + 1 \) and \( |N_p(c)| \geq n \). Thus, the bounds for the distance distribution obtained are summarized next:

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

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. \( \square \)

### 4.2 Case \( p \equiv 1 \) (mod 4)

Unfortunately, the reasoning of the previous case fails to give us a contradiction if \( p \equiv 1 \) (mod 4). Thereof, 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 15.** 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 one hand, by Corollary 10 the cardinal \(|\zeta H| = 2n \). On the other hand, \(|\{x\zeta \mid x \in \mathbb{Z}/p\mathbb{Z}, \ x \neq 0\}| = p - 1 = 2n \) 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 \( x = a - b\frac{u}{u} \in \mathbb{Z}/p\mathbb{Z} \). Therefore,

\[
x \zeta = (a - b\frac{u}{u})(u + vi) = (au - bv) + (av - b\frac{u^2}{u})i = (au - bv) + (av + bu)i = (a + bi)(u + vi) = \beta \zeta.
\]

Finally, note that \( x \) cannot be zero, since it would imply that \( \beta \) were a zero divisor, contradicting \( N(\beta) = 1 \).

The following lemma has its inspiration in Lemma \[16\], but with the intention to generalize to the case of zero divisors and to give a stronger result.

**Lemma 16.** For any proper zero divisor \( \zeta \in \mathbb{Z}[i] / p\mathbb{Z}[i] \),

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

**Proof.** Let \( \zeta = u + vi \) be a proper zero divisor. By Lemma \[15\] and by making few calculations,

\[
\begin{align*}
&\{ N(\beta + \zeta) \mid N(\beta) = 1 \} = \\
&\{ N(1 + \beta \zeta) \mid N(\beta) = 1 \} = \\
&\{ N(1 + x \zeta) \mid x \in \mathbb{Z}/p\mathbb{Z}, \ x \neq 0 \} = \\
&\{ 1 + 2xu \mid x \in \mathbb{Z}/p\mathbb{Z}, \ x \neq 0 \}.
\end{align*}
\]

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

The previous lemma indicates that proper zero divisors are neighbours of each 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 17.** 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 \[8\] 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 \( \beta = a + bi, N(\beta) = a^2 + b^2 = t \) for a generic element \( N(1 + \beta) \) in \( N_p(t) \). Thus, let us check that \( x = a + rb \) satisfies \( N(1 + \beta) = x + tx^{-1} + t + 1 \). By Lemma \[4\], \( x(1 + \beta) = x(N(1) + N(\beta) + 2R(\beta)) = x(t + 1 + 2ax) \). Hence,

\[
x(x + tx^{-1} + t + 1) - xN(1 + \beta) = \\
x^2 + t - 2ax = \\
t + (a + rb)^2 - 2(a + rb) = \\
t + (a^2 + 2rabb + r^2b^2) - (2a^2 + 2rabb) = \\
t - a^2 + r^2b^2 = \\
0
\]

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

The intersection between \( N_p(1) \) and \( N_p(t) \) will be given by the roots of polynomial \( P_t(x, y) = y(x + 1)^2 - y(y + 1)(y + t) \). 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 \[19\] and Corollary \[20\].

**Definition 18.** Given a field \( F \), a polynomial \( P \in F[x, y] \) is called absolutely irreducible if it is irreducible in the algebraic closure of \( F \).

**Lemma 19.** For any primer \( p \), 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 \( P_1(x, y) \). 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 \( A(x, y) = (x - y + ax + by + c), B(x, y) = (y + d) \). Now, the coefficient of \( x^2 \) in \( A(x, y) \cdot B(x, y) \) is \( 0 \) 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 \( A(x, y) = (y - x + ax + by + c), B(x, y) = (x + d) \). 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.

**Corollary 20.** The homogeneous polynomial

\[
^hP_t(x, y, z) = xy(x - y) + (1 - t)xyz + (y - tx)z^2
\]

is absolutely irreducible for \( t \neq 0, 1 \).

**Proof.** If \(^hP_t(x, y)\) had a factorization, then its evaluation at \( z = 1 \) would be a factorization of \( P_t(x, y) \), contradicting Lemma [19].

