UNIVERSIDAD DE CANTABRIA

Dpto. Matemáticas, Estadística y Computación

TESIS DOCTORAL

Códigos y Grafos sobre Anillos de Enteros Complejos

Presentada por María del Carmen Martínez Fernández.

Dirigida por Ramón Beivide Palacio.

Santander, Enero de 2007.

Agradecimientos

Durante estos años de investigación he tenido la suerte de encontrarme con un montón de gente a la que tengo que agradecerle mucho.

En primer y más importante lugar, a mi director de tesis el Profesor Ramón Beivide por su apoyo, buenos consejos y su fé en este trabajo. Sin ninguna duda, esto no hubiese sido posible si no hubiese estado a mi lado.

Al Profesor Tomás Recio, mi tutor en el Departamento de Matemáticas, Estadística y Computación, por ayudarnos a llegar a buen puerto.

Al Profesor Ernst Gabidulin, del Instituto de Física de Moscú, al que tuve la suerte de conocer en la Universidad de Ulm en el 2004 y con el que hemos estado colaborando ininterrumpidamente desde ese momento. Al Profesor Jacobo Torán, de la Universidad de Ulm por acogerme de una manera tan amigable. A Cruz Izu, de la Universidad de Adelaide, por ser tan buena anfitriona en mi viaje a Australia.

A todo el Grupo de Arquitectura y Tecnología de Computadores, por hacer posible ese ambiente de trabajo y compañerismo que creo será difícil encontrar en otro sitio.

A mis compañeros de despacho, que han sido muchos en este tiempo, con los que he pasado tan buenos momentos, en especial a Pablo Abad, Enrique Vallejo y Miquel Moretó (Universidad Politécnica de Cataluña). A Esteban Stafford, gracias al que ha sido posible llegar a los 30.000 nodos.

A mis padres Carlos y Carmen y mi hermana Ana, que han sufrido los viajes tan lejos, por su apoyo infinito.

A Ricardo, que siempre estuvo ahí en los momentos de estrés y se ha tomado la molestia de entender lo que es un grafo Gaussiano.

Resumen de la Tesis

El objetivo de este trabajo es proponer códigos perfectos para diferentes espacios de señal multidimensionales. Para resolver estos problemas, esta tesis presenta una relación original entre las Teorías de Grafos, Números y Códigos. Entre nuestras principales aportaciones se encuentra la propuesta de métricas adecuadas para constelaciones de señal cuadráticas, hexagonales y tetradimensionales. Estas métricas están basadas en la distancia entre los vértices de un nueva clase de grafos de Cayley definida sobre anillos de enteros. Estos grafos son por tanto, modelos matemáticos de las constelaciones multidimensionales bajo estudio.

La palabras código serán los elementos de ciertos anillos finitos de enteros complejos. Los anillos de enteros considerados en este trabajo son los enteros de Gauss, enteros de Eisenstein-Jacobi y los enteros de Lipschitz. Los anillos cociente bajo estudio se definen mediante una relación de equivalencia determinada por los múltiplos de un entero generador. Las tres estructuras poseen una norma multiplicativa, que determina el cardinal del cociente y el orden del grafo de Cayley considerado. Los vértices del grafo constituyen el alfabeto y la adyacencia de éste está determinada por el conjunto de unidades del anillo. Así, el grado del grafo está determinado por por el cardinal del conjunto de unidades.

El problema de Teoría de Grafos conocido como el cálculo del conjunto perfecto dominante se resuelve en las familias de grafos definidas en esta memoria, esto es, grafos Gaussianos, de Eisenstein-Jacobi y de Lipschitz. En cada caso, se dan condiciones suficientes para la existencia de dicho conjunto. La obtención de estos conjuntos de dominación nos lleva directamente a la construcción de códigos perfectos sobre los alfabetos que estamos considerando.

Además, en esta tesis también se obtinen algunos resultados de isomorfía y embebimiento de grafos. Más concretamente, se establecen las relaciones entre grafos circulantes, grafos toroidales y los grafos que aquí presentamos. En particular, existen órdenes para los que un grafo toro puede ser embebido en un grafo Gaussiano, o de Eisenstein-Jacobi o de Lipschitz. Esto implica directamente que la conocida distancia de Lee es un subcaso de las métricas presentadas en esta investigación.

Como hemos afirmado antes, en esta tesis resolvemos ciertos problemas de Teoría de

Códigos usando grafos de Cayley. A continuación, pretendemos poner en contexto nuestra investigación, introduciendo el trabajo publicado más reseñable relacionado con esta tesis. Nos referiremos a dos tópicos diferentes: Teoría de Códigos y Teoría de Grafos.

El diseño de códigos correctores de errores para espacios de señal bidimensionales ha sido considerado recientemente en la literatura técnica. Ha sido provado que tanto la distancia de Hamming como la de Lee son inapropiadas para tratar con conjuntos de señal de tipo QAM y otras constelaciones relacionadas. Hasta lo que sabemos, el primer autor que modeló ciertas constelaciones de tipo QAM mediante anillos cociente de los enteros de Gauss fue Klaus Huber. En sus artículos, Huber introdujo una nueva distancia para usar en este tipo de constelaciones llamada la *métrica de Mannheim*. La idea para la definición de esta métrica es considerar la métrica de Manhattan (o del taxi) módulo una malla bidimensional. Sin embargo, como veremos más adelante en esta tesis, la métrica de Mannheim no es una distancia porque no verifica la desigualdad triangular. Huber propuso códigos bloque sobre los entero Gaussianos basados en la métrica de Mannheim en [37] y [38]. También, en [39] propuso códigos bloque sobre los enteros de Eisenstein-Jacobi y una métrica de Mannheim modificada para ser aplicada sobre las constelaciones hexagonales.

Después de los papeles de Huber, en los cuales los anillos cociente considerados son módulo un ideal primo, otros autores consideraron diferentes grupos de números complejos para codificar señales QAM [22], [62]. Además, otros trabajos han considerado códigos bloque sobre cuerpos de números cuadráticos [58], [63], [23]. Por otro lado, en [19], se considera una aproximación geométrica del problema. Los autores usan retículas y teselaciones planas para definir códigos que emplean la distancia inducida por la métrica Euclídea sobre ciertos grafos embebidos en el Toro plano. Recientemente, en [59] se ha dado una solución para el diseño de códigos en bloque espacio-tiempo sobre constelaciones de señal complejas. Además, en [46] se han propuesto de manera reciente códigos espacio-tiempo sobre el álgebra de los cuaternios.

Es conocido que la Teoría de Grafos tiene aplicaciones a la Teoría de Códigos. Un ejemplo es el *grafo de Tanner* de un código, que supone una herramienta bastante útil en el estudio de las propiedades del código o para la construcción de códigos más largos partiendo de códigos más pequeños [70]. Otro ejemplo es el que aparece en [12], en el que los autores resuelven algunos problemas sobre grafos toro por medio de la utilización de códigos correctores de errores para la métrica de Lee.

Como hemos afirmado anteriormente, nuestros códigos están basados en grafos de Cayley, tema sobre el que hay una gran cantidad de publicaciones. Estos grafos fueron introducidos por Sir Arthur Cayley como una forma significativa e intuitiva de visualizar grupos. Desde este punto de vista, son una herramienta muy útil para estudiar las propiedades de diferentes estructuras algebraicas, lo que ha generado un amplio estudio de sus propiedades geométricas. También, ha sido probado que los grafos de Cayley son un enfoque convincente para la resolución de aplicaciones específicas como problemas de reorganización y el diseño de redes de interconexión para computadores paralelos [18]. Más aún, muchas familias diferentes de grafos bien conocidos son de Cayley, como por ejemplo los circulantes o los toros.

Existen también muchos artículos sobre grafos circulantes, tanto por su interés teórico como por sus aplicaciones prácticas. En [71] Turner mostró que la clase de grafos conexos, vértice-simétricos con número primo de vértices es idéntica a la de los polígonos estrellados. Este autor definió un polígono estrellado como un grafo en el que los vértices v_i y v_j son adyecentes si y sólo si los vértices v_{i+k} y v_{j+k} son también adyacentes, donde $1 \leq k \leq n-1$ y n es el número de vértices del grafo (los subíndices $i+k$ y $j+k$ considerados módulo n). Este es un paso previo esencial para la definición de los circulantes. Esta clase de grafos fue ampliamente estudiada por Wilkov [73], centrándose en los aspectos de fiabilidad. Sin embargo, parece que fue Elspas en [24] quien introdujo estos grafos como grafos con matriz de adyacencia circulante, esto es, una matriz en la que todas sus filas son rotaciones periódicas de la primera. Estas matrices tienen también otras aplicaciones en el área de la Teoría de la Información, tanto en la Teoría de la Codificación como en la Criptología. En [21] se puede encontrar un estudio extenso sobre las propiedades y aplicaciones de estas matrices y, de acuerdo con este libro, las matrices circulantes aparecen por primera vez en la literatura matemática en un artículo de E. Catalan en 1846.

Además, hay un amplio número de artículos tecnológicos sobre grafos circulantes de grado cuatro o *redes de doble lazo*. En [60] fueron propuestas topologías de doble lazo óptimas o casi óptimas para redes de área local. Más tarde, las propiedades de los grafos circulantes y su minimización fueron estudiados en [11] y [26] por medio de teselaciones planas. Seguidamente, en [5] los autores caracterizan completamente una familia de circulantes de grado cuatro con propiedades de distancia mínimas, esto es, diámetro y distancia media mínimas y las proponen como redes con distancias óptimas para computadores paralelos. Finalmente, hay una gran variedad de artículos relacionados con aspectos teóricos de los grafos circulantes como isomorfismos [57], [1], [45], colorabilidad [36], producto de grafos [28], [66], *etcetera.*

En nuestro caso, los grafos de Cayley de grados cuatro y seis serán construidos sobre anillos Euclídeos de enteros. La existencia de un algoritmo de Euclides será utilizada para resolver problemas sobre estos grafos, como el encontrar conjuntos perfectos dominantes u obtener el camino mínimo entre cualquier par de vértices. El caso de los grafos de grado ocho es un poco diferente dado que la estructura algebraica considerada para su definición, el anillo de enteros de los cuaternios, no es un dominio Euclídeo.

Hasta donde nosotros sabemos, hay sólo un trabajo en el que se definen grafos de Cayley sobre estructuras algebraicas de la Teoría de Números. Este es el caso de ciertos grafos de Ramanujan considerados en [20], en el que se buscan buenos grafos de expansión.

A continuación, pasamos a detallar la organización del la memoria. Para cada Capítulo, resumimos los principales resultados obtenidos y además, referenciamos nuestro material publicado.

El Capítulo 2 está dedicado a la definición y propiedades de los grafos Gaussianos. Primeramente, definimos los grafos Gaussianos en la Sección 2.2 como una subfamilia de grafos de Cayley. Estos grafos se construyen sobre anillos cociente de los enteros de Gauss, usando como conjunto generador las unidades del anillo. Además, damos un método general para dibujarlos en dos dimensiones. Esta representación está basada en el hecho de que el conjunto de vértices tiene cardinal la suma de dos cuadrados. En la Sección 2.3, probamos un par de Teoremas que describen el diámetro y la distancia media de los grafos Gaussianos. Estos resultados han sido obtenidos mediante la descripción completa de la distribución de distancias de los vértices del grafo. Finalmente, en la Sección 2.4 consideramos el problema del cálculo del camino mínimo en los grafos Gaussianos. Para ello, damos un algoritmo simple y compacto para encontrar el camino mínimo para cualquier par de vértices basado simplemente en sumas y comparaciones.

Varios artículos sobre los grafos Gaussianos descritos en el Capítulo 2 se han publicado o han sido enviados para su pulicación. Por ejemplo, en [49] hemos presentado un algoritmo de broadcast óptimo y algoritmos de enrutamiento para ciertos casos particulares de Gaussianos. En [6] fue presentada una descomposición en anillos de ciertos casos Gaussianos que heredan las propiedades de distacia y en [48] fueron estudiadas las topologías cordales isomorfas. En [51] resolvemos el problema del conjunto dominante perfecto en los grafos Gaussianos. En este artículo también consideramos la descripción completa de las propiedades de distancia de los grafos Gaussianos.

En el Capítulo 3 consideramos la construcción de códigos perfectos correctores de errores sobre anillos cociente de los enteros de Gauss. Para este propósito, empleamos una métrica que es la distancia entre los vértices en los grafos Gaussianos. Proponemos esta métrica Gaussiana como la métrica correcta para las aplicaciones de la Teoría de Códigos basados en el anillo de los enteros de Gauss. Más aún, mostraremos que la distancia de Mannheim introducida por Huber no es una métrica en realidad, puesto que no verifica la desigualdad triangular. En la Sección 3.2, consideramos el problema de encontrar conjuntos perfectos dominantes sobre los grafos Gaussianos. La solución a este problema nos ha permitido proponer códigos perfectos sobre constelaciones de tipo QAM, que son consideradas en la Sección 3.3.

Hemos llamado a estos códigos, códigos ideales puesto que constituyen ideales del respectivo anillo cociente. Para estos códigos damos un resultado de unicidad en la subsección 3.3.1. En la Sección 3.4, definimos el concepto de grafo cociente de un grafo Gaussiano en el caso en que exista un código perfecto. Estos grafos cocientes son una excelente herramienta para computar las distancias máxima y media de tales códigos. Finalmente, obtenemos como consecuencia de esta investigación que los conocidos códigos perfectos de Golomb para la distancia de Lee son un subcaso de nuestros códigos Gaussianos, como se verá en la Sección 3.5.

Hemos publicado artículos sobre códigos basados en enteros de Gauss descritos en el Capítulo 3 en actas de congresos notables de Teoría de la Información y otros se encuentran en proceso de evaluación para revistas. En particular, en [50] y [52] consideramos códigos perfectos sobre anillos cociente de los enteros de Gauss. La métrica aplicada a estos códigos es la distancia inducida por un grafo Gaussiano y circulante. También, la distribución de pesos de estos circulantes ha sido presentada en [27]. Además, en [53] presentamos códigos perfectos sobre cualquier anillo cociente de enteros de Gauss. En este artículo hemos mostrado también que los códigos perfectos de Golomb introducidos en [30] son un caso particular de códigos Gaussianos perfectos.

El Capítulo 4 está dedicado a la extensión de las técnicas de los Capítulos anteriores al caso de las constelaciones hexagonales. En este caso, las constelaciones y los vértices del grafo son modelados mediante cocientes del anillo de los enteros de Eisenstein-Jacobi. En la Sección 4.2 definimos los grafos de Eisenstein-Jacobi. Estos grafos son también grafos de Cayley sobre anillos cociente, pero en este caso de los enteros de Eisenstein-Jacobi. Nos centraremos entonces en el caso en el que estos grafos son circulantes de grado seis y los compararemos con otras familias de circulantes que han sido estudiadas anteriormente. Posteriormente, en la Sección 4.3, nuevos resultados inspirados en los que obtuvimos para los grafos Gaussianos nos permitirán determinar conjuntos perfectos dominantes en los grafos de Eisenstein-Jacobi. Se podrán definir por tanto códigos perfectos sobre conjuntos de señal hexagonales usando como métrica del código la inducida por estos grafos.

En [50] han sido introducidos códigos perfectos 1-correctores sobre constelaciones hexagonales modeladas mediante anillos cociente de los enteros de Eisenstein-Jacobi. Recientemente, en [54] se ha considerado un método para encontrar ciertos conjuntos perfectos t-dominantes sobre grafos circulantes de grado seis. También, un método extendido para obtener códigos perfectos t-correctores sobre anillos cociente de los enteros de Eisenstein-Jacobi han sido presentados en [55].

En el Capítulo 5 se va a considerar una aproximación preliminar al caso de grado ocho y sus códigos. En este caso, los grafos se construirán sobre ciertos subconjuntos de los enteros cuaternios. Se obtendrán conjuntos perfectos 1-dominantes y en ciertos casos, estos códigos serán comparados con códigos perfectos de Lee, lo que ha sido considerado en [56].

Finalmente, el Capítulo 6 concluye esta tesis con una breve descripción de nuestras contribuciones y una introducción a algunos problemas abiertos.

UNIVERSITY OF CANTABRIA

Dept. Mathematics, Statistics and Computation

DOCTORAL THESIS

Codes and Graphs over Complex Integer Rings

Presented by María del Carmen Martínez Fernández.

Advised by Ramón Beivide Palacio.

Santander, January 2007.

"If the Theory of Numbers could be employed for any practical and obviously honorable purpose, if it could be turned directly to furtherance of human happiness or relief of human suffering, as physiology and even chemistry can, then surely neither Gauss nor any other mathematician would have been so foolish as to decry or regret such applications."

G. H. Hardy, "A Mathematician's Apology".

Abstract

The aim of this work is to propose perfect codes for different multidimensional signal spaces. To solve these problems, this thesis presents an original relationship among the fields of Graph Theory, Number Theory and Coding Theory. One of our main findings is the proposal of a suitable metric over quadratic, hexagonal and four-dimensional constellations of signal points. This metric is the distance among vertices of a new class of Cayley graphs defined over integer rings. Hence, such graphs represent mathematical models of the multidimensional constellations under study.

Our alphabets will be the elements of some finite complex integer rings. The integer rings considered in this work are the Gaussian integers, the Eisenstein-Jacobi integers and the Lipschitz integers. The quotient rings under study are made by an equivalence relation determined by the multiples of an integer generator. The three structures have a multiplicative norm which determines the cardinal number of the quotients and the order of the considered Cayley graph. Graph vertices represent the alphabet and their adjacency is determined by the set of units of the considered ring. The graph degree is determined by the cardinality of this set of units.

A problem in Graph Theory known as the perfect dominating set calculation is solved over the families of graphs defined in this memory, namely Gaussian, Eisenstein-Jacobi and Lipschitz graphs. A sufficient condition for obtaining such a set is given for each case. The obtention of these sets of domination directly yields to the construction of perfect codes for the alphabets under consideration. The provided solutions have been obtained by exploiting the Euclidean divisibility over the considered rings.

In addition, some isomorphism and graph embedding results are going to be obtained in this Thesis. Specially, the relations between circulant, toroidal and the graphs presented in this work are stated. In particular, there always exist orders for which a torus graph can be embedded in Gaussian, Eisenstein-Jacobi and Lipschitz graphs. This implies that the well-known Lee distance is a subcase of the metrics presented in this research.

Contents

List of Figures

Chapter 1

Introduction

This first Chapter introduces the material considered in the whole memory. In order to provide a self-contained context, the Chapter starts introducing a minimal background in Coding Theory, Graph Theory and Elementary Number Theory in the next three Sections followed by a Section describing the most relevant related work and finishing with a Section devoted to describe the thesis structure and its results.

1.1 Background in Coding Theory

The origin of Information Theory comes from a famous Theorem of Claude Shannon which guarantees the existence of codes that can transmit information at rates close to the channel capacity with an arbitrarily small error probability [68].

Although some binary codes were considered as examples by Shannon in 1948 and generalized by Golay in 1949, a paper from Richard Hamming in 1950 is considered the first serious contribution about error-correcting codes [33]. In the 1940s, Hamming worked at the Bell Telephone Laboratories with one of the best computers of that time, the Bell Model V, which could detect errors but not correct them. Therefore, Hamming decided to look for a method to correct those errors. In his seminal paper he describes 1-error correcting codes and 2-error detecting codes and provides all the perfect single-error-correcting binary group codes.

A *binary code* of length n is a subset of all possible strings or vectors of n symbols chosen from the alphabet $\{0, 1\}$. The *Hamming distance* between two vectors is defined as the number of coordinates in which such vectors differ. Thus, the *Hamming weight* of a vector is the number of its non-zero coordinates. The Hamming distance can be geometrically interpreted as the distance among vertices in a binary n-cube graph. In such a graph, adjacent vertices are labeled by binary vectors that differ in just one coordinate. A code is said to have minimum distance d if every two members of the code, or *codewords*, differ at least in d coordinates. If the number of the codewords is M, then we say that it is an (n, M, d)-code. A good code is expected to have n small for speed, M large for efficiency and d large for reliability.

Many new types of codes were introduced after the appearance of Hamming's seminal paper. Golay generalized Hamming's construction and proposed single-correcting non-binary codes for alphabets of cardinal p, being p prime. He also introduced two remarkable binary codes for correcting multiple errors, the well-known *Golay codes*. Later, double-error-correcting codes were discovered by Bose and Chaudhuri in 1960 and by Hocquenghem in 1959, the so called *BCH codes*. Then, the generalization for t-error correcting codes followed immediately for all t. The relatively high complexity of the simplest double-error correcting code contrasts with the simplicity of the Hamming codes. Not in vain, there is almost a decade of research between both discoveries.

In most applications, the encoded sequence of 0s and 1s is given to a modulator which converts these symbols into certain continuous time functions. Three basic schemes are commonly employed: amplitude, frequency and phase modulation. The resulting time functions are used to control the signal characteristics. For example, the amplitude of the transmitted signal might be the voltage on a wire or the instantaneous power emitted by a radio transmitter. There are many variations, combinations and enhancements of these three basic modulation schemes. Each one seeks to deal with the requirements of particular applications and the shortcomings of the basic transmission techniques. They offer trade-offs between spectral efficiency, robustness and implementation cost.

Depending on the selected modulation technique different metrics can be used for error-correcting codes. Hamming distance can be appropriate for amplitude and frequency modulation. The Lee distance can be more convenient for phase modulation. The Lee metric [44], [72], was developed as an alternative to the Hamming metric for transmission of non-binary signals (usually taken from $GF(p)$, the Galois field of order p, being p prime) over noisy channels. Perhaps, the most important and well-known codes for the Lee metric are the negacyclic codes introduced by Berlekamp [8], for which there is an efficient decoding procedure. When using one-dimensional signal spaces, the Lee metric can be seen as the distance among vertices in a ring graph. Similarly, when using two-dimensional signal spaces, the Lee metric can be seen as the distance among vertices in a torus graph, as considered in [8] and [12].

One of the most popular non-basic modulation schemes combining phase and amplitude is Quadrature Amplitude Modulation (QAM). Using this technique, two independent signal components or coordinates can be transmitted over the same carrier leading to a two-dimensional signal space. The different combinations of such coordinates constitute the signal points which are arranged on a lattice. Technically speaking, this lattice receives the name of *constellation*. In this thesis, we model this kind of constellations by means of Cayley graphs whose vertices are labeled by the elements of complex integer rings. We will adopt the distance among vertices of the Cayley graph as the code metric.

1.2 Background in Graph Theory

A *graph* is a mathematical structure that consists of two sets. The first one is a set of points called *vertices* and the second one is a set of lines or *edges*, which in our case will be assumed undirected, joining some pairs of vertices.

The famous *Königsberg Bridge Problem* is widely considered as the birth of Graph Theory as well as Topology. This problem was settled by Euler in 1736 as follows. There were two islands linked to each other and to the banks of the Pregel River by seven bridges. The problem was to begin at any of the four land areas, walk across each bridge exactly once and return to the starting point. In proving that the problem is unsolvable, Euler replaced each land area by a point and each bridge by a line joining the corresponding points, thereby producing a graph.

Later, Kirchhoff began to develop the theory of trees in 1847 in order to solve a problem associated to circuits of an electrical network. Cayley in 1857 completed the study of tree graphs to enumerate chemical molecules by considering the changes of variables in the differential calculus. Other interesting problems that involve graphs are the *Traveling Salesman Problem* (Hamilton, 1859) or the famous *Four Color Conjecture*, which was proved by Appel and Haken in 1976. A simpler and more systematic proof was produced by Robertson, Sanders, Seymour and Thomas in 1994 [64].

Basic concepts and definitions on graphs that we will later need in this thesis are going to be introduced now. Most of them have been obtained from the well-known book of Harary [34]. We also introduce Cayley and circulant graphs, which will be broadly considered in this thesis.

A *graph* $G = (V, E)$ consists of a finite nonempty set V of points called *vertices* together with a set E of ordered pairs of distinct points of V. Each pair $e = (u, v)$ of points in V is an *edge* of G and e is said to *join* u and v. We also say that u and v are adjacent vertices. Furthermore, vertex u and edge e are *incident* with each other, as are v and e. The graph G is undirected if for every pair of vertices such that $(u, v) \in E$ implies that $(v, u) \in E$. If the cardinal number of V is n we say that G has *order* n.

A graph G is *labeled* when the n vertices are distinguished from one another by names such as $v_1, v_2, \ldots, v_n$. In this memory we will deal with different labelings of well-known graphs such as degree four and six circulant graphs, square tori and others. These graphs are typically labeled by means of integers, but in our case Gaussian integers (in case of degree four), Eisenstein-Jacobi integers (in case of degree six) and Lipschitz integers (in case of degree eight) will be used for the labeling.

The *degree* of a vertex v_i in a graph G is the number of edges incident with v_i. If all the vertices have the same degree d, G is called *regular* of degree d.

The *adjacency matrix* $A = [a_{ij}]$ of a labeled graph G with n vertices is the $n \times n$ matrix in which $a_{ij} = 1$ if v_i is adjacent to v_j and $a_{ij} = 0$ otherwise. Thus, there is a one-to-one mapping between labeled graphs of order n and $n \times n$ symmetric binary matrices with zero diagonal.

Two graphs $G = (V, E)$ and $H = (V', E')$ are *isomorphic* if there exists a bijection between their sets of vertices $\Phi : V \longrightarrow V'$ which preserves adjacency, that is, if two vertices $v_1, v_2 \in V$ are adjacent in G, then $\Phi(v_1), \Phi(v_2) \in V'$ must be adjacent in H. We denote that graphs G and H are isomorphic by $G \cong H$.

One of the most elementary properties that any graph can enjoy is that of being connected. A *walk* of a graph G is an alternating sequence of vertices and edges v_0, e_1, v_1, $\ldots$, v_{n-1}, e_n, v_n beginning and ending with vertices in which each edge is incident with the two vertices immediately preceding and following it. This walk joins v_0 and v_n and may also be denoted as $v_0 v_1 \ldots v_n$. It is called a *path* if all the vertices are different and a path is said to be a *cycle* if $v_0 = v_n$. Then, a graph is *connected* if every pair of vertices is joined by a path.

The length of a walk $v_0 v_1 \ldots v_n$ is n, the number of occurrences of edges in it. The *girth* of a graph G, denoted as $g(G)$, is the length of the shortest cycle (if any) in G; conversely, the *circumference*, $c(G)$, is the length of the longest cycle.

The *distance* $D(u, v)$ between two vertices u and v in G is the length of a shortest path joining them if any; otherwise $D(u, v) = \infty$. In a connected graph the distance is a metric ; that is, for all the vertices u, v and w we have that:

i) $D(u, v) \geq 0$, with $D(u, v) = 0$ if and only if $u = v$.

ii) $D(u, v) = D(v, u)$.

iii) $D(u, v) + D(v, w) \geq D(u, v)$.

The *diameter* k of G is the length of any longest shortest path among all pairs of vertices of the graph.

Another interesting graph property is symmetry. Two vertices u and v are *similar* if for some automorphism α of G, $\alpha(u) = v$. Also, two edges $(u_1, v_1), (u_2, v_2)$ are *similar* if there is an automorphism α of G such that $\alpha(\{u_1, v_1\}) = \{u_2, v_2\}$. A graph is *vertex-symmetric* if every pair of vertices are similar; it is *edge-symmetric* if every pair of edges are similar; and it is *symmetric* if it is both vertex-symmetric and edge-symmetric.

Since the graphs we are dealing with are vertex-symmetric, we can study its distance properties starting from an arbitrary vertex. We select vertex v_0. The *average distance* $\overline{k}$ of a vertex-symmetric graph can be calculated as

$$\overline{k} := \frac{\sum_{u \in V, u \neq v_0} D(u, v_0)}{\#V - 1},$$

where $\#V$ denotes the cardinal number of the set of vertices V, that is, the order of the graph.

As our research is mainly focussed on Cayley and circulant graphs, we give their definitions next.

Definition 1 *Given a group $(\mathcal{G}, \cdot)$ (finite or infinite) and S a nonempty finite subset of $\mathcal{G}$, the* Cayley graph *$Cay(\mathcal{G}, S)$ is the graph with vertex set $V = \mathcal{G}$ and edge set*

$$E = \{(x, y) \mid x, y \in \mathcal{G}, \exists s \in S \mid y = x \cdot s\},$$

where $x \cdot s$ denotes the group operation.

Note that the Cayley graph $Cay(\mathcal{G}, S)$ is connected if and only if S generates $\mathcal{G}$.

Definition 2 *A* circulant graph *with N vertices and jumps $\{j_1, j_2, \ldots, j_m\}$ is an undirected graph in which each vertex n, $0 \leq n \leq N-1$, is adjacent to all the vertices $n \pm j_i \pmod N$, with $1 \leq i \leq m$. We denote this graph as $C_N(j_1, j_2, \ldots, j_m)$.*

Therefore, circulant graphs are Cayley graphs defined over cyclic groups. Circulants, $C_N(j_1, j_2, \ldots, j_m)$, are regular of degree $2m$ and symmetric. It was proved in [10] that a circulant graph $C_N(j_1, j_2, \ldots, j_m)$ is connected if and only if $\gcd(j_1, j_2, \ldots, j_m, N) = 1$.

It is easy to establish an upper bound for the order of circulants as a function of their degree and diameter. For any degree, $d = 2m$, and a given diameter, k, the maximum order of $C_N(j_1, j_2, \ldots, j_m)$ may not be higher than the cardinal of the set:

$$V_d^k = \{(x_1, x_2, \ldots, x_d) \in \mathbb{Z}^d \mid |x_1| + |x_2| + \ldots + |x_d| \leq k\},$$

which we denote as $\#V_d^k$. We can compute the maximum order of a circulant of degree $d = 2m$, with $m > 1$ and diameter k, with $k \geq 1$, using a recursive expression as:

$$\begin{cases} \#V_d^k = \#V_{d-2}^k + 2\sum_{i=0}^{k-1} \#V_{d-2}^i, \\ \#V_2^k = 2k+1. \end{cases}$$

If for a given degree and diameter a circulant with such a number of vertices exist, we say that it is *dense.* Note that the degree-two circulant is the cyclic graph or *ring.* It is straightforward to see that the dense ring of diameter k has order $2k+1 = k+k+1$. By using the previous expression, the dense degree four circulant would have $2k^2+2k+1 = k^2+(k+1)^2$ vertices. As we will see, dense degree four circulants exist but there are not dense graphs for higher degrees, except the trivial cases for diameter 1. This result was conjectured by Golomb in [30] and, as far as we know, it has not been proved yet.

Later, in Chapter 3, we will look for perfect t-dominating sets over several families of graphs. This problem has been previously considered with other graphs [47], [42]. The concepts of domination and perfect dominating set are defined as follows:

Definition 3 *A vertex u of a graph G is said to* t-dominate *another vertex v if $D(u,v) \leq t$, where D denotes the graph distance. Then, a vertex subset $S \subset V$ is called a* perfect t-dominating set *if every vertex of G is t-dominated by a unique vertex in S.*

1.3 Background in Elementary Number Theory

Now, we introduce some background in Number Theory that will be used later in this thesis. Most of the classical definitions and results about quadratic fields and integer rings in Section 1.3.1 have been obtained from the famous book by Hardy, "An Introduction to the Theory of Numbers", [35]. We concentrate on integer rings of those fields that are Euclidean domains. In particular, we focus on Gaussian integers and Eisenstein-Jacobi integers, which will be used in next Chapters to define Cayley graphs over their quotient rings. Finally, for the general stuff about quaternions in Section 1.3.2, we have used the two excellent books of Conway and Smith [17] and Davidoff, Sarnak and Valette [20] about the geometry of quaternions and Ramanujan graphs, respectively.

1.3.1 The General Quadratic Field $\mathbb{Q}(\sqrt{m})$

Let $\mathbb{Q}$ be the field of the rational numbers. To avoid ambiguity, we will call the integers of $\mathbb{Q}$ as *rational integers* and denote the set of them as $\mathbb{Z}$. Let $\mathbb{Q}(\sqrt{m})$ be a quadratic extension of $\mathbb{Q}$, being m a square-free rational integer. We define the *integers* of $\mathbb{Q}(\sqrt{m})$ as those algebraic integers which belong to $\mathbb{Q}(\sqrt{m})$. Let $\xi = \dfrac{a+b\sqrt{m}}{c}$ be an integer, where $c > 0$ and $\gcd(a,b,c) = 1$. If $b \neq 0$, ξ is quadratic and there are two possible cases as next Theorem shows:

Theorem 4 *The integers of* $\mathbb{Q}(\sqrt{m})$ *are the numbers of the form:*

- $a + b\sqrt{m}$ *if* $m \equiv 2$ *or* $m \equiv 3 \pmod 4$,
- $a + b\tau = a + b\frac{-1+\sqrt{m}}{2}$ *if* $m \equiv 1 \pmod 4$,

with a *and* b *being in either case rational integers.*

Example 1 $\mathbb{Q}(\sqrt{-1})$ *is an example of the first case and* $\mathbb{Q}(\sqrt{-3})$ *is an example of the second one. Both cases will be considered in next Sections.*

The integers of $\mathbb{Q}(\sqrt{m})$, or $\mathbb{Z}(\sqrt{m})$, form an integral domain. Also, if $\mathbb{Q}(\sqrt{m})$ can be expressed as $a + b\phi$, we say that $[1, \phi]$ is a *basis* of the integers of $\mathbb{Q}(\sqrt{m})$. Thus, $[1, i]$ is a basis of the integers of $\mathbb{Q}(i)$, the well-known *Gaussian integers*. Also, $[1, \rho]$ is a basis of the integers of $\mathbb{Q}(\sqrt{-3})$, or the *Eisenstein-Jacobi integers*, where $\rho = \dfrac{-1 + \sqrt{-3}}{2}$.

1.3.1.1 Norm, Units and Primes

The concepts of *divisibility*, *divisor*, *unit*, *prime* and *associate* in $\mathbb{Z}(\sqrt{m})$ can be defined as usual. Also, given an integer $\xi = r + s\sqrt{m}$, we call $\overline{\xi} = r - s\sqrt{m}$ the *conjugate* of ξ.

The *norm* $\mathcal{N}(\xi)$ of ξ is defined by

$$\mathcal{N}(\xi) = \xi\overline{\xi} = (r + s\sqrt{m})(r - s\sqrt{m}) = r^2 - ms^2.$$

Therefore,

i) If $m \equiv 2$ or $3 \pmod 4$ and $\xi = a + b\sqrt{m}$ then $\mathcal{N}(\xi) = a^2 - mb^2$.

ii) If $m \equiv 1 \pmod 4$ and $\xi = a + b\tau$ then $\mathcal{N}(\xi) = (a - \frac{1}{2}b)^2 - \frac{1}{4}mb^2$.

Norms are positive in complex fields, but not necessarily in real fields. In both cases, the norm is a multiplicative mapping, that is, $\mathcal{N}(\xi\eta) = \mathcal{N}(\xi)\mathcal{N}(\eta)$.

Theorem 5 *The norm of a unit is* ± 1 *and every number whose norm is* ± 1 *is a unit.*

In real quadratic number fields, the units form an infinite cyclic group. In fact, the problem of determining the units of any real quadratic number field is related to the Pell's equations, namely $x^2 - my^2 = \pm 1$, for some positive and square-free integer m [16]. Let us consider the next example to illustrate this fact.

Example 2 *Let us consider as an example $\mathbb{Q}(\sqrt{2})$. The element $1+\sqrt{2}$ has norm equal to -1, so it is a unit. Moreover, we have the following equation:*

$$u_n + v_n\sqrt{2} = (1+\sqrt{2})^n \tag{1.1}$$

for which we obtain the recursive formula:

$$\begin{cases} u_{n+1} &= u_n + 2v_n \\ v_{n+1} &= u_n + v_n \end{cases} \qquad (u_1 = v_1 = 1).$$

Taking norms in Equation 1.1 we obtain that

$$u_n^2 - 2v_n^2 = (-1)^n,$$

which implies that the previous recursive formula gives us a collection of units of $\mathbb{Q}(\sqrt{2})$.

However, in the complex case, the units form a finite set, as the next Theorem states.

Theorem 6 *Let m be a square-free negative integer. Then,*

- *If $m = -1$, the units of the Gaussian integers are $\{\pm 1, \pm i\}$.*
- *If $m = -3$, the units of the Eisenstein-Jacobi integers are $\{\pm 1, \pm\rho, \pm\rho^2\}$.*
- *If $m = -2$ or $m < -3$, the units are $\{\pm 1\}$.*

An integer whose norm is a rational prime, is prime. Moreover, an integer, neither zero nor a unit, can be expressed as a product of primes. The question of the uniqueness of such a expression will be considered in the next subsection.

In particular, for the Gaussian integers and the Eisenstein-Jacobi integers we have the following characterization of primes:

Lemma 7 *Let $a+bi \in \mathbb{Z}[i]$. Then, $a+bi$ is prime if and only if one of the following mutually exclusive cases occur:*

- *$a, b \neq 0$ and $a^2 + b^2$ rational prime.*
- *$a = 0$ and b rational prime with $b \equiv 3 \pmod 4$.*
- *$b = 0$ and a rational prime with $a \equiv 3 \pmod 4$.*

Lemma 8 *Let $a+b\rho \in \mathbb{Z}[\rho]$. Then, $a+b\rho$ is prime if and only if one of the following mutually exclusive cases occur:*

- $a + b\rho = 1 - \rho$.
- $b = 0$ *and* a *a rational prime with* $a \equiv 2 \pmod 3$.
- $a = 0$ *and* b *a rational prime with* $b \equiv 2 \pmod 3$.
- $a, b \neq 0$ *and* $a + b\rho$ *such that* $\mathcal{N}(a + b\rho) = a^2 + b^2 - ab$ *a rational prime with* $a^2 + b^2 - ab \equiv 1 \pmod 3$.

Since we are interested on algebraic structures with a finite number of units, from here onwards we focus on Complex Fields. Moreover, since the Gaussian integers and the Eisenstein-Jacobi integers are the only ones with more than two units, we just consider these two number fields for our graph definitions. The number of units of the ring will determine the degree of the Cayley graph considered. In particular, the Cayley graphs defined over these quadratic number fields will have degrees four and six, respectively.

1.3.1.2 Complex Euclidean Fields

In order to solve certain problems over the graphs introduced in this work we will deal with the Euclidean division algorithm. Hence, we consider next some definitions and properties of complex Euclidean fields.

A complex quadratic number field is called a Unique Factorization Domain (UFD) if the Fundamental Theorem of the Arithmetic is true. Such fields are called *simple* and their arithmetic follows the lines of rational arithmetic. In the "Elements" by Euclides (300 a.C.) there were some basic theorems about rational integer divisibility and primes. Gauss formally proved the *Fundamental Theorem of the Arithmetic*, which appears in "Disquisitiones Arithmeticae" around 1800. A particular expression of this Theorem for rational integers can be found in [35] as:

Theorem 9 *The standard form of a rational integer n is unique. Apart from rearrangement of factors, n can be expressed as a product of primes in one way.*

Not all complex quadratic number fields are UFDs. The Fundamental Theorem is true, for example, in $\mathbb{Q}(i)$ and $\mathbb{Q}(\rho)$, but it is not true in every $\mathbb{Q}(\sqrt{m})$ as next example shows.

Example 3 *Since* $-5 \equiv 3 \pmod 4$, *the integers of* $\mathbb{Q}(\sqrt{-5})$ *or* Kummer integers *are* $a + b\sqrt{-5}$, *where* a *and* b *integers. It is easy to check that the four numbers*

$$2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$$

are primes. But

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

and therefore, 6 has two distinct decompositions into primes.

The well-know concept of *Euclidean Domain* is defined, in general, as follows:

Definition 10 *Let $\mathbb{Z}^+$ be the set of nonnegative integers and R a commutative ring. R is an* Euclidean ring *if there is a function $\mathcal{N} : R - \{0\} \longrightarrow \mathbb{Z}^+$ such that:*

- *if $a, b \in R$ and $ab \neq 0$, then $\mathcal{N}(a) \leq \mathcal{N}(ab)$;*
- *if $a, b \in R$ and $b \neq 0$, then there exists $q, r \in R$ such that $a = qb + r$ with $r = 0$, or $r \neq 0$ and $\mathcal{N}(r) < \mathcal{N}(b)$.*

Also, an Euclidean ring which is an integral domain is called an Euclidean domain*.*

As in the case of UFDs, not all complex quadratic number fields are Euclidean. The problem of determining all simple quadratic fields was solved by Heegner (1952) and reestablished independently by Baker and Stark (1967) in the complex case, [16]. First approaches to the proof for determining all simple quadratic fields were considered using the following result:

Theorem 11 *The Fundamental Theorem is true in any Euclidean quadratic field.*

Finally, the next two Theorems completely characterize those quadratic number fields being Euclidean or unique factorization domains.

Theorem 12 *There are just five complex Euclidean quadratic fields, that is, the fields with discriminants*

$$m = -1, -2, -3, -7, -11.$$

Theorem 13 *There are only nine complex simple quadratic fields, namely those with discriminants*

$$m = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

1.3.2 The Algebra of Quaternions

In this Section we introduce the algebra of *quaternions* and the *Lipschitz integers*. The results and definitions in this subsection have been taken from the books of Davidoff *et al* [20] and Conway *et al* [17].

Hamilton invented the quaternions when he was looking for a three-dimensional normed division algebra. The problem was that there exists no such algebra and what he really needed was a four-dimensional algebra. It is well-known the story of how, on the 16th of October 1843 while we was walking with his wife along the Royal Canal to a meeting of the Royal Irish Academy in Dublin, he discovered the fundamental equations between i, j, k, and carved them into the stone of the Brougham Bridge:

$$i^2 = j^2 = k^2 = ijk = -1.$$

Quaternions are far from being commutative and therefore we will talk of the "division with small remainder" property in analogy with the Euclidean remainder for Euclidean domains (Definition 10). That is, we have the "division with small remainder" if one can divide any integer α by any non-zero β and obtain an integer quotient q and a remainder r with norm strictly smaller than the norm of the divisor β. The integer quaternions loose this property of "division with small remainder" which was later solved with the definition of the *Hurwitz integers.* However, for our application of defining Cayley graphs of degree eight it is enough to consider the Lipschitz integers.

Next, we define quaternions and Lipschitz integers and give a partial Euclidean algorithm based on previous definitions just for odd quaternions, that is, integer quaternions with odd norm and right-hand division.