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

**Theorem 21.** If \( p \) is a prime such that \( p \equiv 1 \) (mod 4) and \( p > 5 \), then the diameter of \( G_p \) is 3.

**Proof.** Let us proceed again by *reductio ad absurdum*. In this aim, let us assume the existence of a vertex \( \gamma \) at distance 4 from 0 in \( G_p \), with \( p \) fulfilling the hypothesis of the statement. Let \( t = N(\gamma) \). Note that \( t \neq 1 \) since vertices with norm equal to 1 are at distance 1. Also, \( t \neq 0 \) by Lemma [16]. Hence, by Lemma [17] 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 [17], 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 \( \gamma H \) 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 \((x, y) \in \{(0, 0), (-1, -1), (-1, 1)\} \). In this aim, let us define the varieties

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

\[
X_t = \{(x : y : z) \in \mathbb{F}_2^2/\mathbb{Z}/p\mathbb{Z} \mid ^hP_t(x, y, z) = 0\},
\]

where \( \mathbb{F}_2^2/\mathbb{Z}/p\mathbb{Z} \) 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

\[ |X_t| - (p + 1) | \leq 2\sqrt{p}, \]

for absolutely irreducible polynomial curves \( X_t \) of degree 3. Note that, by Corollary [20], Hasse-Weil's theorem can be applied to \(^hP_t(x, y, z)\). Therefore,

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

Now, the only 3 projective solutions for \(^hP_t(x, y, z) = 0\) with \( z = 0 \) are \((x : y : z) \in\]
Remark 22. \(G_p\) has diameter 4 since, vertex \(2 + 2i\) and its associates are at distance 4 from vertex 0.

5 Discussion

In this final section conclusions of this work and future research are going to be presented. In the first subsection, the main result is rewritten using parity-check matrices. Also, 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 addressed. Moreover, other examples of codes presenting greater density and an upper error correction capacity are shown. In the final subsection, the authors aim to exhibit the connections of 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, \(G_p\) has error correction capacity 2 and diameter 3, for any prime \(p \geq 5\) and \(p \equiv \pm 5 \pmod{12}\).

Dirichlet’s theorem on arithmetic progressions asserts that in an arithmetic progression there are infinite primes. As a natural consequence, congruences can be considered as arithmetics progressions, and therefore it can be straightforwardly obtained the following:

\[
\{0 : 1 : 0), (1 : 0 : 0), (1 : 1 : 0)\}. \text{ Thus, } |V_i| = |X_i| - 3, \text{ which implies: } |V_i| \geq p - 2 - 2\sqrt{p}.
\]

As a consequence, those primes \(p\) such that \(|V_i| \geq 4\) give the contradiction looked for. Clearly, if \(p \geq 17\) then,

\[
|V_i| \geq p - 2 - 2\sqrt{p} \geq 17 - 2 - 2\sqrt{17} \geq 6.7.
\]

Finally, the unique prime \(p \equiv 1 \pmod{4}\) such that \(5 < p < 13\) is 13. In this particular case, it can be computed that \(|V_i| \geq 9\) for any \(t\), which concludes the proof. □

This can be verified by realizing that the word \(c\) is associated to vertex \(Mc\) and that \(c\) belongs to the code if and only if it is associated to vertex 0; i.e., the codewords are exactly the words \(c\) such that \(Mc = 0\).

However, the code associated to this matrix belongs to the space \((\mathbb{Z}/p\mathbb{Z})^{n/2}\). In order to obtain the Lee code over \((\mathbb{Z}/p\mathbb{Z})^n\) and a parity-check matrix with integer entries, every \(\beta\) has to be substituted by

\[
\beta \mapsto \begin{pmatrix} \Re(\beta) & -\Im(\beta) \\ \Im(\beta) & \Re(\beta) \end{pmatrix}.
\]

Therefore, the parity-check matrix associated to the graph \(G_p\) is

\[
\begin{pmatrix}
\Re(\beta_1) & -\Im(\beta_1) & \ldots & \Re(\beta_2) & -\Im(\beta_2) \\
\Im(\beta_1) & \Re(\beta_1) & \ldots & \Im(\beta_2) & \Re(\beta_2)
\end{pmatrix}.
\]

Now, let us give some considerations on the quality of the codes constructed. Note that, since the Lee sphere of radius 2 contains \(|B_2| = 2n^2 + 2n + 1\) words, then the graph induced by any 2-quasi-perfect linear code has at least \(2n^2 + 2n + 1\) vertices. The graphs \(G_p\) 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

\[\text{Corollary 23. There are infinite } n \in \mathbb{N} \text{ such that } p = 2n + 1, \ p \geq 7 \text{ prime in } \mathbb{Z}, \ p \equiv \pm 5 \pmod{12}.\]

Then, when applying the previous result it is obtained:

\[\text{Corollary 24. The family of graphs } G_p \text{ contains infinite graphs with error correction capacity 2 and diameter 3.}\]
\( p = 2n - 1 \), 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 which 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 dimension), 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 graphs will be \( H = \{1, 4 + 10i, 8, 7 + 11i\} \). In this case the Cayley graph \( G = Cay(\mathbb{Z}[i]/p\mathbb{Z}[i], H) \) induces a 2-quasi-perfect code. Note that \( G \) has \( p^2 = 169 \) vertices, which is just 17% over \( |B_2^n| = 145 \), the cardinal of the sphere in this dimension.

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

The previous small examples suggest that there exist codes very close to be perfect, although general constructions appear to be difficult to find.

From the result by Post [30] it was obtained that there are not perfect codes with radius greater than the dimension of the space. Previously to that paper, Golomb and Welch [13] had already 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 there are not \( t \)-quasi-perfect codes for \( t \geq t_n \). Hence, this might suggest that radius 2 case is an exceptional one. Nevertheless, a few 3-quasi-perfect codes have been found for small dimensions. Note that in this case the \( n \)-dimensional sphere of radius 3 has cardinal \( |B_3^n| = \frac{1}{2}(1 + 2n)(3 + 2n + 2n^2) \). 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 \( n, p, H \) indicated 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 one.

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

### Table 1: 3-quasi-perfect Lee codes over \( \mathbb{Z}_p^n \)

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

#### 5.2 Related Problems

Other interesting problems from different areas than from Coding Theory could be profited from this study. 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 caring about 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] [33]. In that 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 some infinite degrees \( 2n \) of graphs of diameter 2 and \( \frac{1}{2}(n^2 - 1) = \frac{1}{2}|B_2^n| - \frac{n}{2} - \frac{n}{2} \) vertices. Then,
Vetrík constructs graphs with diameter 3 and \(\frac{9}{2}B_{n}^{2}(2n+3)^{2}(2n-5)\) vertices, which is asymptotically \(B_{n}^{2}\). It is remarkable that these graphs have error correction capacity 1 instead of the hoped 2, and thus they do not induce quasi-perfect codes. Note that a Cayley graph attaining the degree-diameter bound [10] is a Ramanujan graph. Therefore, the proof of this conjecture and the study of Gaussian integers are summarized, for the completeness of the article.

Furthermore, the graphs considered in this paper seemed to be good expanders. Therefore, the authors believe that
\[\lambda_{p} < 1000;\]
the only primes in that range for which Conjecture 25.

Conjecture 25. \(G_{p}\) is a Ramanujan graph for any prime \(p \equiv 3 \pmod{4}\).