Let R be a commutative ring with unit. Then, quaternions are defined as:

Definition 14 *The* Hamilton Quaternion Algebra *over R denoted by $\mathbb{H}(R)$ is the associative unital algebra given by the following representation:*

i) *$\mathbb{H}(R)$ is the free R-module over the symbols $1, i, j, k$; that is*

$$\mathbb{H}(R) = \{a_0 + a_1 i + a_2 j + a_3 k \mid a_0, a_1, a_2, a_3 \in R\}.$$

ii) 1 is the multiplicative unit.

iii) $i^2 = j^2 = k^2 = -1$.

iv) $ij = -ji = k$; $jk = -kj = i$; $ki = -ik = j$.

If $q = a_0 + a_1 i + a_2 j + a_3 k$ is a quaternion, its *conjugate* quaternion is $\overline{q} = a_0 - a_1 i - a_2 j - a_3 k$. The *norm* of q is $\mathcal{N}(q) = q\overline{q} = \overline{q}q = a_0^2 + a_1^2 + a_2^2 + a_3^2$, which is multiplicative, that is, $\mathcal{N}(q_1 q_2) = \mathcal{N}(q_1)\mathcal{N}(q_2)$. Note that, as a consequence, the product of two sums of four squares is itself a sum of four squares.

Now, we restrict our attention to the ring of the integers of $\mathbb{H}(R)$ and explore its arithmetic properties. From here onwards, we denote by

$$\mathbb{H}(\mathbb{Z}) = \{a_0 + a_1 i + a_2 j + a_3 k \mid a_0, a_1, a_2, a_3 \in \mathbb{Z}\},$$

the set of the integer quaternions or *Lipschitz integers*. Obviously, the conjugate of any integer quaternion is another integer and its norm is a rational integer. The next Lemma characterizes the units of $\mathbb{H}(\mathbb{Z})$ which will determine the degree of the Cayley graphs constructed over them.

Lemma 15 *For $\alpha \in \mathbb{H}(\mathbb{Z})$ the following properties are equivalent:*

- *α is a unit in $\mathbb{H}(\mathbb{Z})$.*
- *$\mathcal{N}(\alpha) = 1$.*
- *$\alpha \in \{\pm 1, \pm i, \pm j, \pm k\}$.*

There is a factorization into primes for any integer quaternion, though in $\mathbb{H}(\mathbb{Z})$ this factorization is no longer unique. For example,

$$13 = (1 + 2i + 2j + 2k)(1 - 2i - 2j - 2k) = (3 + 2i)(3 - 2i),$$

are two different factorizations of 13 into prime quaternions. However, as a non-commutative ring, $\mathbb{H}(\mathbb{Z})$ has a modified Euclidean algorithm and the corresponding right-hand and left-hand divisors that are unique up to associates.

Definition 16 *Let $\alpha \in \mathbb{H}(\mathbb{Z})$. Then:*

- *α is* odd *(respectively* even*) if $\mathcal{N}(\alpha)$ is odd (respectively even).*
- *α is* prime *if it is not a unit and whenever $\alpha = \beta\gamma$ in $\mathbb{H}(\mathbb{Z})$ then β or γ is a unit.*
- *α and $\alpha' \in \mathbb{H}(\mathbb{Z})$ are* associate *if there exist unit quaternions $\varepsilon, \varepsilon' \in \mathbb{H}(\mathbb{Z})$ such that $\alpha' = \varepsilon\alpha\varepsilon'$.*
- *$\delta \in \mathbb{H}(\mathbb{Z})$ is a* right-hand divisor *of α if there is $\gamma \in \mathbb{H}(\mathbb{Z})$ such that $\alpha = \gamma\delta$.*

In particular, it can be obtained that:

Lemma 17 *For any $\alpha \in \mathbb{H}(\mathbb{Z})$, α is prime in $\mathbb{H}(\mathbb{Z})$ if and only if $\mathcal{N}(\alpha)$ is a prime in $\mathbb{Z}$.*

Let α and $\beta \neq 0$ be two Lipschitz integers, let $q = \alpha\beta^{-1} = a + bi + cj + dk$ and let A, B, C, D be the nearest integers to a, b, c, d. If we define $Q = A + Bi + Cj + Dk$ and $r = \alpha - Q\beta$, then we find that:

$$\mathcal{N}(r\beta^{-1}) = (a - A)^2 + (b - B)^2 + (c - C)^2 + (d - D)^2 \leq 4\Big(\frac{1}{2}\Big)^2 = 1,$$

showing only that $\mathcal{N}(r) \leq \mathcal{N}(\beta)$. The fact that the inequality is not strict is what forces the loss of the "division with small remainder" property. In fact, $\mathcal{N}(r) = \mathcal{N}(\beta)$ can be only true when:

$$|a - A| = |b - B| = |c - C| = |d - D| = \frac{1}{2},$$

that is, when a, b, c, d are all in

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{n}{2^m} \mid n \in \mathbb{Z}, m \in \mathbb{N}\right\}.$$

This is what motivates the definition of *Hurwitz integers*, that is the set $\mathbb{H}\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)$. Therefore, Hurwitz integers have the "division with small remainder" property. Then, despite the fact that there is no Euclidean algorithm in $\mathbb{H}(\mathbb{Z})$ as in $\mathbb{Z}$, we can consider a partial Euclidean algorithm, which is described in Algorithm 1, just for odd Lipschitz integers and right-hand division based on the next result:

Lemma 18 *Let $\alpha, \beta \in \mathbb{H}(\mathbb{Z})$ with β odd. There exists $\gamma, \delta \in \mathbb{H}(\mathbb{Z})$ such that*

$$\alpha = \gamma\beta + \delta \text{ with } \mathcal{N}(\delta) < \mathcal{N}(\beta).$$

```
Data: $\alpha$; $\beta$ odd divisor;
Result: $q$ quotient; $r$ remainder
begin
    STEP 1. Compute $m := \beta\overline{\beta}$;
    STEP 2. Compute $\sigma := \alpha\overline{\beta} = s_0 + s_1 i + s_2 j + s_3 k$;
    STEP 3. Find $q \in \mathbb{H}(\mathbb{Z}) \mid \mathcal{N}(\sigma - qm) < m^2$;
    STEP 4. Compute $r = \alpha - q\beta$;
end
```

Algorithm 1: Euclidean Division Algorithm for Lipschitz Integers.

Step 3 in Algorithm 1 is performed as follows. We define $q = r_0 + r_1 i + r_2 j + r_3 k$ where

$$mr_i - \frac{m}{2} < s_i < mr_i + \frac{m}{2}.$$

That is, we have to find for every $i \in \{0, 1, 2, 3\}$ such r_i. In fact, the following Lemma states the existence of r_i.

Lemma 19 *Let $s, m \in \mathbb{Z}$, with m odd. There exists $r \in \mathbb{Z}$ such that*

$$mr - \frac{m}{2} < s < mr + \frac{m}{2}.$$

The proof of the rightness of Algorithm 1 can be found in [20]. From here onwards, we restrict to integer quaternions $\alpha \in \mathbb{H}(\mathbb{Z})$.

1.4 Related Work

As stated at the beginning of this Chapter, we solve in this thesis a set of problems in Coding Theory by using Cayley graphs defined both over integer rings of imaginary quadratic fields and over the Lipschitz integers. In this Section we put in context our research by introducing the most outstanding published work related to the results presented here. We will refer to two different topics: Coding Theory and Graph Theory.

The design of error-correcting codes for two-dimensional signal spaces has been recently considered in the technical literature. Hamming and Lee distances have been proved to be inappropriate metrics to deal with QAM signal sets and other related constellations. Up to our knowledge, the first author who modeled certain QAM constellations with quotient rings of Gaussian integers was Klaus Huber. In his papers, Huber introduced a new distance for using in QAM-like constellations denoted as *Mannheim metric*. The rational behind this metric is to consider the Manhattan (or taxicab) metric modulo a two-dimensional grid. Notwithstanding, as we will see later on this thesis, the Mannheim metric is not a distance because it does not fulfill the triangular inequality. Huber proposed block codes over Gaussian integers based on the Mannheim metric in [37] and [38]. Also, in [39] block codes over Eisenstein-Jacobi integers for a modified Mannheim metric were proposed in order to deal with hexagonal constellations.

After Huber's papers, in which the quotient rings considered are taken modulo a prime ideal, other authors considered different groups of complex numbers to be used for coding QAM signals [22], [62]. In addition, other works have considered block codes over quadratic number fields [58], [63], [23]. In [19], a geometrical approach to the problem is considered. The authors use lattices and plane tessellations to derive codes which employ a distance induced by the Euclidean metric over certain graphs embedded in Flat Tori. Recently, a solution for the design of space-time block codes over complex signal constellations is given in [59]. Also, space-time codes over the quaternion algebra have been proposed [7], [46].

Graph theory has known applications to Coding Theory. One example is the *Tanner graph* of a code which provides a useful tool to study the properties of the code or to construct longer codes from smaller ones [70]. Another example appeared in [12], in which the authors solve some problems over torus graphs by means of error-correcting codes based on the Lee metric.

As stated before, our codes are based on Cayley graphs, which have deserved many publications. These graphs were introduced by Sir Arthur Cayley as a significant and intuitive way to visualize groups. From this point of view, they are an excellent tool to study the properties of different algebraic structures. This has lead to a wide research about their geometric properties. Also, it has been proved that Cayley graphs are a powerful approach to solve specific applications such as rearrangement problems and the design of interconnection networks for parallel computers, [18]. Moreover, many different families of well-know graphs such as circulants or tori are Cayley graphs.

There are also many papers concerning circulant graphs much as for its theoretical interest as for its practical applications. It was shown by Turner [71] that the class of connected vertex-symmetric graphs having a prime number of points are identical to the starred polygons. Turner defined a *starred polygon* to be a graph in which vertices v_i and v_j are adjacent if and only if vertices v_{i+k} and v_{j+k} are also adjacent, where $1 \leq k \leq n-1$ and n is de number of vertices of the graph (the subscripts $i+k$ and $j+k$ are taken to be integers modulo n). This is in essence a previous step for the definition of circulants. These kind of graphs were deeply studied by Wilkov [73] focusing on reliability issues. However, it seems that it was Elspas in [24] who introduced these graphs as graphs having circulant adjacency matrices. A matrix is circulant if all its rows are periodic rotations of the first one. These matrices have also other applications to the field of Information Theory in the areas of Coding Theory and Cryptology. An extensive study about the properties and applications of circulant matrices can be found in [21]. According to this book, circulant matrices first appeared in the mathematical literature in 1846 in a paper by E. Catalan.

In addition, there is a wide number of technological papers concerning degree four circulants or *double loop networks*. In [60] optimal or nearly optimal double loop topologies were proposed for local area networks. Later, distance properties of circulant graphs and their minimization were studied in [11] and [26] by means of plane tessellations. Next, in [5] the authors completely characterize a family of degree four circulants with minimum distance-related properties, that is, minimum diameter and average distance and propose them as optimal distance networks for parallel computers. Finally, there are several papers dealing with theoretical aspects of circulants such as isomorphisms [57], [1], [45], colorability [36], graph products [28], [66], *etcetera*.

In our case, Cayley graphs of degrees four and six will be built over Euclidean integer rings. The existence of the Euclidean algorithm will be useful to solve problems over these graphs such as finding perfect dominating sets or obtaining the shortest path between any pair of vertices. The case of degree eight graphs is a bit different since the algebraic structure considered for their definition, the integer ring of quaternions, is not an Euclidean domain.

Up to our knowledge, there is just one work in which Cayley graphs are defined over Number-theoretic algebraic structures. This is the case of certain Ramanujan graphs considered in [20] looking for good expander graphs.

1.5 Thesis Structure and Results

In this Section we detail the organization of the rest of this memory. For each Chapter, we summarize our main findings and, in addition, we reference our published material.

Chapter 2 is devoted to the definition and properties of Gaussian graphs. Firstly, we define Gaussian graphs in Section 2.2 as a subfamily of Cayley graphs. These graphs are built over quotient rings of Gaussian integers using as a set of generators the units of the ring. We also give a simple two-dimensional drawing for all the members of the family of Gaussian graphs. This drawing is based on the fact that the set of graph vertices has as cardinal the sum of two squares. In Section 2.3, we prove a couple of Theorems describing the diameter and the average distance of Gaussian graphs. These results have been obtained by means of a complete description of the distance distribution of the graph vertices. Finally, Section 2.4 is devoted to the problem of the *shortest path calculation* in Gaussian graphs. There, we provide a simple and compact algorithm for finding such a shortest path for any pair of vertices just based on sums and comparisons.

Several papers about Gaussian graphs described in Chapter 2 have been either published or submitted for publication. For example, we have presented optimal broadcast and routing algorithms for particular cases of Gaussian graphs in [49]. A distance-hereditary ring decomposition of Gaussian graphs was presented in [48] and their isomorphic chordal topologies were studied in [6]. In [51] we solve the perfect dominating set problem in Gaussian graphs. In this paper, a complete description of the distance-related properties of Gaussian graphs is also considered.

In Chapter 3, we consider the construction of perfect error-correcting codes over quotient rings of Gaussian integers. For this purpose, we employ a metric which is the distance among vertices in Gaussian graphs. We propose this *Gaussian metric* as the correct one for Coding Theory applications based on rings of Gaussian integers. Moreover, we will show that the Mannheim metric introduced by Huber is not a distance since it does not fulfil the triangular inequality. In Section 3.2, we consider the problem of finding *perfect t-dominating sets* over Gaussian graphs. The solution of this problem has allowed us to propose perfect codes over QAM constellations, which are considered in Section 3.3. We have denoted these codes as *ideal* codes since they constitute ideals of the underlying quotient rings. For these ideal codes we give a uniqueness result in subsection 3.3.1. In Section 3.4, we define the concept of quotient graph of a Gaussian graph when a perfect code exists. These quotient graphs have revealed to be excellent tools to compute maximum and average distances of such codes. Finally, a consequence of this research is that Golomb well-known perfect codes over spaces doted with the Lee-metric are a subcase of our Gaussian codes. This will be shown in Section 3.5.

Papers concerning codes over Gaussian integers described in Chapter 3 have been published in notable Information Theory conferences' proceedings or are in reviewing process in journals. Specifically, in [50] and [52] perfect codes over quotient rings of Gaussian integers are considered. The metric applied to these codes is the distance induced by a circulant Gaussian graph. Also, the weight distribution of these circulants has been presented in [27]. In addition, perfect codes over any quotient ring of Gaussian integers are presented in [53]. In this paper we have shown, as well, that Lee perfect codes introduced by Golomb in [30] are a particular case of our Gaussian perfect codes.

Chapter 4 is devoted to the extension of the techniques from the previous Chapters to hexagonal constellations. In this case, constellations and graph vertices are modeled by quotient rings of Eisenstein-Jacobi integers. In Section 4.2, we define Eisenstein-Jacobi graphs. They are also Cayley graphs over quotient rings, but in this case of Eisenstein-Jacobi integers. Then, we will focus on the case in which these graphs are degree six circulant graphs and compare them with other families of circulants that have been studied before. Later, in Section 4.3, new results inspired in the ones considered for Gaussian graphs will allow us to determine perfect t-dominating sets in Eisenstein-Jacobi graphs. Therefore, perfect codes over hexagonal signal sets can be defined by using as code metric the distance induced by these graphs.

In [50], 1-perfect error correcting codes over hexagonal constellations modeled by quotient rings of Eisenstein-Jacobi integers have been introduced. Recently, in [54], a method for finding certain perfect t-dominating sets over degree six circulant graphs has been considered. Also, an extended method for obtaining perfect t-correcting codes over quotient rings of Eisenstein-Jacobi integers has been given in [55].

A preliminary approach to degree eight graphs and codes over them is going to be considered in Chapter 5. In this case, the graphs will be built over certain subsets of the integer quaternions. Perfect 1-dominating sets are obtained and perfect codes over these sets are compared, in some cases, with perfect Lee codes, which we have considered in [56].

Finally, Chapter 6 concludes this thesis with a brief description of its contributions together with the introduction of some open problems.

Chapter 2

Gaussian Graphs

Gaussian graphs are going to be introduced in this Chapter. These graphs are defined as Cayley graphs over quotient rings of Gaussian integers. We will see that well-known families of graphs such as Circulant and Toroidal graphs are, actually, Gaussian graphs. These graphs have deserved a broad interest both in Graph Theory as well as in other applied areas.

Also in this Chapter, the main distance-related properties of these graphs, such as diameter and average distance, are going to be described. Finally, the problem of finding the shortest path between any pair of vertices is going to be considered.

2.1 Quotient Rings of Gaussian Integers

The *Gaussian integers* $\mathbb{Z}[i]$ is the subset of the complex numbers with integer real and imaginary parts, that is:

$$\mathbb{Z}[i] := \{x + yi \mid x, y \in \mathbb{Z}\}.$$

$\mathbb{Z}[i]$ is an Euclidean domain and the norm is defined as:

$$\begin{array}{rccc} \mathcal{N}: & \mathbb{Z}[i] & \longrightarrow & \mathbb{Z}^+ \\ & x + yi & \longmapsto & x^2 + y^2 \end{array}$$

Then, for every $\alpha, \beta \in \mathbb{Z}[i]$ with $\alpha \neq 0$ there exist $q, r \in \mathbb{Z}[i]$ such that $\beta = q\alpha + r$ with $\mathcal{N}(r) < \mathcal{N}(\alpha)$.

If $0 \neq \alpha \in \mathbb{Z}[i]$, we consider $\mathbb{Z}[i]_\alpha$ which is the ring of the classes of $\mathbb{Z}[i]$ modulo the ideal (α) generated by α. To simplify the notation we will denote both the element of $\mathbb{Z}[i]$ and its class in $\mathbb{Z}[i]_\alpha$ by β. Therefore, we will write $\beta \equiv \beta' \pmod{\alpha}$ if β and β' belong to the same class modulo (α).

As in this research we deal with quotient rings of the the Gaussian integers, we will need an expression for the cardinality of quotients over principal ideals. In addition, we will also need a ring isomorphism between $\mathbb{Z}_N$ and $\mathbb{Z}[i]_\alpha$. We present bellow a couple of theorems dealing with these issues. We have addressed these results and their corresponding proofs since we have not found them in the technical literature.

Theorem 20 *Let $0 \neq \alpha \in \mathbb{Z}[i]$. Then, $\mathbb{Z}[i]_\alpha$ has $\mathcal{N}(\alpha)$ elements.*

Proof.– This proof is based on the proof of Theorem 58 (Chapter 5), whose guidelines were suggested in [32]. Let $\alpha \neq 0$ be a Gaussian integer and $N = \mathcal{N}(\alpha)$. It is easy to prove that $\mathbb{Z}[i]_N$ has N^2 elements. Note that if $\beta = b_1 + b_2 i$ and $\beta' = b_1' + b_2' i$ are congruent modulo N, there exist $\beta'' = b_1'' + b_2'' i$ such that $\beta - \beta' = \beta'' N$ which implies that $b_1 - b_1' = b_1'' N$ and $b_2 - b_2' = b_2'' N$. Therefore, necessarily $b_1 \equiv b_1' \pmod{N}$ and $b_2 \equiv b_2' \pmod{N}$, which implies that we have N^2 possibilities for the coefficients of β.

Now, we have that $(\mathcal{N}(\alpha)) = (\overline{\alpha}\alpha) \subseteq (\alpha)$. Therefore, by the Third Ring Isomorphism Theorem (see [40]), we have that:

$$\frac{\frac{\mathbb{Z}[i]}{(\overline{\alpha}\alpha)}}{\frac{(\alpha)}{(\overline{\alpha}\alpha)}} \cong \frac{\mathbb{Z}[i]}{(\alpha)}$$

Then, applying a consequence of the Lagrange's Theorem for indices of abelian groups we have that the cardinal number of $\dfrac{\mathbb{Z}[i]}{(\overline{\alpha}\alpha)}$ is nm, where the cardinal number of $\dfrac{(\alpha)}{(\overline{\alpha}\alpha)}$ is denoted by n and the cardinal number of $\dfrac{\mathbb{Z}[i]}{(\alpha)}$ is denoted by m.

Finally, the following mapping

$$f : \frac{\mathbb{Z}[i]}{(\overline{\alpha})} \longrightarrow \frac{(\alpha)}{(\overline{\alpha}\alpha)}$$

defined as $f(\beta + (\overline{\alpha})) = \beta\alpha + (\overline{\alpha}\alpha)$ is an isomorphism and $\dfrac{\mathbb{Z}[i]}{(\overline{\alpha})}$ has the same number of elements as $\dfrac{\mathbb{Z}[i]}{(\alpha)}$, which concludes the proof. □

Theorem 21 *Let $\alpha = a + bi \in \mathbb{Z}[i]$ and $N = a^2 + b^2$ be the norm of α. It is obtained that $\mathbb{Z}_N$ and $\mathbb{Z}[i]_\alpha$ are isomorphic rings if and only if $\gcd(a, b) = 1$.*

Proof.– Let us first prove the direct implication. If $\mathbb{Z}_N$ and $\mathbb{Z}[i]_\alpha$ are isomorphic, we denote such ring isomorphism as $f : \mathbb{Z}[i]_\alpha \longrightarrow \mathbb{Z}_N$. We suppose that

$\gcd(a, b) = d \neq 1$ and prove that it is not possible that $\mathbb{Z}[i]_\alpha$ and $\mathbb{Z}_N$ are isomorphic rings.

Since $d = \gcd(a, b)$ divides a and b, we have that $\dfrac{\mathcal{N}(\alpha)}{d}$ is an integer. Moreover, $1 < d$ implies that $0 < \frac{\mathcal{N}(\alpha)}{d} < N$. Hence, $f(\frac{\mathcal{N}(\alpha)}{d}) = \frac{\mathcal{N}(\alpha)}{d} f(1) = \frac{\mathcal{N}(\alpha)}{d} \neq 0 \pmod{N}$.