The set of the Gaussian integers
\[\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}\]
is the extension of the integers by a symbol \(i\), satisfying \(i^{2} + 1 = 0\). Given an element \(\gamma = a + bi \in \mathbb{Z}[i]\), its conjugate is defined as \(\gamma^{*} = a - bi\). Then, the norm is defined as \(N(\gamma) = |\gamma\gamma^{*}| = a^{2} + b^{2}\). Thus, this norm is a function from \(\mathbb{Z}[i]\) into \(\mathbb{Z}\). Furthermore, the norm makes \(\mathbb{Z}[i]\) an Euclidean domain, since for any \(\alpha, \beta \neq 0 \in \mathbb{Z}[i]\), there exist \(\kappa, \rho \in \mathbb{Z}[i]\) such that \(\alpha = \kappa\beta + \rho\) with \(N(\rho) \leq \frac{1}{2}N(\beta) < N(\beta)\). The norm is multiplicative, this is, \(N(\alpha\beta) = N(\alpha)N(\beta)\). Also, as conjugation is an involution, the norm of a Gaussian integer is equal to the norm of its conjugate, that is, \(N(\gamma^{*}) = N(\gamma) = |\gamma\gamma^{*}| = N(\gamma)\). For a Gaussian integer \(\gamma = a + bi\), let us define its real part \(\Re(\gamma) = a = \frac{1}{\sqrt{2}}\) and its imaginary part \(\Im(\gamma) = b = \frac{1}{\sqrt{2}}\). Both \(\Re\) and \(\Im\) are also functions from \(\mathbb{Z}[i]\) into \(\mathbb{Z}\).

Since the Gaussian integers are an Euclidean domain, they also form a principal ideal domain and a unique factorization domain. The four units of \(\mathbb{Z}[i]\) are \(\{1, i, -1, -i\}\) and the uniqueness of factorization is considered up to commutativity and multiplication by these units. If two Gaussian integers have the same factorization, then they are said to be associates. Now, Gaussian primes fall into two categories:
- \(\alpha = p\) for some \(p \in \mathbb{Z}\) prime over the integers satisfying \(p \equiv 3 \pmod{4}\). Its norm is \(N(\alpha) = p^{2}\).
- \(\alpha = a + bi\) with norm \(N(\alpha) = a^{2} + b^{2} = p\) for some integer prime \(p\). This integer must satisfy \(p = 2\) or \(p \equiv 1 \pmod{4}\).

Given a Gaussian integer \(\alpha \in \mathbb{Z}[i]\), the quotient ring \(\mathbb{Z}[i]/\alpha\mathbb{Z}[i]\) can be considered. This is, if for \(\gamma_{1}, \gamma_{2} \in \mathbb{Z}[i]\), their difference is a multiple of \(\alpha\), then \(\gamma_{1} \equiv \gamma_{2} \pmod{\alpha}\) and \(\gamma_{1}, \gamma_{2}\) are representatives of the same element in \(\mathbb{Z}[i]/\alpha\mathbb{Z}[i]\). The number of elements of the quotient ring \(\mathbb{Z}[i]/\alpha\mathbb{Z}[i]\) is \(N(\alpha)\). When \(\alpha\) is a Gaussian prime, the quotient ring is also a field; otherwise, the divisors of \(\alpha\) become representatives of zero divisor elements in the quotient.

The special case of \(\mathbb{Z}[i]/p\mathbb{Z}[i]\) for some integer prime \(p\) has interesting consequences. The cardinal

Acknowledgments

This work has been supported by the Spanish Science and Technology Commission (CICYT) under contracts TIN2010-21291-C02-02 and AP2010-4900.

A Gaussian Integers

For more details on the ring of Gaussian integers the book by Hardy and Wright [15] is a classical reference. In this Appendix some standard definitions and results on Gaussian integers are summarized, for the completeness of the article.
is always $p^2$. Then, the ring is a field if and only if $p \equiv 3 \pmod{4}$. The Gaussian norm becomes a function $N : \mathbb{Z}[i]/p\mathbb{Z}[i] \to \mathbb{Z}/p\mathbb{Z}$; and $\mathbb{Z}/p\mathbb{Z}$ is always a field. Finally, the norm of an element is 0 if and only if it is a zero divisor.

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. Des. Codes 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, Sept. 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, Jan. 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, oct. 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, Nov. 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, Oct 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, Aug 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. IEEE Transactions on Information Theory, 40(1):207–216, Jan 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. IEEE Transactions on Information Theory, 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, Aug. 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 Širáň. 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 dimensione. Atti Accad. Naz. Lincei, VIII. Ser., 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, Sept. 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, Jul 1994.

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

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