On the other side, $\dfrac{\mathcal{N}(\alpha)}{d} = \alpha \dfrac{\overline{\alpha}}{d} = 0 \pmod{\alpha}$, from where we get a contradiction since we obtain $f(0) \neq 0$.

To prove the other implication, consider the mapping:

$$\begin{array}{rccc} \mu: & \mathbb{Z}_N & \longrightarrow & \mathbb{Z}[i]_\alpha \\ & g & \longmapsto & g \pmod{\alpha} \end{array}$$

Note that μ is well-defined. Let $g, g' \in \mathbb{Z}_N$ be such that $g \equiv g' \pmod{N}$. Then, there exists $z \in \mathbb{Z}$ such that $g - g' = zN = z\alpha\overline{\alpha}$. Hence, we obtain that $g \equiv g' \pmod{\alpha}$.

Also, μ is injective since, if $\mu(g) \equiv 0 \pmod{\alpha}$ then $g \equiv 0 \pmod{N}$. Let $\mu(g) = g = \beta\alpha$, with $\beta = x + yi \in \mathbb{Z}[i]$. Then, $g = (x + yi)(a + bi) = (xa - yb) + (xb + ya)i$, so we obtain

$$xa - yb = g, \tag{2.1}$$

$$xb + ya = 0. \tag{2.2}$$

Solving (2.2) we have that $(x, y) = (-at, bt)$ where $t \in \mathbb{Z}$. Thus, from (2.1) we obtain $g = -ata - btb = (-t)(a^2 + b^2) = -tN$, so $g \equiv 0 \pmod{N}$.

Now, in order to prove that the mapping is surjective just consider $\gamma = x + yi$ and a pair of integers (x_0, y_0) such that $x_0 b + y_0 a = -y$. Then, $x + yi + (x_0 + y_0 i)(a + bi) = (x + x_0 a - y_0 b) + (y + x_0 b + y_0 a)i = x + x_0 a - y_0 b = g$ is an integer such that $g \equiv \gamma \pmod{\alpha}$. □

Next, we state the following trivial consequence of the previous Theorem:

Corollary 22 *Let* $0 \neq \alpha \in \mathbb{Z}[i]$.

i) Let $\beta \in \mathbb{Z}[i]$ *be such that* β *divides* α*. Then, the ideal generated by* β*,* $(\beta) \subseteq \mathbb{Z}[i]_\alpha$ *has* $\dfrac{\mathcal{N}(\alpha)}{\mathcal{N}(\beta)}$ *elements.*

ii) Let $\beta \in \mathbb{Z}[i]$ *be such that* β *does not divide* α *and* $\eta = \gcd(\beta, \alpha)$*. Then, the ideal* $(\beta) \subseteq \mathbb{Z}[i]_\alpha$ *is generated by* η *and has* $\dfrac{\mathcal{N}(\alpha)}{\mathcal{N}(\eta)}$ *elements.*

Proof.– The first item of the Corollary is a consequence of Theorem 20 and the Third Ring Isomorphism Theorem (see [40]). Since β divides α, we have that $(\alpha) \subseteq (\beta)$. Hence, $\dfrac{(\beta)}{(\alpha)}$, is an ideal of $\dfrac{\mathbb{Z}[i]}{(\alpha)}$ and we have that

$$\frac{\frac{\mathbb{Z}[i]}{(\alpha)}}{\frac{(\beta)}{(\alpha)}} \cong \frac{\mathbb{Z}[i]}{(\beta)},$$

from where we find that $\dfrac{(\beta)}{(\alpha)}$ has order $\dfrac{\mathcal{N}(\alpha)}{\mathcal{N}(\beta)}$.

For the second item of the Corollary, consider $\gamma = \gcd(\alpha, \beta)$. Then, there exists $\gamma_1, \gamma_2 \in \mathbb{Z}[i]$ such that $\gamma = \gamma_1\beta + \gamma_2\alpha$. This implies that $\gamma \equiv \gamma_1\beta \pmod{\alpha}$, so $(\gamma) \subseteq (\beta)$. On the other hand, since γ divides β then $(\beta) \subseteq (\gamma)$. Finally, we have to apply the first item of the corollary to (γ) since γ divides α. □

2.2 Definition of Gaussian Graphs

In this Section we are going to define Gaussian graphs. In addition, we present a simple two-dimensional drawing which characterizes Gaussian graphs. Some examples that include well-known graphs are given at the end of the Section.

Gaussian graphs are a special family of Cayley graphs. Cayley graphs are defined over groups but in our case, they are defined over quotient rings of Gaussian integers using the units of the ring as the set of generators.

Definition 23 *Let $0 \neq \alpha \in \mathbb{Z}[i]$. We define the* Gaussian graph *generated by α, $G_\alpha = (V, E)$, as follows:*

i) $V = \mathbb{Z}[i]_\alpha$ *is the set of vertices.*

ii) $E = \{(\eta, \beta) \in V \times V \mid \beta - \eta \equiv \pm 1, \pm i \pmod{\alpha}\}$ *is the set of edges.*

According to Theorem 20, the Gaussian graph generated by $\alpha \in \mathbb{Z}[i]$ has order $\mathcal{N}(\alpha)$. Gaussian graphs are regular of degree four since every vertex is adjacent to other different four vertices. Also, they are undirected, connected and vertex-symmetric by definition.

The following Lemma can be easily proved:

Lemma 24 *Given $a + bi, c + di \in \mathbb{Z}[i]$ it is obtained that $G_{a+bi} \cong G_{c+di}$ if and only if exists $u \in \{\pm 1, \pm i\}$ such that $a + bi = u(c + di)$ or $a - bi = u(c + di)$.*

Consequently, we can assume that any Gaussian graph is generated by a Gaussian integer $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$ such that $0 \leq a \leq b$.

Next, we describe in a constructive way, a simple two-dimensional drawing of any Gaussian graph. Let us assume first $\alpha = a + bi \in \mathbb{Z}[i]$ with $0 < a \leq b$; the case $a = 0$ will be considered later. Gaussian graphs can be represented as mesh-like drawings in which peripheral vertices complete their adjacency by means of wrap-around edges. The idea is to arrange the $a^2 + b^2$ vertices in two attached square meshes of $a \times a$ and $b \times b$ vertices, respectively. We will consider vertex 0 located, for convenience, at the left lower corner of the smaller square mesh, as shown in Figure 2.1. The four adjacent vertices to vertex zero are $\{\pm 1, \pm i\}$. Vertices 1 and i are also located at the smaller square mesh. As $-1 \equiv (a + b - 1) + (b - a)i \pmod{\alpha}$ and $-i \equiv a + (b - 1)i \pmod{\alpha}$, vertices -1 and $-i$, which are located at the periphery of the bigger square mesh, are reached from node 0 by means of two wrap-around edges. Thanks to vertex symmetry, all the peripheral vertices are connected following the same wrap-around pattern.

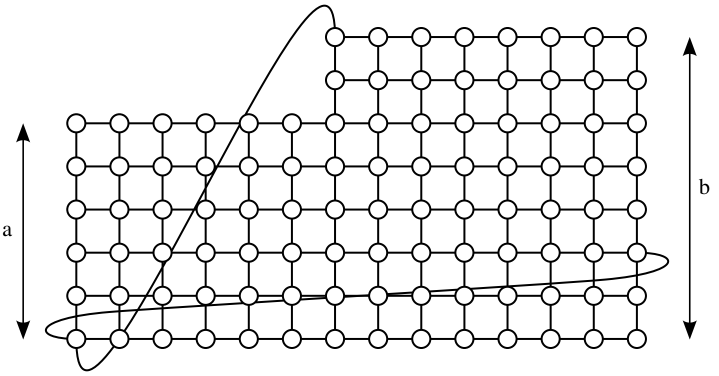

Figure 2.1: Adjacent Vertices to Vertex 0 in G_{6+8i}.

Now, we are going to prove that graphs resulting from the previous two-dimensional drawing are, actually, Gaussian graphs. We will state a couple of Theorems characterizing the set of vertices and the wrap-around edges of these mesh-based graphs. Previously, we state the following straightforward Lemma as it is needed for proving the first Theorem.

Lemma 25 *Let $0 \neq a + bi \in \mathbb{Z}[i]$. Then, $x + yi \equiv x' + y'i \pmod{a + bi}$ if and only if there exist $u, v \in \mathbb{Z}$ such that $x' = x + ua - vb$ and $y' = y + ub + va$.*

Theorem 26 *Let $a, b \in \mathbb{Z}$ be such that $0 < a \leq b$, and two finite sets defined as*

i) $S_a = \{x + yi \in \mathbb{Z}[i] \mid 0 \leq x \leq a-1 \wedge \; 0 \leq y \leq a-1\}$.

ii) $S_b = \{x + yi \in \mathbb{Z}[i] \mid a \leq x \leq a+b-1 \wedge \; 0 \leq y \leq b-1\}$.

Then, $\mathcal{D} = S_a \cup S_b$ is a reduced residue system of $\mathbb{Z}[i]_\alpha$.

Proof.– Given $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$, a reduced residue system of $\mathbb{Z}[i]_\alpha$ has $\mathcal{N}(\alpha) = a^2 + b^2$ elements. As we have that $|S_a| = a^2$, $|S_b| = b^2$ and $S_a \cap S_b = \emptyset$, it is enough to prove that all the elements in $\mathcal{D}$ are different. Given $\eta = x + yi$, $\eta' = x' + y'i \in \mathcal{D}$ such that $\eta \equiv \eta' \pmod{\alpha}$, we have to see that $\eta = \eta'$. By Lemma 25, we have

$$x + yi \equiv x' + y'i \pmod{\alpha} \;\Leftrightarrow\; \left\{ \begin{array}{l} x - x' = ua - vb \\ y - y' = ub + va \end{array} \right.$$

First, if we suppose that $uv > 0$, as a and b are positive integers we have that $|ub + va| = |v|a + |u|b \geq a + b$. Now, as $y, y' \in \{0, \ldots, b-1\}$, we have that $|y - y'| \leq b - 1 < a + b$. Thus, we get a contradiction.

Next, if we suppose $uv < 0$, we have that $|ua - vb| = |u|a + |v|b \geq a + b$. Now, as $x, x' \in \{0, \ldots, a+b-1\}$, we have that $|x - x'| \leq a + b - 1 < a + b$. Thus, we get a contradiction, too.

The last possibility is to consider $uv = 0$. If we suppose $u = 0$, we have that $x - x' = -vb$ and $y - y' = va$. As $|x - x'| < a + b$, the first condition implies that $|v| < 2$. We just have to consider three cases. If $v = 1$, then $x - x' = -b$ and $y - y' = a$. The first condition forces that $\eta \in S_a$ and $\eta' \in S_b$. But the second condition forces $\eta \in S_b$. As $S_a \cap S_b = \emptyset$, we get another contradiction. The case $v = -1$ can be analyzed in the same way. Finally, if we suppose $v = 0$, we have that $|ub + va| = |u|b$. As $|y - y'| < b$, this condition forces $u = 0$. Thus, the only possibility is $x = x'$ and $y = y'$. □

Theorem 27 *Let $0 < a \leq b$. Let the set $\mathcal{D}$ be as previously defined. Suppose that all the points in $\mathcal{D}$ are mesh-like connected and that wrap-around edges are defined as:*

i) *x is connected to $(x + a) + (b - 1)i$ if $0 \leq x \leq b - 1$.*

ii) *x is connected to $(x - b) + (a - 1)i$ if $b \leq x \leq a + b - 1$.*

iii) *yi is connected to $(a + b - 1) + (y + b - a)i$ if $0 \leq y \leq a - 1$.*

iv) *$a + yi$ is connected to $(a + b - 1) + (y - a)i$ if $a \leq y \leq b - 1$.*

Then, the graph defined by this adjacency pattern is isomorphic to the Gaussian graph generated by $a + bi$.

Sketch of the Proof.– The proof is straightforward when considering these graphs as plane tessellations as in [26] or [74]. In both papers, degree four circulants were studied by means of the tessellation that they infer in the plane. More specifically, if we represent each vertex of the graph as a unitary square with its four neighbors attached to its sides, the complete graph can be fully characterized by a L-shape tile whose area equals the graph order. Then, the observable periodical tessellation dictates the connectivity of the wrap-around edges. Figure 2.2 shows the plane tessellation associated the Gaussian graph G_{6+8i}. □

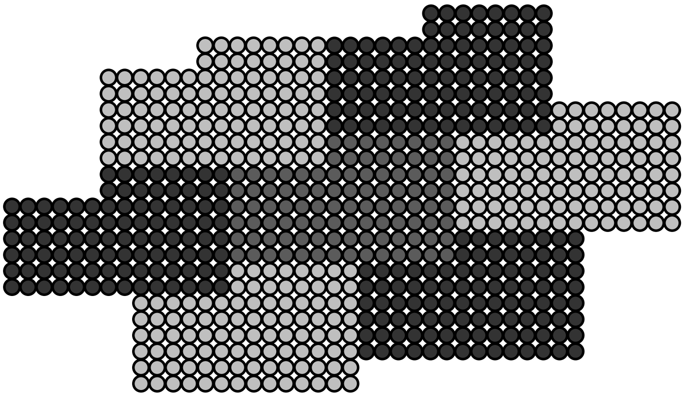

Figure 2.2: Plane Tessellation Associated to G_{6+8i}.

Example 4 *Let us consider the Gaussian graph generated by $\alpha = 6+8i$. We arrange the 100 vertices of G_α in two attached meshes of 6^2 and 8^2 vertices respectively. Then, following the wrap-around edges pattern described in Theorem 27 we obtain the 2D-drawing of the graph shown in Figure 2.3.*

As stated before, some well-known graphs are Gaussian graphs. Two notable examples are Tori and certain Circulant graphs. A *Torus* with b^2 vertices can be defined as $\mathbb{T}_b = (V, E)$, where $V = \mathbb{Z}_b \times \mathbb{Z}_b$ and two vertices $(n, m), (n', m') \in V$ are adjacent if and only if $n = n'$ and $m - m' \equiv \pm 1 \pmod b$ or $m = m'$ and $n - n' \equiv \pm 1 \pmod b$. Theorem 29 formally states the relationship between these known graphs and the Gaussian graphs introduced in this thesis. We will need the following Lemma to prove it whose proof we have not find it in the literature and hence, we address it next.

Lemma 28 *Let $Cay(\mathcal{G}, S)$ be a connected Cayley graph. Then, it is circulant if and only if $(\mathcal{G}, \cdot)$ is cyclic.*

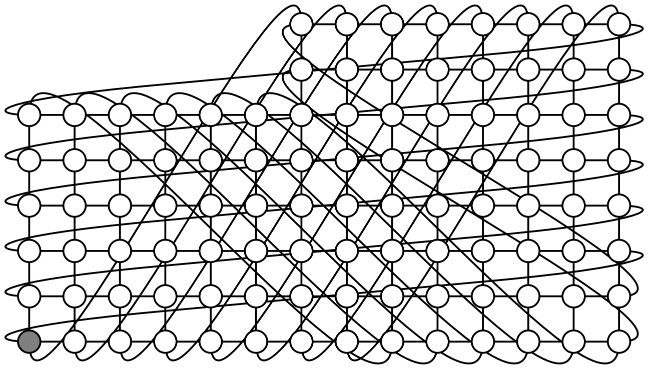

Figure 2.3: 2D-drawing of G_{6+8i}.

Proof.– The undirect implication is a straightforward consequence of the definition of circulant graphs. Let us proof the direct implication. Therefore, we suppose that $Cay(\mathcal{G}, S)$ is circulant. Hence, the degree of the graph d is the cardinal of S and the order N is the cardinal of $\mathcal{G}$. Consequently, $Cay(\mathcal{G}, S) \cong C_N(j_1, \ldots j_d)$ for some different integers $j_1, \ldots j_d$. Let us denote by $f : \mathcal{G} \longrightarrow \mathbb{Z}_N$ the graph isomorphism between $Cay(\mathcal{G}, S)$ and $C_N(j_1, \ldots j_d)$. By the definition of graph isomorphism, we have that

$$y = x + s_i \Leftrightarrow f(y) = f(x) + j_k$$

for $i, k \in \{1, \ldots d\}$. We can assume without loss of generality that $f(s_i) = f(j_i)$ for $i = 1, \ldots d$. Note that, as a consequence $f(ms_i) = f(m)f(s_i) = f(m)j_i$. Also, $f(0_\mathcal{G}) = 0_{\mathbb{Z}_N}$.

Let $x, y \in G$ be two vertices. Since $Cay(\mathcal{G}, S)$ is connected, there exist $x_i, y_i \in \mathbb{Z}$ such that $x = \sum_{i=1}^d x_i s_i$ and $y = \sum_{i=1}^d y_i s_i$. Now, $f(x + y) = f(\sum_{i=1}^d x_i s_i + \sum_{i=1}^d y_i s_i) = f(\sum_{i=1}^d (x_i + y_i)s_i) = \sum_{i=1}^d f(x_i + y_i)f(s_i) = \sum_{i=1}^d (f(x_i) + f(y_i))f(s_i) = f(x) + f(y)$, which implies that f is a group isomorphism. Therefore, $\mathcal{G}$ is cyclic. □

Theorem 29 *Let $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$ be such that $0 \leq a \leq b$, and G_α the Gaussian graph generated by α. Then,*

i) $G_\alpha \cong C_{a^2+b^2}(a, b)$ if and only if $\gcd(a, b) = 1$.

ii) $G_\alpha \cong \mathbb{T}_b$ if and only if $a = 0$.

Proof.– We only prove direct implications since the others are direct consequences of Lemma 28. We know that a circulant is a Cayley graph over a cyclic group and the only case in which $\mathbb{Z}[i]_{a+bi}$ is cyclic is when $\gcd(a, b) = 1$. Also, $\mathbb{Z}[i]_\alpha \cong \mathbb{Z}_b \times \mathbb{Z}_b$

if and only if real or imaginary parts of α are zero. Let us discuss now the direct implications.

For the first item, consider $\alpha = a + bi$ such that $\gcd(a, b) = 1$. We have that $C_{\mathcal{N}(\alpha)}(a, b)$ and G_α are isomorphic graphs with the graph isomorphism defined as:

$$\begin{array}{rccc} \Phi: & \mathbb{Z}_{\mathcal{N}(\alpha)} & \longrightarrow & \mathbb{Z}[i]_\alpha \\ & j & \longmapsto & x + yi \pmod{\alpha} \end{array}$$

where $j \equiv ax + by \pmod{\mathcal{N}(\alpha)}$.

We have to prove that Φ is a bijection that preserves the distances. Firstly, note that the set of solutions of the Diophantine equation $aX + bY = s(a^2 + b^2)$ is $\{(X, Y) = (sa + bt, sb - at) | t \in \mathbb{Z}\}$. We denote $N = a^2 + b^2$.

Φ is well-defined. Let $j \in \mathbb{Z}$ such that $j \equiv ax + by \pmod{N}$ and $h \equiv j \pmod{N}$. We have to prove that $\Phi(j) \equiv \Phi(h) \pmod{\alpha}$. Suppose that $h \equiv ax' + by' \pmod{N}$. Then, assuming the hypothesis, we have that $a(x - x') + b(y - y') \equiv 0 \pmod{N}$, that is, there exists $s \in \mathbb{Z}$ verifying $a(x - x') + b(y - y') = sN$. Now, if $a(x - x') + b(y - y') = s(a^2 + b^2)$ then $(x - x') + (y - y')i \equiv 0 \pmod{\alpha}$. We have that $(x - x') + (y - y')i = (sa + bt) + (sb - at)i = s(a + bi) + t(b - ai) = s(a + bi) - t(a + bi)i = (s - ti)(a + bi)$, which concludes this part of the proof, since $s - ti \in \mathbb{Z}[i]$.

Φ is injective. We are going to prove that if $\Phi(j) \equiv \Phi(h) \pmod{\alpha}$, with $j, h \in \mathbb{Z}_N$, implies that $j \equiv h \pmod{N}$. Suppose that $\Phi(j) = x + yi$, $\Phi(h) = x' + y'i$. Then, $(x - x') + (y - y')i = \gamma\alpha$, with $\gamma \in \mathbb{Z}[i]$. Let $\gamma = \gamma_1 + \gamma_2 i$. Thus, $(x - x') + (y - y')i = \gamma\alpha = (\gamma_1 a - \gamma_2 b) + (\gamma_1 b + \gamma_2 a)i$, so we get:

$$x - x' = \gamma_1 a - \gamma_2 b \Rightarrow a(x - x') = \gamma_1 a^2 - \gamma_2 ab,$$

$$y - y' = \gamma_1 b + \gamma_2 a \Rightarrow b(y - y') = \gamma_1 b^2 + \gamma_2 ab.$$

Now, $a(x - x') + b(y - y') = \gamma_1(a^2 + b^2)$, with $\gamma_1 \in \mathbb{Z}$, that is, $j \equiv h \pmod{N}$.

Also, it can be easily proved that Φ is surjective.

To prove the second item just consider the graph isomorphism between the square Torus $\mathbb{T}_b$ with b^2 vertices and G_b:

$$\begin{array}{rccc} \Phi': & \mathbb{Z}_b \times \mathbb{Z}_b & \longrightarrow & \mathbb{Z}[i]_b \\ & (x, y) & \longmapsto & x + yi \pmod{b} \end{array}$$

□

Other topologies that have been used in the field of Interconnection Networks also correspond to particular cases of Gaussian Graphs. Indeed, we have that the doubly twisted torus introduced in [67] is isomorphic to G_{1+ti}. Furthermore, the rectangular twisted tori used in [75] corresponds to G_{t+ti} and, finally, the dense Midimew from [5] is isomorphic to $G_{t+(t+1)i}$. These topologies have been analyzed for their use as interconnection networks in [14]. Using Theorem 27, all of them can be represented as orthogonal meshes with wrap-around edges. Figure 2.4 shows some of these graphs represented as Gaussian graphs. It is worthwhile to note that all of them have a planar lay-out when laid on a torus surface [38].

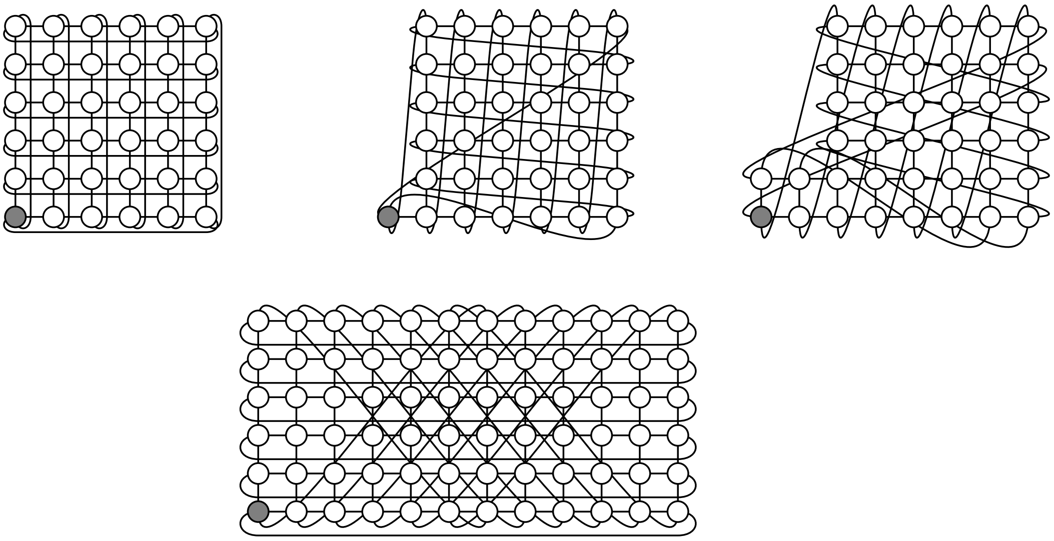

Figure 2.4: Gaussian Graphs G_6, G_{1+6i}, G_{2+6i} and G_{6+6i}.

2.3 Distance Properties of Gaussian Graphs

In this Section, general expressions for the diameter and the average distance of a Gaussian graph are going to be obtained. To this aim, we will describe the *vertex-to-vertex* distance distribution of any Gaussian graph. Note that the distance between two vertices β and γ in G_α can be expressed as

$$D_\alpha(\beta, \gamma) = \min\{|x| + |y| \mid (\beta - \gamma) \equiv x + yi \pmod{\alpha}\}.$$

Also, since G_α is vertex-symmetric, we can define the *weight* of a vertex β (its distance to vertex 0) as

$$w_\alpha(\beta) = D_\alpha(\beta, 0) = \min\{|x| + |y| \mid \beta \equiv x + yi \pmod{\alpha}\}.$$

Then, to compute the distance distribution of a Gaussian graph it is enough to find its number of vertices of weight s, for $s = 0, 1, \ldots, k$, where k is the diameter of the graph. This number will be denoted as $\Delta_\alpha(s)$. Next, we state a couple of Theorems that characterize the distance distribution of odd and even order Gaussian graphs , respectively.

Theorem 30 *Let $0 \neq \alpha = a + bi \in \mathbb{Z}$ be such that $0 \leq a \leq b$, $N = a^2 + b^2$ an odd integer and $t = \dfrac{a+b-1}{2}$. The distance distribution of the graph G_α is as follows:*

i) $\Delta_\alpha(0) = 1$.

ii) $\Delta_\alpha(s) = 4s$ *if* $1 \leq s \leq t$.

iii) $\Delta_\alpha(s) = 4(b - s)$, *if* $t < s \leq b - 1$.

Theorem 31 *Let $0 \neq \alpha = a + bi \in \mathbb{Z}$ be such that $0 \leq a \leq b$, $N = a^2 + b^2$ an even integer and $t = \dfrac{a+b}{2}$.*
When $a < b$, the distance distribution of the graph G_α is as follows:

i) $\Delta_\alpha(0) = 1$.

ii) $\Delta_\alpha(s) = 4s$, *if* $0 < s < t$.

iii) $\Delta_\alpha(t) = 2(b - 1)$.

iv) $\Delta_\alpha(s) = 4(b - s)$, *if* $t < s < b$.

v) $\Delta_\alpha(b) = 1$.

When $0 < a = b$, the distance distribution of the graph G_{b+bi} is as follows:

i) $\Delta_\alpha(0) = 1$.

ii) $\Delta_\alpha(s) = 4s$, *if* $0 < s < b$.

iii) $\Delta_\alpha(b) = 2b - 1$.

Proofs of Theorems 30 and 31 follow similar steps. In order to prove them we need the following Lemma:

Lemma 32 *Given $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$, we define $|\alpha| = |a| + |b|$.*

i) If $0 \neq \gamma \in \mathbb{Z}[i]$, then $|\alpha| \leq |\gamma\alpha|$.

ii) If $a < b$ and $0 \neq \gamma \in \mathbb{Z}[i]$, then $|\alpha| = |\gamma\alpha|$ if and only if $|\gamma| = 1$.

iii) If $\gamma \in \mathbb{Z}[i]$ and $0 \leq a \leq b$, we have that if $|\alpha\gamma| < 2b$, then $|\gamma| \leq 1$.

Proof.– We prove the first item of the Lemma exploring the different possibilities. Given $0 \neq \gamma = u + vi \in \mathbb{Z}[i]$, we have that $\gamma\alpha = (au - bv) + (av + bu)i$.

- If $uv > 0$, then $|av + bu| \geq a + b$.
- If $uv < 0$, then $|au - bv| \geq a + b$.
- If $u = 0$ and $v \neq 0$, then $|\gamma\alpha| = |v|(a + b)$.
- If $u \neq 0$ and $v = 0$, then $|\gamma\alpha| = |u|(a + b)$.

To prove the second item, we just have to use the assumption that $a < b$ an proceed as in the previous item.

Finally, to prove the last item, we have that as $x^2 + y^2 \leq (|x| + |y|)^2$, then $\mathcal{N}(\gamma\alpha) \leq |\gamma\alpha|^2 < 4b^2$. Thus, $\mathcal{N}(\gamma) < 4$ as $\mathcal{N}(\alpha) \geq b^2$. Noting that as $\gamma \in \mathbb{Z}[i]$, we just have to check the case $\mathcal{N}(\gamma) = 2$, but it is straightforward to obtain that in this case $|\gamma\alpha| = 2b$. □

Proof.– (of **Theorem 30**). Consider $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$ with $0 \leq a \leq b$ and $N = a^2 + b^2$, an odd integer. First, note that $\dfrac{a + b - 1}{2} \geq 0$ is always integer since $a^2 + b^2 \equiv 1 \pmod 2$ if and only if $a + b \equiv 1 \pmod 2$. Also, $\Delta_\alpha(0) = 1$ since 0 is the only Gaussian integer with weight 0.

Now, we consider the cases $s = 1, \ldots, t$. First, we denote the square with vertices $-t$, ti, t and $-ti$ as $Q_t = \{x + yi \in \mathbb{Z}[i] \mid |x| + |y| \leq t\}$. Such a square can be seen in Figure 2.5. Two different Gaussian integers $\eta, \eta' \in Q_t$ are not congruent modulo α. If $\eta \equiv \eta' \pmod \alpha$, we have that $\eta - \eta' = \gamma\alpha$ for $0 \neq \gamma \in \mathbb{Z}[i]$. By Lemma 32, we have that $|\eta - \eta'| \geq |\alpha| = a + b$. However, thanks to the triangular inequality, we have that $|\eta - \eta'| \leq |\eta| + |\eta'| \leq 2t = a + b - 1$, which is a contradiction. Therefore, since there are $4s$ solutions to the equation $|\eta| = s$, for $s = 1, \ldots, t$ in Q_t, we have proved the second item of the Theorem.

Finally, we consider the case $s = t + 1, \ldots, b - 1$. First, note that for $b = a + 3$, the four Gaussian integers $(a + 1) + i$, $(-a - 1) - i$, $1 - (a + 1)i$ and $-1 + (a + 1)i$ have weight $s = a + 2 = (a + b - 1)/2 + 1 = b - 1$. Moreover, these couples do not belong to the same class modulo α.

Otherwise, we denote as T the triangle with vertices $t + i$, $(a + 1) + (t - a)i$ and $t + (t - a)i$, as seen in Figure 2.5. In the region included in T they are $(b - s)$ Gaussian integers η such that $|\eta| = s$, for $s = t + 1, \ldots, b - 1$. The triangle T does not intersect with the region Q_t. If there exists $\eta \in Q_t$ and $\eta' \in T$ such that $\eta - \eta' = \alpha\gamma$ for $0 \neq \gamma \in \mathbb{Z}[i]$, then $|\eta - \eta'| \leq |\eta| + |\eta'| \leq t + b - 1 < 2b$. By Lemma 32, we have

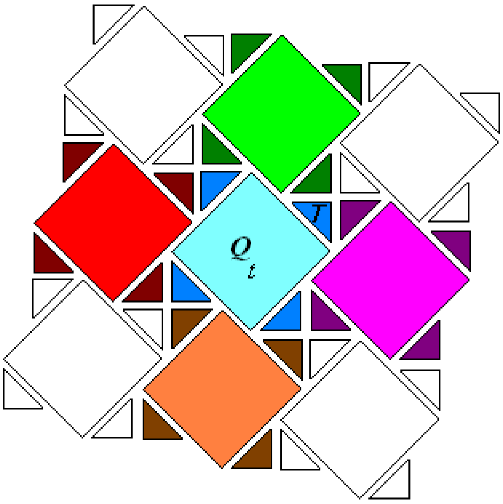

Figure 2.5: Translations of Regions Q, T, $-T$, iT and $-iT$.

that $\gamma \in \{\pm 1, \pm i\}$ and regions $Q_t + \gamma\alpha$ and T do not intersect.

Moreover, regions T, $-T$, iT and $-iT$ do not intersect as it can be seen in Figure 2.5. As $\eta \equiv \eta \pmod{\alpha} \Leftrightarrow \eta \equiv \eta' + \gamma \cdot \alpha \pmod{\alpha}$ for any $\gamma \in \mathbb{Z}[i]$, we can consider the triangles T, $iT - i \cdot \alpha$, $-T + \alpha$ and $-iT + i \cdot \alpha$ to prove that they do not intersect. These triangles are adjacent as it can be seen in Figure 2.5 and, given two vertices η and η' in these triangles, they satisfy that $|\eta - \eta'| < 2(t - a) = b - a - 1 < a + b$. Thus, by Lemma 32 we have that these vertices are not congruent modulo α. □

Proof.– (of **Theorem 31**). First of all, note that $N = a^2 + b^2 \equiv 0 \pmod{2}$ if and only if $a + b \equiv 0 \pmod{2}$. Hence $\dfrac{a+b}{2}$ is always an integer. Once more, we can choose a and b two integers such that $0 \leq a \leq b$ and $N = a^2 + b^2$ even.

Obviously, $\Delta_\alpha(0) = 1$ since 0 is the only Gaussian integer with weight 0. Analogously to the odd case proof, regions Q_{t-1} and $Q_{t-1} + \gamma\alpha$ do not intersect for any $0 \neq \gamma \in \mathbb{Z}[i]$. Therefore, the Gaussian integers in Q_{t-1} belong to different classes modulo α, where $Q_{t-1} = \{\eta \mid |\eta| \leq t - 1\}$. Thus, there are $4s$ elements of weight s, for $s = 1, \ldots, t - 1$ in Q_{t-1} which proves second item for both cases.

Firstly, we consider the case $a < b$. Suppose that $s = t = (a + b)/2$. In this case we consider the Gaussian integers in four segments of four different straight lines. The first two ones are the segments $S_1 = \overline{A_1 B_1}$ and $S_2 = \overline{A_2 B_2}$, where

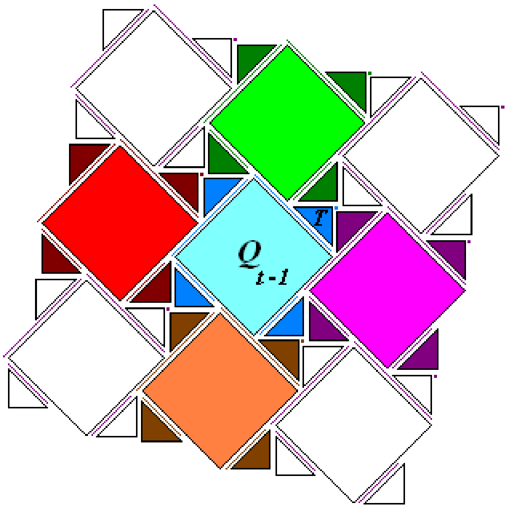

Figure 2.6: Translations of Region Q_{t-1}, Segments and Triangles of the Proof.

$$\begin{array}{rcc} A_1 & = & (t-1)+i \\ B_1 & = & ti \\ A_2 & = & (-1-a)+(t+1-b)i \\ B_2 & = & (1-t)-i \end{array}$$

Note that S_1 is a portion of the straight line defined by $S = \{x+yi \mid x+y=t\}$. The second segment is a translation by $-\alpha$ of a portion of this line. Therefore, we have that $(S_1-\alpha)\cap S_2 = \emptyset$.

The two segments left are $R_1 = \overline{C_1D_1}$ and $R_2 = \overline{C_2D_2}$, where

$$\begin{array}{rcc} C_1 & = & -1+(t-1)i \\ D_1 & = & -t \\ C_2 & = & (t-a-1)+(-1-a)i \\ D_2 & = & 1+(1-t)i \end{array}$$

Note that R_1 is a portion of the line $R = \{x+yi \mid -x+y=t\}$ and R_2 is a translation by means of $-\alpha i$ of a portion of this line as well. Once more, we have that $(R_1-\alpha i)\cap R_2 = \emptyset$.

It is easy to check that there are exactly $2(b-1)$ Gaussian integers in the set of points belonging to $S_1 \cup S_2 \cup R_1 \cup R_2$. We now show that any pair of Gaussian integers η, η' in this set of points are not congruent modulo α. As $|\eta-\eta'| \leq |\eta|+|\eta'| \leq 2t = a+b < 2b$, by Lemma 32, we have that $\eta-\eta' = u\alpha$, with $u \in \{\pm 1, \pm i\}$. Thanks to the previous comments it is very easy to see that this can never occur.

Now, we consider the case $s = t+1, \ldots, b-1$. Just note that this case only exists when $b \geq a+4$. First, note that in the case $b = a+4$ the four Gaussian integers $(a+1)+2i$, $(-a-1)-2i$, $2-(a+1)i$ and $-2+(a+1)i$ have weight $s = a+3 = b-1$. These Gaussian integers do not belong to the same class modulo α.

Otherwise, we denote the triangle with vertices $(t-1)+2i$, $(t-1)+(t-a)i$ and $(a+1)+(t-a)i$ as T. In the region T we have $(b-s)$ Gaussian integers η such that $|\eta| = s$, for $s = t+1, \ldots, b-1$. Analogously to the odd case, triangle T does not intersect with the region $Q_{t-1} \cup S_1 \cup S_2 \cup R_1 \cup R_2 \subset Q_t$. If there exist $\eta \in Q_t$ and $\eta' \in T$ such that $\eta - \eta' = \alpha\gamma$ for $0 \neq \gamma \in \mathbb{Z}[i]$, then $|\eta - \eta'| \leq |\eta| + |\eta'| \leq t+b-1 < 2b$. By Lemma 32, we have that $\gamma \in \{\pm 1, \pm i\}$ and regions $Q_t + \gamma\alpha$ and T do not intersect. Moreover, triangles T, $-T$, iT and $-iT$ do not intersect, which concludes the proof of this item.

Finally, the four Gaussian integers $t+(t-a)i$, $(a-t)+ti$, $-t+(a-t)i$ and $(t-a)-ti$ have weight b. The four points belong to the same class modulo α, so we select the first one $t+(t-a)i$ as the representant of weight b.

For the particular case where $0 < a = b$, the first two items are proved equivalently to the case $a < b$. For the third item, as $t = \dfrac{a+b}{2} = b$, we have that the three regions specified in the previous case, collapse to only one region. This region is defined by the segments $T_1 = \overline{E_1F_1}$ and $T_2 = \overline{E_2F_2}$, where

$$\begin{array}{rcl} E_1 & = & (b-1)+i \\ F_1 & = & ti \\ E_2 & = & 1+(b-1)i \\ F_2 & = & (b-1)+i \end{array}$$

This region has exactly $2b-1$ points and, following similar steps to the previous case, it is easy to see that they are all different classes modulo α. □

Using the distance distribution of Gaussian graphs proved in Theorems 30 and 31, a closed formula for their diameter and average distance can be easily deduced.

Corollary 33 *Let $0 \neq \alpha = a+bi \in \mathbb{Z}[i]$ be such that $0 \leq a \leq b$. Let $N = a^2+b^2$ be the norm of α. The diameter k of the Gaussian graph G_{a+bi} is:*

$$k = \begin{cases} b & \textit{if} \quad N \textit{ is even} \\ b-1 & \textit{if} \quad N \textit{ is odd} \end{cases}$$

Corollary 34 *Let $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$ be such that $0 \leq a \leq b$. Let $N = a^2 + b^2$ be the norm of α. We can compute the average distance $\bar{k}$ of the Gaussian graph G_α as:*

$$\bar{k} = \begin{cases} \frac{3bN+2a(a^2-1)}{6(N-1)} & if \quad N \text{ is even} \\ \frac{3b(N-1)+2a(a^2-1)}{6(N-1)} & if \quad N \text{ is odd} \end{cases}$$

It is worthwhile to note that the problem of obtaining a closed formula for the diameter of arbitrary degree four circulants is not solved. In fact, if we restrict the problem to degree four *chordal rings*, that is, circulant graphs having a jump equal to one the problem is also unsolved [9]. Just particular solutions for smaller families such as the optimal circulants considered in [5] have been obtained. However, the special structure of Gaussian graphs has allowed us to solve a problem not easy to deal with in other families of graphs having a similar algebraic nature as Gaussian graphs.

Finally, we would like to highlight that Theorems 30 and 31 give us not only the distance distribution but also a new representation of these graphs since in the proofs we also obtain a reduced residue system of $\mathbb{Z}[i]_\alpha$ in both cases. This new representation of the graph has the special feature that all the vertices are obtained at a minimum distance from the central vertex, which we have stated to be vertex zero. The next Figure 2.7 gives an example of this representation for the Gaussian graph generated by $\alpha = 6 + 8i$.

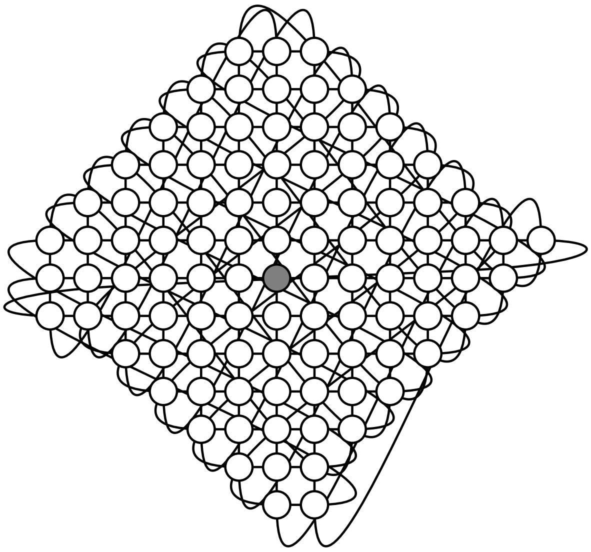

Figure 2.7: Minimum Distance Representation of the Graph G_{6+8i} Viewed from Vertex 0.

2.4 Shortest Paths in Gaussian Graphs

In this Section, we consider the *shortest path problem* in Gaussian graphs giving a simple routing algorithm. An algorithm is said to be a *routing algorithm* if given a pair of vertices it routes a message from the source to the destination vertices. Also, a routing algorithm is called *oblivious* if the route depends only on the source and the destination vertex. A shortest routing path may be as long as the diameter k, which implies that the worst-case time complexity of any routing algorithm is bounded below by $\Omega(k)$ [65]. We call a routing algorithm *optimal* if its worst-case time complexity is $\mathcal{O}(k)$.

Throughout the years, many efforts have been done in order to obtain optimal algorithms to find minimum paths in circulant graphs, as for example the ones introduced in [13], [31] and [65]. Such algorithms consider graphs whose vertices are labeled by integers. If $n, m \in \mathbb{Z}_N$ are two vertices of the circulant graph $C_N(j_1, j_2)$, a shortest path from n to m will consist of $|x|$ hops in j_1 and $|y|$ hops in j_2, where $x, y \in \mathbb{Z}$. Hence, all these routing algorithms have a common preprocessing step $Compute(x, y)$. Consequently, a generic routing algorithm could be as the one described in Algorithm 2, (see [65]).

```
begin
    STEP 1. Compute(x, y);
    STEP 2. for $i := 0$ to $|x|$ do $n := n + sign(x) * j_1 \pmod{N}$;
    STEP 3. for $i := 0$ to $|y|$ do $m := m + sign(y) * j_2 \pmod{N}$;
end
```

Algorithm 2: Shortest Path Calculation in Degree Four Circulant Graphs.

Step 1 corresponds to the calculation of $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ such that $n - m \equiv xj_1 + yj_2 \pmod{N}$ with $|x| + |y|$ minimum.

Steps 2 and 3 take $|x| + |y| \leq k$ hops, where k is the diameter of the graph. Hence, the algorithms worst case complexity is the worst case time of Step 1 plus $\mathcal{O}(k)$. For this reason, most of the papers about routing in circulant graphs focus on algorithms to solve Step 1. In particular, in [65] an algorithm with worst-case complexity $\Theta(k)$ is presented. Also, in [31] an algorithm to compute (x, y) in $\Theta(\log^3 N)$ total bit operations is obtained, where N is the order of the corresponding degree four circulant. In other families of graphs such as Tori or Midimews [5] the routing algorithm has been also studied in order to obtain a particular solution.

As in degree four circulant graphs, if we want to find the path from a source vertex η to a destination vertex η' in a Gaussian graph we will have to compute $r = r_1 + ir_2 \equiv \eta' - \eta \pmod{\alpha}$ with $|r_1| + |r_2|$ minimum. Then, any combination of r_1 jumps in real dimension and r_2 jumps in imaginary dimension will give us a shortest path joining source vertex η and destination vertex η'. Therefore, a similar routing algorithm to the one presented in Algorithm 2 can be also used in Gaussian graphs. Here, we propose a new algorithm that finds such $r = r_1 + r_2 i$ with $|r_1| + |r_2|$ minimum. This Algorithm is based on the next Lemma and takes advantage of the labeling of the vertices in terms of Gaussian integers.

Lemma 35 *Let $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$ and k be the diameter of G_α. Let $\eta = x + yi$ and $\eta' = x' + y'i$ be such that $|x| + |y| \leq k$ and $|x'| + |y'| \leq k$. If $r \equiv (\eta' - \eta) \pmod{\alpha}$ is such that $|Re(r)| + |Im(r)|$ is minimum, then $r = (\eta' - \eta) + \gamma\alpha$ with*

$$\gamma \in \{0, \pm 1, \pm i, \pm(1+i), \pm(1-i), \pm 2, \pm 2i\}.$$

Proof.– We use the distance distribution introduced in Theorems 30 and 31. If $N = a^2 + b^2$ is odd, the maximum norm is obtained for vertex $\sigma = \frac{a+b-1}{2} + \frac{b-a-1}{2} i$ or any of its associates. Then, we have that

$$\mathcal{N}(\sigma) = \left(\frac{a+b-1}{2}\right)^2 + \left(\frac{b-a-1}{2}\right)^2 = \frac{a^2 + (b-1)^2}{2}.$$

Now, given $\eta = x + yi$ and $\eta' = x' + y'i$, as $r = (\eta' - \eta) + \gamma\alpha$ with $|Re(r)| + |Im(r)|$ minimum, we obtain that $\gamma\alpha = r - (\eta' - \eta)$. Applying the norm at both sides of the equality, we obtain:

$$\mathcal{N}(\gamma\alpha) = \mathcal{N}(r - (\eta' - \eta)) \leq \mathcal{N}(3\sigma) = 9\frac{a^2 + (b-1)^2}{2}.$$

Applying that the norm is multiplicative and that $\mathcal{N}(\alpha) = a^2 + b^2$, we get:

$$\mathcal{N}(\gamma) \leq \frac{9}{2}\frac{a^2 + (b-1)^2}{a^2 + b^2} < \frac{9}{2}.$$

The only possible values of γ that fulfill this inequality are

$$\{0, \pm 1, \pm i, \pm(1+i), \pm(1-i), \pm 2, \pm 2i\}.$$

If N is even, the maximum norm is achieved for vertex $\sigma = \frac{a+b}{2} + \frac{b-a}{2} i$. We have that

$$\mathcal{N}(\sigma) = \left(\frac{a+b}{2}\right)^2 + \left(\frac{b-a}{2}\right)^2 = \frac{a^2 + b^2}{2}.$$

So, with analogous steps as in the previous case we obtain the same restrictions for the norm of γ. □

Algorithm 3 presents a parallel version of the shortest path calculation for any Gaussian graph based on previous Lemma.

```
**Data**: $x + yi$: Source; $x' + y'i$: Destination; $a + bi$: graph generator
**Result**: $r_1 + r_2 i \equiv (x' - x) + (y' - y)i \pmod{a + bi}$: with $|r_1| + |r_2|$ minimum
**begin**
    $x_0 := x' - x$; $y_0 := y' - y$;
    DO IN PARALLEL:
    **begin**
        $\begin{cases} x_1 := x_0 - a; \\ y_1 := y_0 - b; \end{cases}$    $\begin{cases} x_2 := x_0 + a; \\ y_2 := y_0 + b; \end{cases}$
        $\begin{cases} x_3 := x_0 - b; \\ y_3 := y_0 + a; \end{cases}$    $\begin{cases} x_4 := x_0 + b; \\ y_4 := y_0 - a; \end{cases}$
        $\begin{cases} x_5 := x_0 + (a - b); \\ y_5 := y_0 + (a + b); \end{cases}$    $\begin{cases} x_6 := x_0 - (a - b); \\ y_6 := y_0 - (a + b); \end{cases}$
        $\begin{cases} x_7 := x_0 + (a + b); \\ y_7 := y_0 + (b - a); \end{cases}$    $\begin{cases} x_8 := x_0 - (a + b); \\ y_8 := y_0 - (b - a); \end{cases}$
        $\begin{cases} x_9 := x_0 + 2a; \\ y_9 := y_0 + 2b; \end{cases}$    $\begin{cases} x_{10} := x_0 - 2a; \\ y_{10} := y_0 - 2b; \end{cases}$
        $\begin{cases} x_{11} := x_0 - 2b; \\ y_{11} := y_0 + 2a; \end{cases}$    $\begin{cases} x_{12} := x_0 + 2b; \\ y_{12} := y_0 - 2a; \end{cases}$
    **end**
    END DO IN PARALLEL
    $(r_1, r_2) := (x_i, y_i)$ such that $|x_i| + |y_i|$ is minimum;
**end**
```

Algorithm 3: Shortest Path Calculation in Gaussian Graphs.

If we look at Algorithm 3 in detail, just sums and comparisons are needed to preform the routing in a Gaussian graph. Source vertex $x+yi$ and destination vertex $x'+y'i$ are supposed to be such that $|x|+|y| \leq k$ and $|x'|+|y'| \leq k$, where k is the diameter of the Gaussian graph. Note that to obtain the diameter we only have to check the parity of the number of vertices a^2+b^2, which just means to inspect a bit in such a number. Hence, the Step 1 to $Compute(x, y)$ in this case would have constant complexity since it only involves 12 sums and 14 comparisons.

Chapter 3

Perfect Codes over Gaussian Integers

In this Chapter, we present error-correcting codes over QAM-like constellations modeled by the Gaussian graphs previously introduced. These codes are perfect and the metric employed is the distance among vertices of the Gaussian graph which models the constellation under consideration. We are able to obtain these codes by providing a solution to a problem in Graph Theory known as the *perfect t-dominating set* computation.

The rest of this Section is organized as follows. Section 3.1 defines the Gaussian graph metric. In Section 3.2 perfect t-dominating sets are obtained which lead to the perfect codes considered in Section 3.3. Next, in Section 3.4 we introduce the concept of quotient graph of a Gaussian graph that characterizes the code distance properties. The Chapter concludes with Section 3.5 showing that the Lee metric is a particular case of the Gaussian graph metric.

3.1 The Gaussian Graph Metric

As the vertices of a Gaussian graph are, in fact, the elements of the corresponding quotient ring of the Gaussian integers, the proposed distance can be defined as:

Definition 36 *Let $0 \neq \alpha \in \mathbb{Z}[i]$. We define the* Gaussian distance *in $\mathbb{Z}[i]_\alpha$ between points β and γ, $D_\alpha(\beta,\gamma)$ as its distance in the graph G_α. With preciseness,*

$$D_\alpha(\beta,\gamma) = \min\{|x| + |y| \mid (\beta - \gamma) \equiv x + yi \pmod{\alpha}\}.$$

Obviously, D_α is a metric over the quotient ring $\mathbb{Z}[i]_\alpha$. It should be noted that the distance D_α is not the Mannheim distance defined in [37]. Moreover, the Mannheim distance is not really a metric as we show next. If $\alpha, \pi \in \mathbb{Z}[i]$ and π has odd prime norm, in [58] it is proved that there is a unique element in the class of α with minimum norm, which we denote as r_α. In addition, in [37] it is asserted that r_α can be computed as $r_\alpha = \alpha - q_\alpha \pi$ where,

$$q_\alpha := \left[\frac{\alpha\overline{\pi}}{\mathcal{N}(\pi)} \right].$$

The operation $[c + di]$ denotes rounding in Gaussian integers and is defined by $[c + di] = [c] + [d]i$ with $[c]$ denoting rounding to the closest integer. The Mannheim distance between two elements β and γ in $\mathbb{Z}[i]_\pi$ is defined in [37] as:

$$d_M(\beta, \gamma) = |x| + |y|,$$

where $x + yi = r_{\gamma-\beta}$ is the member with minimum norm of the class of $\gamma - \beta$. The next example shows that the mapping d_M is not a metric over $\mathbb{Z}[i]_\pi$ since it does not fulfil the triangular inequality.

Example 5 *Let $\pi = 7 + 12i$ be such that its norm is $\mathcal{N}(\pi) = 7^2 + 12^2 = 193$, a prime number. Consider $\mathbb{Z}[i]_\pi$ and the elements $x = 2-6i$, $z = 3+2i$ and $y = 2-5i$. It should be verified that $d_M(x, z) \leq d_M(x, y) + d_M(y, z)$, but this is not true:*

- $d_M(x, z) = 10$ *since* $6 + 4i \equiv 2 - 6i - (3 + 2i) \pmod{\pi}$ *with minimum norm.*
- $d_M(x, y) = 1$ *since* $-i \equiv 2 - 6i - (2 - 5i) \pmod{\pi}$ *with minimum norm.*
- $d_M(y, z) = 8$ *since* $-1 - 7i \equiv 2 - 5i - (3 + 2i) \pmod{\pi}$ *with minimum norm.*

3.2 Perfect t-Dominating Sets in Gaussian graphs

In this Section, we solve the perfect t-dominating set problem in Gaussian graphs. The perfect t-dominating set calculation for Hypercubes and Tori are well-known results in Coding Theory as they lead to perfect codes for Hamming and Lee metrics respectively [8]. Next, we are going to provide a sufficient condition to find perfect t-dominating sets in any Gaussian graph if they exist. Let us first introduce some definitions.

Given $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$, an integer $t > 0$ and a vertex $\eta \in G_\alpha$, we denote the *ball* of radius t centered in η embedded in G_α as

$$B_t(\eta) = \{\gamma \in G_\alpha \mid D_\alpha(\gamma, \eta) \leq t\}.$$

Then, by definition, a vertex η of G_α t-dominates vertex $\beta \in G_\alpha$ if $\beta \in B_t(\eta)$. Therefore, a perfect t-dominating set, S, constitutes a subset of the graph vertices such that the set of balls with centers in S and radii t is a disjoint partition of the vertex set. Note that if S is a perfect t-dominating set, then $S+\beta \pmod{\alpha} = \{\eta+\beta \pmod{\alpha} \mid \eta \in S\}$ is also a perfect t-dominating set and consequently, we can assume that $0 \in S$.

Remark 37 *Note that, for every $\beta \in \mathbb{Z}[i]_\alpha$ and for every $t \leq b$ we have that $B_t(\beta)$ has $2t^2+2t+1 = t^2+(t+1)^2$ elements. Hence, if there exists a perfect t-dominating set in G_α, then $2t^2+2t+1$ must divide $\mathcal{N}(\alpha) = a^2+b^2$. Nevertheless, this is not a sufficient condition for obtaining such a set. For example, $85 = 2 \cdot 6^2 + 2 \cdot 6 + 1$ divides $170 = 7^2 + 11^2$ but there is not a 6-dominating set in G_{7+11i}.*

Theorem 38 *Let $0 \neq \alpha \in \mathbb{Z}[i]$ and t be a positive integer. We have that:*

i) If $\beta = t + (t+1)i$ divides α then the ideal $S = (\beta) \subseteq \mathbb{Z}[i]_\alpha$ is a perfect t-dominating set in G_α.

ii) If $\overline{\beta} = t - (t+1)i$ divides α then the ideal $S = (\overline{\beta}) \subseteq \mathbb{Z}[i]_\alpha$ is a perfect t-dominating set in G_α.

Proof.– First note that, due to Corollary 22, S has exactly $\dfrac{a^2+b^2}{t^2+(t+1)^2}$ elements. Next, we are going to prove the first item of the Theorem. The second one follows the same procedure. We just need to prove that, if $\beta_1, \beta_2 \in S$ then $D_\alpha(\beta_1, \beta_2) \geq 2t+1$, where D_α denotes the Gaussian graph distance.

Consider $\beta_1, \beta_2 \in (\beta)$. Then, $\beta_1 = \alpha_1\beta$ and $\beta_2 = \alpha_2\beta$, with $\alpha_1, \alpha_2 \in \mathbb{Z}[i]$. We have to prove that $D_\alpha(\beta_1, \beta_2) = D_\alpha(\alpha_1\beta, \alpha_2\beta) = D_\alpha((\alpha_1 - \alpha_2)\beta, 0) \geq 2t+1$. Note that it is enough to prove that for any $\eta \in \mathbb{Z}[i]$ such that $\eta\beta \not\equiv 0 \pmod{\alpha}$ it is fulfilled that $D_\alpha(\eta\beta, 0) \geq 2t+1$. It is clear that for $\eta \in \{1, i, -1, -i\}$ we have $D_\alpha(\eta\beta, 0) = 2t+1$.

Suppose the contrary. If $D_\alpha(\eta\beta, 0) < 2t+1$ then $\eta\beta \equiv x + yi \pmod{\alpha}$, with $|x| + |y| < 2t+1$ minimum. Therefore, $\eta\beta = (x+yi) + \gamma_1\alpha = (x+yi) + \gamma_2\beta$, where γ_1, $\gamma_2 \in \mathbb{Z}[i]$, which implies $x + yi = \beta(\eta - \gamma_2)$. Now, $\mathcal{N}(x+yi) \leq 4t^2$ since $|x| + |y| \leq 2t$. As $\mathcal{N}(\beta) = 2t^2 + 2t + 1 > 2t^2$ for $t > 0$, then $\mathcal{N}(\eta - \gamma_2) < 2$. Consequently, $x + yi = \beta u$, with $u \in \{1, i, -1, i\}$. So, in any case, $|x| + |y| = 2t+1$, which is a contradiction. □

Example 6 *Let $\alpha = 6 + 8i = 2(3+4i)$. As $3+4i$ divides $6+8i$, the ideal $S = (3+4i) = \{0, 3+4i, 10+5i, 7+i\}$ is a perfect 3-dominating set of G_{6+8i}. Moreover, as $1-2i$ divides $6+8i$, the ideal $S' = (1-2i) = \{0, 5, 10, 10+5i, 11+3i, 12+6i, 9+7i, 9+2i, 12+i, 5+5i, 6+3i, 7+6i, 2+i, 1+3i, 5i, 3+4i, 13+4i, 7+i, 4+2i, 8+4i\}$ is a perfect 1-dominating set in G_{6+8i}. Note that representants of the classes of the ideals $(3+4i)$ and $(1-2i)$ of $\mathbb{Z}[i]_{6+8i}$ have been chosen in the domain $\mathcal{D}$, as it was defined in Theorem 26. Figure 3.1 illustrates these examples. Wrap-around edges have been omitted for simplicity.*

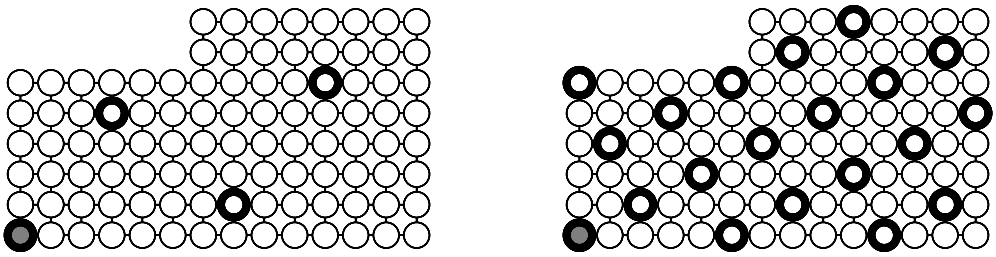

Figure 3.1: Perfect 3-dominating and 1-dominating Sets of G_{6+8i}.

Example 7 *Let* $\alpha = 6 + 7i = (1 + 2i)(4 - i)$*. As* $1 + 2i$ *divides* $6 + 7i$*, the group* $S = (1+2i) = \{1+2i, 2+4i, -3-i, -2+i, -1+3i, 5i, -5, -4+2i, 4-2i, 5, -5i, 1-3i, 2-i, 3+i, -2-4i, -1-2i, 0\}$ *is a perfect 1-dominating set in* G_{6+7i}*. Figure 3.2 illustrates this example. Note that in this case the vertices have been chosen according to Theorem 31. For the sake of the clarity the wrap-around edges are omitted in the Figure.*

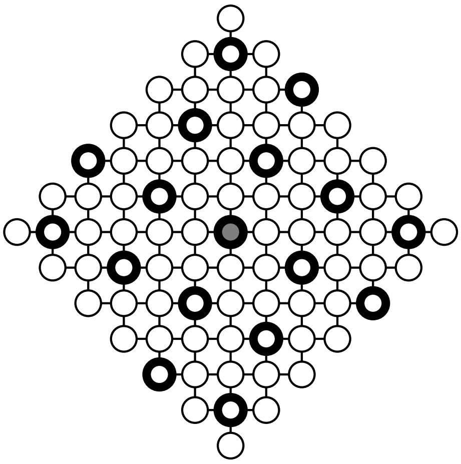

Figure 3.2: Perfect 1-Dominating Set in G_{6+7i}.

3.3 Perfect Codes over Gaussian Integers

The guidelines presented in the previous Section can be used for designing different perfect error-correcting codes over the Gaussian integers. As stated before, there is a natural way of defining perfect codes by means of perfect dominating sets over known graphs. An illustrative example for Torus graphs and the Lee metric can be seen in

Theorem 13.25 in [8]. For example, the subset $\mathcal{C} = \{(2,0),(4,1),(1,2),(3,3),(0,4)\}$ of $\mathbb{Z}_5 \times \mathbb{Z}_5$ is a perfect error 1-correcting code for the Lee metric. Therefore, this perfect code defines a perfect 1-dominating set in the corresponding Torus graph.

In our case, it is easy to define perfect codes of length 1 over Gaussian integers by using their associated Gaussian graph. Using Theorem 38, if t is a positive integer such that $t + (t+1)i$ or $t - (t+1)i$ divides α, there is a perfect t-dominating set S of G_α. Therefore, we can define a code $\mathcal{C} = S$ over $\mathbb{Z}[i]_\alpha$ whose codewords are the elements of S which form an ideal. This code of length 1 is a perfect code of minimum distance $2t+1$, in which the metric considered in the one induced by the associated Gaussian graph.

Figure 3.3 shows an example of this distance, which was introduced in Section 3.1. The distance between vertices -1 and $1+i$ in G_{3+4i} is 2 when traversing the path -1, $-1-i$, $1+i$. There is also a path -1, 0, 1, $1+i$ having length 3. Therefore, this distance should be used with the codes considered in [37] and [23] and any other codes whose words are considered over this kind of alphabets. Obviously, the definition of the distance can be extended to any n-length word as follows: if $\Lambda = [\lambda_1, \lambda_2, \ldots, \lambda_n], \Gamma = [\gamma_1, \gamma_2, \ldots, \gamma_n] \in \mathbb{Z}[i]_\alpha^n$ then,

$$D_\alpha^n(\Lambda, \Gamma) = \sum_{j=1}^{n} D_\alpha(\lambda_j, \gamma_j).$$

Furthermore, other families of codes based on the covering properties shown in this thesis can be defined. One of these codes is proposed, as an example, in the following result.

Proposition 39 *Let $\alpha = a+bi$ be such that $\gcd(a,b) = 1$. Let t be a positive integer such that $t+(t+1)i$ or $t-(t+1)i$ divides α. We denote such an exact divisor as β. We define the vector $v = [\beta, 2\beta, \ldots, (r-1)\beta] \in \mathbb{Z}[i]_\alpha^{r-1}$, where r is the order of the group generated by β. Then, the additive group generated by v, $\mathcal{C} = (v)$ is a group code with $r-1$ non zero elements over $\mathbb{Z}[i]_\alpha^{r-1}$.*

Example 8 *As we have seen in Example 7, $S = (1+2i)$ is a perfect 1-dominating group in G_{6+7i}. We consider (v), the group generated by the vector:*

$$v = [1+2i, 2+4i, -3-i, -2+i, -1+3i, 5i, -5, -4+2i, 4-2i, 5, -5i, 1-3i, 2-i, 3+i, -2-4i, -1-2i],$$

which has 16 elements. The distance of the group code generated by v is $D(v,0) = \sum_{j=1}^{16} D_\alpha(v_j, 0) = 72$.

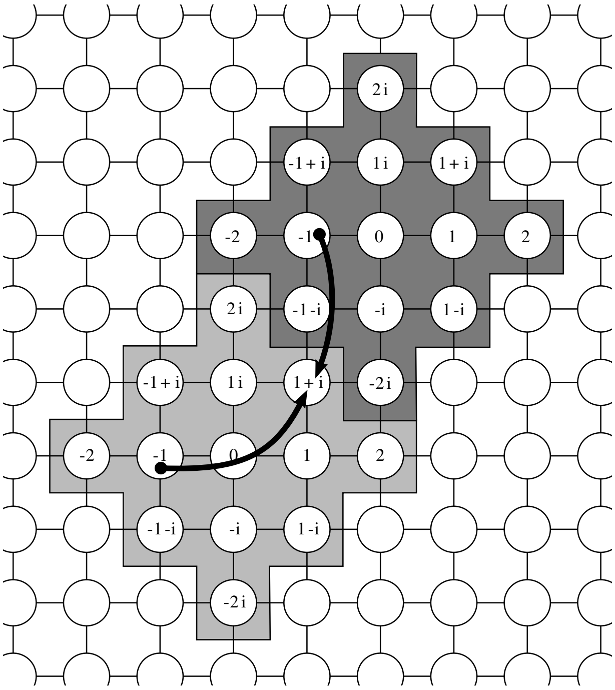

Figure 3.3: Graphical Representation of the Distance Induced by the Gaussian Graph Generated by $3 + 4i$.

3.3.1 Uniqueness Result for Perfect Ideal Codes

The problem of characterizing all perfect codes is an interesting research which has been considered for all the well-known metrics in Coding Theory. For example, in [8] perfect codes of length 1 for the Lee metric were characterized. In a similar way, here we provide a uniqueness result for perfect t-error correcting ideal codes of length 1 over $\mathbb{Z}[i]_\alpha$ in Theorem 41. For this purpose we need to introduce the following Lemma:

Lemma 40 *Let t be a positive integer and $\alpha \in \mathbb{Z}[i]$. For every $\eta \in \mathbb{Z}[i]_\alpha$ we have that*

$$B_t(\eta) \cap B_t(0) = \emptyset \;\Leftrightarrow\; D_\alpha(\eta, 0) \geq 2t + 1.$$

Proof.– First, let η be such that $D_\alpha(\eta, 0) \geq 2t + 1$ and suppose that there exists a vertex $\gamma \in B_t(\eta) \cap B_t(0)$, that is $D_\alpha(\eta, \gamma) \leq t$ and $D_\alpha(\beta, \gamma) \leq t$. Therefore, $2t + 1 \leq D_\alpha(\eta, \beta) \leq D_\alpha(\eta, \gamma) + D_\alpha(\beta, \gamma) \leq 2t$, which is a contradiction.

Finally, let η be such that $B_t(\eta) \cap B_t(0) = \emptyset$ and suppose the contrary, that is, $D_\alpha(\eta, 0) \leq 2t$. We have to prove that $B_t(\eta) \cap B_t(0) \neq \emptyset$. It is clear that if we prove that $B_t(\eta) \cap B_t(0) \neq \emptyset$ for η with $D_\alpha(\eta, 0) = 2t$, we have proven the result for any η' with $D_\alpha(\eta', 0) \leq 2t$. Hence, without loss of generality we can suppose that $D_\alpha(\eta, 0) = 2t$. Then, there exists a representant β of the class of η with $\beta = x + yi$, with $|x| + |y| = 2t$ minimum.

Let us analyze the cases in which $x, y \geq 0$; the others can be solved analogously. Then, we have that $0 \leq x \leq 2t$ and $y = 2t - x$. As $x + y \equiv 0 \pmod 2$, we have that $x \equiv y \pmod 2$. If $x \equiv y \equiv 0 \pmod 2$, then $\gamma = \frac{a}{2} + \frac{b}{2}i \in \mathbb{Z}[i]_\alpha$ and $D_\alpha(0, \gamma) = t = D_\alpha(\eta, \gamma)$. This is a contradiction.

If $x \equiv y \equiv 1 \pmod 2$, then $\gamma = \dfrac{a-1}{2} + \dfrac{b+1}{2}i \in \mathbb{Z}[i]_\alpha$ and $D_\alpha(0, \gamma) = t = D_\alpha(\eta, \gamma)$. This is also a contradiction. □

Hence, using Corollary 22 and the previous Lemma we can prove the following:

Theorem 41 *Let $\alpha = a + bi$ and t a positive integer. If there exists a perfect t-error correcting* ***ideal*** *code $\mathcal{C}$ of length 1 over $\mathbb{Z}[i]_\alpha$, then it must be the ideal generated by $t + (t+1)i$ or $t - (t+1)i$.*

Proof.– Since $\mathcal{C}$ is a perfect t-error correcting code over $\mathbb{Z}[i]_\alpha$, it has cardinal $\dfrac{a^2 + b^2}{t^2 + (t+1)^2}$. Since we are in a Principal Ideal Domain, $\mathcal{C}$ must be generated by an element $\beta = x + yi \in \mathbb{Z}[i]$ such that β divides α, Moreover, this element must satisfy, according to Corollary 22, that the cardinal number $\#\mathcal{C}$ equals $\dfrac{\mathcal{N}(\alpha)}{\mathcal{N}(\beta)}$, which implies $x^2 + y^2 = t^2 + (t+1)^2$.

Now, we prove that necessarily $|x| + |y| = 2t + 1$. If $|x| + |y| < 2t + 1$, we have that $D_\alpha(\beta, 0) \leq |x| + |y| < 2t + 1$ and, by Lemma 40, $B_t(\beta) \cap B_t(0) \neq \emptyset$. This is a contradiction since 0 and β belong both to $\mathcal{C}$. Next, if we suppose that $|x| + |y| > 2t + 1$, we get

$$|x| + |y| > 2t + 1,$$
$$x^2 + y^2 = t^2 + (t+1)^2.$$

Then, $|x| > 2t + 1 - |y|$ which implies $|x|^2 > (2t+1)^2 - 2(2t+1)|y| + |y|^2$. According to the second equation we have that $t^2 + (t+1)^2 = x^2 + y^2 > (2t+1)^2 - 2(2t+1)|y| + |y|^2 + |y|^2$. This is equivalent to $0 > t(t+1) - (2t+1)|y| + |y|^2 = (|y| - (t+1))(|y| - t)$, which is also a contradiction as y and t are integers. So, necessarily $|x| + |y| = 2t + 1$. Hence, $\beta = x + yi$ with

$$|x| + |y| = 2t + 1,$$
$$x^2 + y^2 = t^2 + (t+1)^2.$$

It is easy to prove that this implies $\beta = x + yi$ with $|x| = t$ and $|y| = t + 1$ or $|x| = t + 1$ and $|y| = t$, from where we get that $\beta = t + (t+1)i$ or $\beta = t - (t+1)i$. □

The previous uniqueness result is just for codes that are ideals of the corresponding quotient ring. However, we conjecture that the perfect dominating sets obtained in Theorem 38 are the only ones that can be obtained on these graphs. Specifically,

Conjecture 42 *Let $0 \neq \alpha \in \mathbb{Z}[i]$ and t be a positive integer such that there exists a perfect t-dominating set S of G_α with $0 \in S$. Then, S must be an ideal of $\mathbb{Z}[i]_\alpha$.*

3.4 Quotient Graphs and Code Distance Properties

In this Section, we define the *quotient graph* of a Gaussian graph, which will be useful to study the distance-related properties of the codes presented in the previous Section. Other definitions of quotient graphs can be found in the study of crystallographic nets, which form finite graphs from infinite nets [43]. In our case, we define the quotient Gaussian graph as follows.

Definition 43 *Let $0 \neq \alpha \in \mathbb{Z}[i]$ be such that there exists a positive integer t such that $t + (t+1)i$ or $t - (t+1)i$ divides α. Let β denote such exact divisor and G_α be the Gaussian graph generated by α. We define the quotient graph of G_α by β, $\dfrac{G_\alpha}{\beta} = (V, E)$ as follows:*

- *The ideal $V = (\beta)$ is the set of vertices.*
- *$E = \{(\gamma_1, \gamma_2) \in V \times V \mid D_\alpha(\gamma_1, \gamma_2) = 2t + 1\}$ is the set of edges, where D_α is the graph distance in G_α.*

Although the Definition could appear a bit cryptic, the idea of constructing such a graph is very simple. If there is a perfect code over $\mathbb{Z}[i]_\alpha$, we build a graph whose vertices are the codewords and the adjacency pattern is determined by the minimum distance of the code, that is, codewords of adjacent balls are connected by an edge. Note that $\dfrac{G_\alpha}{\beta}$ is regular of degree four since S is perfect. Moreover, we have the following:

Theorem 44 *Let $0 \neq \alpha \in \mathbb{Z}[i]$ be such that there exists a positive integer t such that $t + (t+1)i$ or $t - (t+1)i$ divides α. Let β denote such exact divisor. Then, the graphs $\dfrac{G_\alpha}{\beta}$ and $G_{\frac{\alpha}{\beta}}$ are isomorphic.*

Proof.– Since $S = (\beta) \subseteq \mathbb{Z}[i]_\alpha$ consider the graph isomorphism:

$$\begin{array}{rccc} \phi: & \mathbb{Z}[i]_{\frac{\alpha}{\beta}} & \longrightarrow & S \subset \mathbb{Z}[i]_\alpha \\ & \gamma & \longmapsto & \gamma \cdot \beta \pmod{\alpha} \end{array}$$

□

Therefore, the product of the minimum distance of the code and the diameter of the quotient graph is an upper bound of the maximum distance of the perfect code. The same happens with the average distance. Next Corollary states this result and Example 9 illustrates it.

Corollary 45 *Let $0 \neq \alpha \in \mathbb{Z}[i]$ be such that there exists a positive integer t such that $t+(t+1)i$ or $t-(t+1)i$ divides α. Let β denote such exact divisor and $\mathcal{C} = (\beta)$ be the Gaussian code generated by β. Also, let G_α denote the Gaussian graph generated by α and $\dfrac{G_\alpha}{\beta}$ the quotient graph of G_α by β. We denote the maximum distance of $\mathcal{C}$ as $max(\mathcal{C})$ and its average distance as $avg(\mathcal{C})$. Then, if k denotes the diameter of $\dfrac{G_\alpha}{\beta}$ and $\overline{k}$ its average distance, we have that:*

- *$max(\mathcal{C}) \leq (2t+1)k$.*
- *$avg(\mathcal{C}) \leq (2t+1)\overline{k}$.*

Note that k and $\overline{k}$ of previous Corollary can be calculated using Corollaries 33 and 34 from Chapter 2.

Example 9 *Let $\alpha = 6+7i = (4-i)(1+2i)$. Since $1+2i$ divides α we have seen that the ideal generated by $1+2i$ forms a perfect 1-correcting code over $\mathbb{Z}[i]_\alpha$. Using Theorem 44 the quotient graph G_{4-i} is isomorphic to G_{1+4i}. Hence, the diameter of this graph is $k = 3$ and its average distance is $\overline{k} = 2$. Also, the maximum distance of the code is 6 and its average distance is 4.5. Figures 3.5 and 3.4 illustrate the quotient graphs and the code considered in this example for the two graph representations considered in this work.*

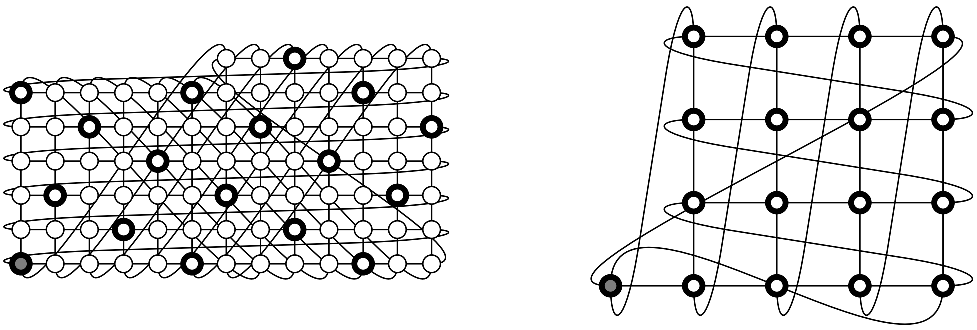

Figure 3.4: Perfect Code over $\mathbb{Z}[i]_{6+7i}$ and Quotient Graph $\frac{G_{6+7i}}{1+2i}$.

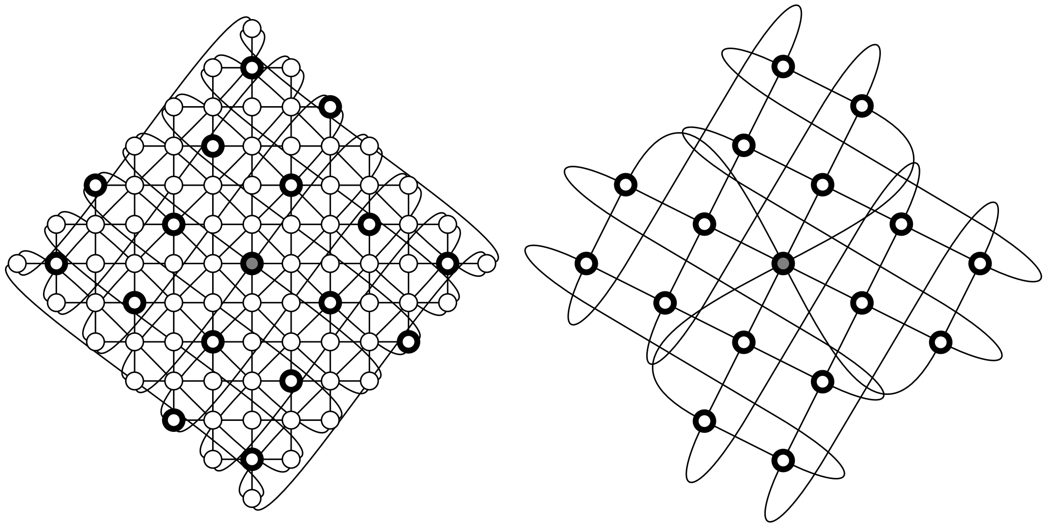

Figure 3.5: Perfect Code over $\mathbb{Z}[i]_{6+7i}$ and Quotient Graph $\frac{G_{6+7i}}{1+2i}$.

3.5 Perfect Lee-Codes over Gaussian Integers

An important subcase of the previous study is when $\alpha = b$ or $\alpha = bi$, with $0 \neq b \in \mathbb{Z}$. According to Theorem 29, in this case the Gaussian graph induced by α is a Torus. It is known that the Lee distance defined over $\mathbb{Z}_N \times \mathbb{Z}_N$ can be seen as the graph distance in a N^2-vertices Torus whose vertices are labeled by means of $\mathbb{Z}_N \times \mathbb{Z}_N$ [8], [12]. So, for these particular cases, the Gaussian distance considered in this paper is, actually, the Lee distance. In conclusion, the perfect codes obtained by Golomb in [30] which are broadly discussed by Berlekamp in [8] can be seen as a particular subcase of Theorem 38. Next, we introduce these results obtained by Golomb as they appear in [8].

Theorem 46 *For any given t, there exists a perfect t-Lee correcting code of block length $n = 2$ over the alphabet $\mathbb{Z}_q$, where $q = 2t^2 + 2t + 1$. This code may be taken as the negacyclic code generated by $g(x) = x + (2t + 1)$.*

Corollary 47 *If $2t^2 + 2t + 1$ divides q, there exists a perfect t-Lee correcting code of length $n = 2$ over the alphabet of $\mathbb{Z}_q$.*

The perfect t-error correcting code from Theorem 46 uses the Lee distance in $\mathbb{Z}_{2t^2+2t+1} \times \mathbb{Z}_{2t^2+2t+1}$ and has $2t^2 + 2t + 1$ words. In fact, as stated in Theorem 41, this code coincides with the code built over the Gaussian graph G_{2t^2+2t+1}, with $\mathcal{C} = (\beta)$ and $\beta = t + (t + 1)i$. In this case, G_{2t^2+2t+1} is, actually, a Torus of side $2t^2 + 2t + 1$.

However, this code is essentially different to the code built over $\mathbb{Z}[i]_{\beta^2}$ with $\mathcal{C}' = (\beta)$, that has the same number of codewords but different maximum distances. In Example 10 we study some of these different codes.

Example 10 *Let us consider now $N = 625$ which can be expressed as the norm of the three Gaussian integers $\alpha_1 = 25$, $\alpha_2 = 7 - 24i$ and $\alpha_3 = 15 + 20i$, all of them having the common divisor $3 + 4i$. Consequently, we can explore the three possibilities that correspond to three different Gaussian graphs and, a priori, three different perfect codes. If such codes exist, all of them would be ideals generated by the same divisor, but over different rings. Let us study the three cases.*

First, when $\alpha_1 = 25 = (3+4i)(3-4i)$, the ideal $(3+4i)$ in $\mathbb{Z}[i]_{\alpha_1}$ is a perfect 3-error correcting code by Theorem 38. Figure 3.6 shows this perfect code over $\mathbb{Z}[i]_{\alpha_1}$, where highlighted points represent the codewords. This code coincides with the Golomb code for the Lee metric over $\mathbb{Z}_{25} \times \mathbb{Z}_{25}$, as reflected in [8]. Its maximum distance is 21 and its average distance 13.

Second, as $3 + 4i$ divides $\alpha_2 = 7 - 24i = (3 + 4i)(-3 - 4i)$, we have that the ideal $(3 + 4i)$ in $\mathbb{Z}[i]_{\alpha_2}$ is a perfect 3-error correcting code. Figure 3.7 shows this perfect code over $\mathbb{Z}[i]_{7-24i}$, which has maximum distance 20 and average distance 12.83.

Finally, as $3+4i$ also divides $\alpha_3 = 15+20i = (3+4i)5$, the ideal generated by $3+4i$ in $\mathbb{Z}[i]_{\alpha_3}$ is also a perfect 3-error correcting code. Figure 3.8 shows such a perfect code over $\mathbb{Z}[i]_{15+20i}$, which has maximum distance 16 and average distance 12.16.

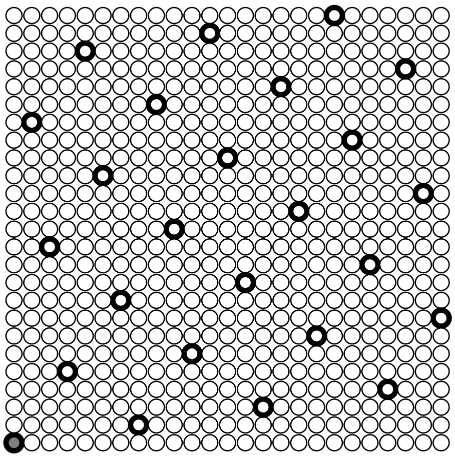

Figure 3.6: Perfect Code over $\mathbb{Z}[i]_{25}$.

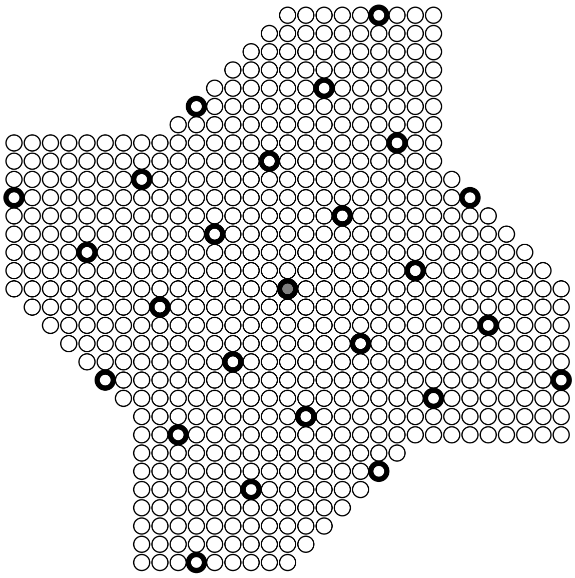

Figure 3.7: Perfect Code over $\mathbb{Z}[i]_{7-24i}$.

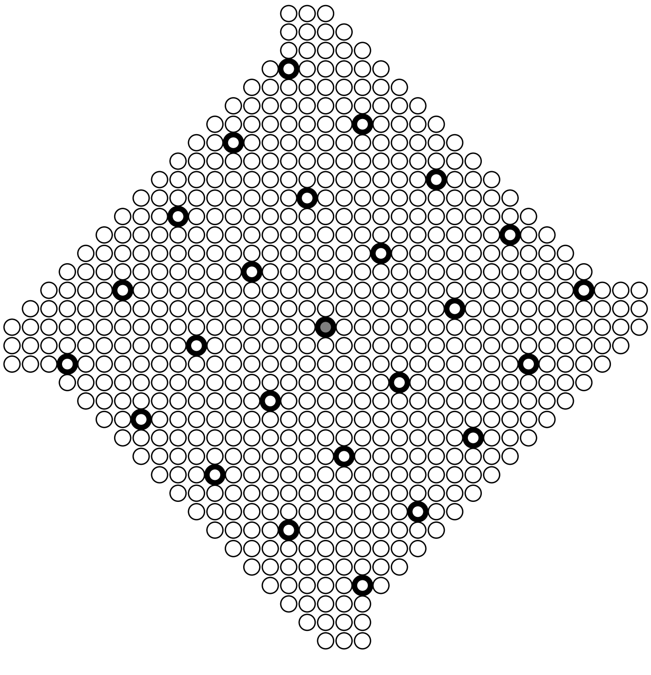

Figure 3.8: Perfect Code over $\mathbb{Z}[i]_{15+20i}$.

The codes obtained for α_1 and α_2 have isomorphic quotient graphs. Note that both quotients, $(-3-4i)$ and $(3-4i)$, generate the same Gaussian graph G_{3+4i} whose vertices are the codewords. Nevertheless, in the case of α_3, its factor 5 leads to the quotient graph G_5. Figure 3.9 shows a representation of the quotient graphs G_{3+4i} and G_5.

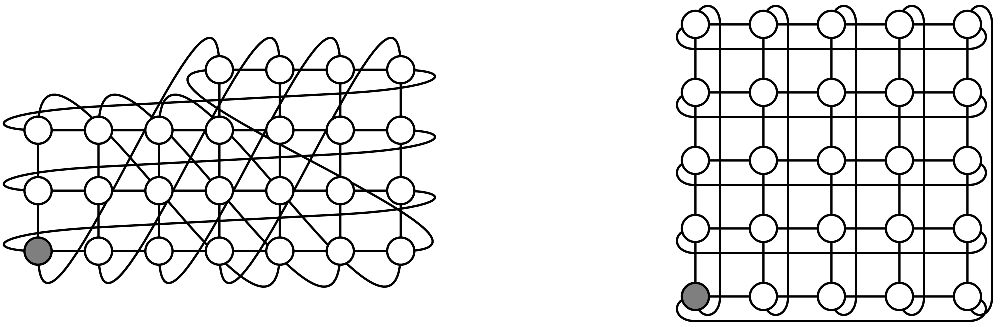

Figure 3.9: G_{3+4i} and G_5.

Some other interesting examples in which $N = c^2 = a^2 + b^2$, with N being the cardinal of the alphabet, can be considered. Note that any triplet $(a, b, c) \in \mathbb{Z}$ such that $c^2 = a^2 + b^2$ is a *Pythagorean triplet*. We can build different Gaussian perfect codes over them with the same error-correction capacity but with different maximum and average distances among codewords. Concerning the codes in Corollary 47, they coincide with the codes built over the quotient ring $\mathbb{Z}[i]_{(2t^2+2t+1)K}$, for any integer K, choosing $C = (\beta)$ with $\beta = t + (t+1)i$.

Chapter 4

Graphs and Codes over Eisenstein-Jacobi Integers

The methodology described in the previous Chapters for Gaussian graphs can also be applied to define perfect codes over hexagonal constellations. In these constellations, every signal point has six other neighbor points at distance one, which makes them suitable to be modeled by the ring of the Eisenstein-Jacobi integers [39]. Here, we introduce a new family of degree six Cayley graphs whose vertices are labeled by the elements of quotient rings of Eisenstein-Jacobi integers. As a consequence, perfect codes over these rings can be defined by solving again a problem of vertex domination over the resulting graphs.

The rest of the Chapter is organized as follows. Section 4.1 introduces some results about quotient rings of Eisenstein-Jacobi integers. In Section 4.2, Eisenstein-Jacobi graphs are defined and their relation with circulant graphs of degree six is stated. In Section 4.3, the problem of finding perfect t-dominating sets over Eisenstein-Jacobi graphs is solved which leads to the definition of perfect codes over hexagonal signal constellations.

4.1 Quotients of Eisenstein-Jacobi Integers

The ring of the *Eisenstein-Jacobi integers* (EJ-integers for short) is defined as:

$$\mathbb{Z}[\rho] = \{x + y\rho \mid x, y \in \mathbb{Z}\},$$

where $\rho = \frac{-1+\sqrt{-3}}{2}$. It is easy to see that ρ is such that $\rho^2 + \rho + 1 = 0$. It can be proved that $\mathbb{Z}[\rho]$ is an Euclidean domain with norm (see Proposition 1.4.2. in [41]):

$$\begin{array}{rccc} \mathcal{N}: & \mathbb{Z}[\rho] & \longrightarrow & \mathbb{Z}^+ \\ & x + y\rho & \longmapsto & x^2 + y^2 - xy \end{array}$$

Note that $\mathcal{N}(x+y\rho) = (x+y\rho)\overline{(x+y\rho)}$ since $\overline{(x+y\rho)} = (x-y) - y\rho$. Remember that the units of $\mathbb{Z}[\rho]$ are the elements with unitary norm, that is $\{\pm 1, \pm\rho, \pm\rho^2\}$.

For every $0 \neq \alpha \in \mathbb{Z}[\rho]$ we can consider $\mathbb{Z}[\rho]_\alpha = \{\beta \pmod{\alpha} \mid \beta \in \mathbb{Z}[\rho]\}$. Analogously to the Gaussian case, it can be obtained that:

Theorem 48 *Let $0 \neq \alpha \in \mathbb{Z}[\rho]$. Then, $\mathbb{Z}[\rho]_\alpha$ has $\mathcal{N}(\alpha)$ elements.*

Moreover, we have the following result.

Theorem 49 *Let $\alpha = a + b\rho \in \mathbb{Z}[\rho]$ and consider $N = \mathcal{N}(\alpha)$. Then, $\mathbb{Z}_N$ and $\mathbb{Z}[\rho]_\alpha$ are isomorphic rings if and only if* $\gcd(a,b) = 1$.

Proof.– We address this proof since we have not found it in the literature. We will prove that the mapping:

$$\begin{array}{rccc} f: & \mathbb{Z}_N & \longrightarrow & \mathbb{Z}[\rho]_\alpha \\ & n & \longmapsto & n \pmod{\alpha} \end{array}$$

is a ring isomorphism.

f is well-defined: Let $n \equiv m \pmod{N}$. Then, $r \in \mathbb{Z}$ exists such that $n - m = rN = r\alpha\overline{\alpha}$, so $n \equiv m \pmod{\alpha}$.

f is injective: Let $n \equiv m \pmod{\alpha}$. Then, $\gamma = x + y\rho \in \mathbb{Z}[\rho]$ exists such that $n - m = \gamma\alpha = (x+y\rho)(a+b\rho) = (ax - by) + (bx + (a-b)y)\rho$, from where we obtain the equations:

$$\left\{ \begin{array}{l} ax - by = n - m \\ bx + (a-b)y = 0 \end{array} \right.$$

From the second equation we infer that $\{(x,y) = ((a-b)t, -bt) \mid t \in \mathbb{Z}\}$ since $\gcd(a,b) = 1$. Now, by substituting this value in the first equation we get that $n - m = a(a-b)t - b(-bt) = (a^2 + b^2 - ab)t = t\mathcal{N}(a + b\rho) = tN$, so $n \equiv m \pmod{N}$, as we wished to prove.

f is surjective: Let $\gamma = x + y\rho \in \mathbb{Z}[\rho]_\alpha$. We have to show that $n \in \mathbb{Z}_N$ exists such that $n \equiv \gamma \pmod{\alpha}$, or similarly, a couple of integers (x_0, y_0) exists such that $(x + y\rho) + (x_0 + y_0\rho)(a + b\rho)$ is an integer. For this purpose, the ρ-part must be zero, that is

$$bx_0 + (a-b)y_0 = -y,$$

which always has a solution since $\gcd(a,b) = 1$ by hypothesis. □

As a consequence of previous Theorems we can straightforwardly obtain the following result:

Corollary 50 *Let* $0 \neq \alpha = a + b\rho \in \mathbb{Z}[\rho]$.

i) Let $\beta \in \mathbb{Z}[\rho]$ *such that* β *divides* α. *Then, the ideal generated by* β, $(\beta) \subseteq \mathbb{Z}[\rho]_\alpha$ *has* $\dfrac{\mathcal{N}(\alpha)}{\mathcal{N}(\beta)}$ *elements.*

ii) Let $\beta \in \mathbb{Z}[\rho]$ *such that* β *does not divide* α *and* $\eta = \gcd(\beta, \alpha)$. *Then, the ideal* $(\beta) \subseteq \mathbb{Z}[\rho]_\alpha$ *is generated by* η *and has* $\dfrac{\mathcal{N}(\alpha)}{\mathcal{N}(\eta)}$.

4.2 Definition of Eisenstein-Jacobi Graphs

Next, we define a new family of graphs in terms of the EJ-integers. These graphs are also Cayley graphs over quotient rings of the EJ-integers and therefore, connected and vertex-symmetric. Moreover, we can define a metric over these quotient rings of EJ-integers induced by the distance among vertices in this family of graphs. Also, we give some distance-related properties of these graphs which, in some cases, coincide with other previously considered degree-six circulants, [2], [69].

Definition 51 *Let* $\alpha = a + b\rho \in \mathbb{Z}[\rho]$ *and consider* $\mathbb{Z}[\rho]_\alpha$. *We denote the* Eisenstein-Jacobi graph *(EJ-graph for short) generated by* α *as* $EJ_\alpha = (V, E)$ *which is defined as follows:*

- $V = \mathbb{Z}[\rho]_\alpha$ *is the set of vertices, and*
- $E = \{(\beta, \gamma) \in V \times V \mid (\gamma - \beta) \equiv \pm 1, \pm\rho, \pm\rho^2 \pmod{\alpha}\}$ *is the set of edges.*

Example 11 *Let* $\alpha = 3 + 4\rho$. *Figure 4.1 shows a representation of the EJ-graph generated by* α.

Note that any EJ-graph is a regular graph of degree six since every vertex is adjacent to exactly six other vertices. Moreover, some of these graphs are degree six circulant graphs as the next result proves.

Theorem 52 *Let* $\alpha = a + b\rho \in \mathbb{Z}[\rho]$ *be such that* $\gcd(a, b) = 1$ *and* $N = \mathcal{N}(\alpha)$. *Then, the graphs* EJ_α *and* $C_N(a, b, a - b)$ *are isomorphic.*

Proof.– An integer n can be represented in the form $n \equiv bx - ay \pmod{N}$ because $\gcd(a, b) = 1$. We will prove that the ring homomorphism defined as

$$\begin{array}{rccc} \Phi : & \mathbb{Z}_N & \longrightarrow & \mathbb{Z}[\rho]_\alpha \\ & n \equiv bx - ay \pmod{N} & \longmapsto & x + y\rho \pmod{\alpha} \end{array} \tag{4.1}$$

is a graph isomorphism.

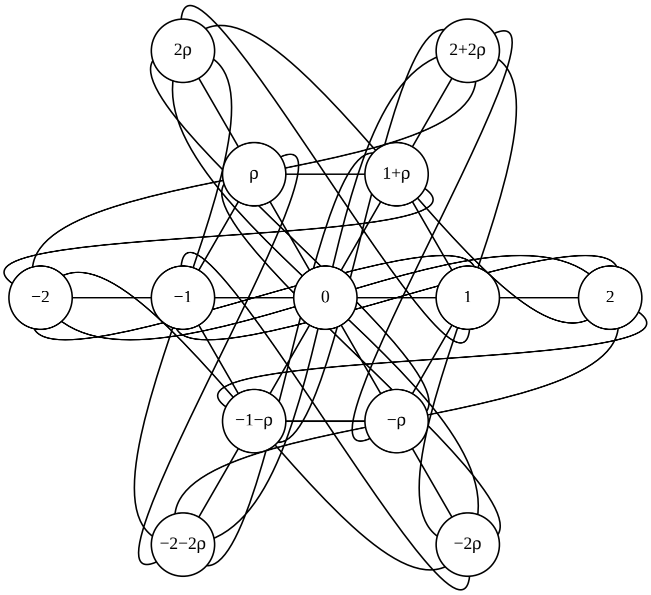

Figure 4.1: $EJ_{3+4\rho}$.

Φ is well defined: If $bx - ay \equiv 0 \pmod N$, then $k, t \in \mathbb{Z}$ exist such that

$$\begin{cases} x &= k(a+b) + at \\ y &= k(2b-a) + bt \end{cases}$$

Then, $\Phi(bx - ay) = x + y\rho = k((a+b) + (2b-a)\rho) + t(a+b\rho) = k(1-\rho)(a+b\rho) + t(a+b\rho) \equiv 0 \pmod \alpha$.

Φ is injective: Now, if $\Phi(bx - ay) = x + y\rho \equiv 0 \pmod \alpha$, then $c, d \in \mathbb{Z}$ exist such that $x + y\rho = (ac - db) + (ad + bc - db)\rho$, so

$$\begin{cases} x &= ac - bd \\ y &= ad + bc - db \end{cases}$$

from where we obtain that $bx - ay = -d(a^2 + b^2 - ab) = -dN \equiv 0 \pmod N$.

Finally, since both sets have the same number of elements, Φ is a bijection. Now, if two nodes j, h are adjacent in the circulant, then $j - h \equiv \pm a, \pm b, \pm(a-b) \pmod N$. Hence, $\Phi(j) - \Phi(h) = \Phi(j - h) \equiv \pm\Phi(a), \pm\Phi(b), \pm\Phi(a-b)$. Since $\Phi(a) = \rho$, $\Phi(b) = -1$ and $\Phi(a-b) = \Phi(a) - \Phi(b) = 1 + \rho$, then $\Phi(j)$ and $\Phi(h)$ are adjacent nodes in EJ_α. □

Remark 53 *The mapping (4.1) can be rewritten as*

$$\begin{array}{rccc} \Phi_1 : & \mathbb{Z}_N & \longrightarrow & \mathbb{Z}[\rho]_\alpha \\ & n \equiv bx - ay + (a-b)z & \longmapsto & x + y\rho + z\rho^2 \end{array} \tag{4.2}$$

since we have $n \equiv bx - ay + (a-b)z \equiv b(x-z) - a(y-z) \equiv bx' - ay' \pmod{N}$*, where* $x' = x - z$*,* $y' = y - z$*. On the other hand,* $x + y\rho + z\rho^2 \pmod{\alpha} \equiv (x-z) + (y-z)\rho \pmod{\alpha} \equiv x' + y'\rho \pmod{\alpha}$*.*

In particular, one can choose a representation $n \equiv bx - ay + (a-b)z \pmod{N}$ *in such a manner, that the sum* $|x| + |y| + |z|$ *is minimal. Thus, this value is the distance between a vertex* n *and vertex* 0 *in the graph* $C_N(a, b, a-b)$*.*

In [39] a distance in certain quotients of Eisenstein-Jacobi integers is defined. On the other hand, the preceding graph isomorphisms allows us to define a distance over $\mathbb{Z}[\rho]_\alpha$, which is the distance induced by the EJ_α graph. This distance can be expressed as:

Lemma 54 *Let* $0 \neq \alpha = a + b\rho \in \mathbb{Z}[\rho]$*. We denote the distance between vertices* β *and* γ *in* EJ_α *as* $D_\alpha(\beta, \gamma)$*. This distance can be expressed as:*

$$D_\alpha(\beta, \gamma) = \min\{|x| + |y| + |z| \mid x + y\rho + z\rho^2 \equiv (\gamma - \beta) \pmod{\alpha}\}.$$

Proof.– Theorem 52 and Remark 53 guaranty that the EJ-graph distance can be rewritten in terms of the distance of its isomorphic circulant graph. □

Example 12 *Let* $\alpha = 3 + 4\rho$*. Figure 4.2 illustrates the distance between points* -1 *and* $2 + 2\rho$ *in* $\mathbb{Z}[\rho]_{3+4\rho}$ *induced by* $EJ_{3+4\rho}$*. Obviously, the distance between those points in* $\mathbb{Z}[\rho]$ *is 3. However, if we consider their distance in* $\mathbb{Z}[\rho]_{3+4\rho}$ *we have that* $D_{3+4\rho}(-1, 2 + 2\rho) = 1$*.*

There is not much in the literature about degree six circulant graphs. Most relevant results about these graphs have been considered in [69] and [2]. In [69], the author focuses on cases in which the number of vertices is $N = 3k^2 + 3k + 1$ and graphs defined as $C_N(1, 3k+1, 3k+2)$, where k is the diameter. Note that it is easy to infer that the dense EJ-graph with diameter k is $EJ_{k+(2k+1)\rho}$. The next result shows that this specific family of graphs is contained in the family of EJ-graphs.

Theorem 55 *Let* k *be a positive integer and* $N = 3k^2 + 3k + 1$*. Then* $C_N(1, 3k+1, 3k+2) \cong EJ_{k+(2k+1)\rho}$*.*

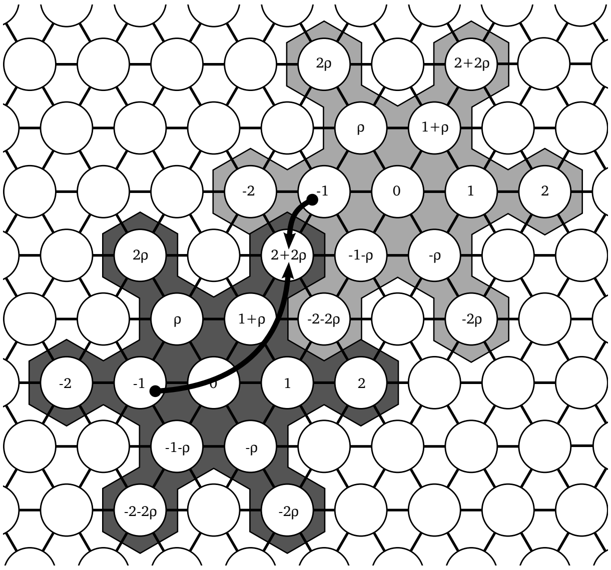

Figure 4.2: Distance $D_{3+4\rho}$ between Points -1 and $2+2\rho$.

Proof.– According to Theorem 52, $EJ_{k+(2k+1)\rho} \cong C_N(k, k+1, 2k+1)$. The isomorphism mapping between the graphs $C_N(1, 3k+1, 3k+2)$ and $C_N(k, k+1, 2k+1)$ is defined as the ring automorphism $f : \mathbb{Z}_N \longrightarrow \mathbb{Z}_N$ defined as $f(1) = k$. □

In [2], the authors focus on degree six circulants defined as $C_N(a, b, a+b)$ for any number of vertices N with $0 < a < b < \lfloor \frac{N}{2} \rfloor$ and they study some cases in which this definition minimizes the graph diameter. This family clearly contains our EJ-graphs when they are circulants.

After dealing with circulant EJ-graphs, a natural step forward is to analyze the structure of EJ-graphs when $0 \neq \alpha = a + b\rho$ with $\gcd(a, b) \neq 1$. The problem of completely characterize these graphs would be a future research topic. In Figure 4.3 a particular case for $a = 0$ is shown. We can also assert that the only case in which an EJ-graph is circulant is when $\gcd(a, b) = 1$ since that is the only case in which $\mathbb{Z}[\rho]_\alpha$ is cyclic.

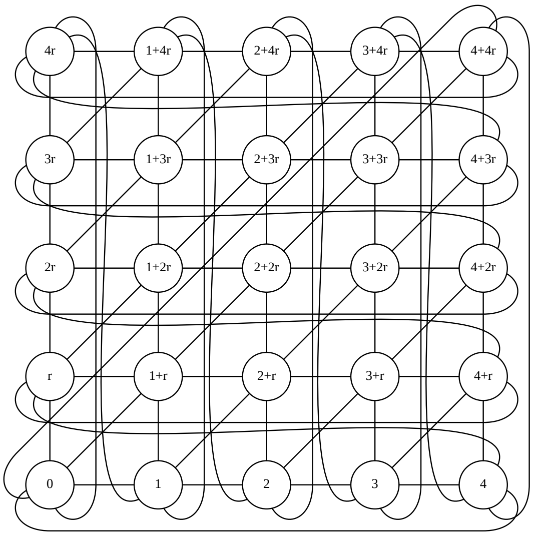

Figure 4.3: EJ-graph for $\alpha = 5\rho$.

4.3 Codes Over Quotient Rings of Eisenstein-Jacobi Integers

In this Section we study the existence of perfect t-dominating sets on EJ-graphs. Analogously as in the Gaussian case, these sets directly yield to the construction of perfect codes over quotient rings of EJ-integers respect to the associated graph distance. Moreover, such dominating sets are ideals of $\mathbb{Z}[\rho]_\alpha$ and therefore the resulting codes are *ideal codes*. Let us to introduce first some previous definitions.

Given $0 \neq \alpha = a + b\rho \in \mathbb{Z}[i]$, a vertex $\eta \in EJ_\alpha$ and an integer $0 < t \leq k$ (where k denotes the diameter of EJ_α), we denote the ball of radius t centered in η embedded in EJ_α as

$$B_t(\eta) = \{\gamma \in EJ_\alpha \mid D_\alpha(\gamma, \eta) \leq t\}.$$

The cardinality of any $B_t(\beta)$ embedded in an EJ_α graph is $1+\sum_{d=1}^{t} 6d = 3t^2+3t+1$. Again, if there exists a perfect t-dominating set over EJ_α then $3t^2 + 3t + 1$ must divide $\mathcal{N}(\alpha)$. However, this is not enough for the existence of a perfect dominating set as the following example shows.

Example 13 *Let $\alpha = 1 + 10\rho$. According to Theorem 52 this graph is isomorphic to the degree six circulant graph $C_{91}(1, 9, 10)$. It is easy to see that the number of vertices of this graph equals the cardinal of the ball of radii $t = 5$, since $91 = 3t^2 + 3t + 1$. However, this graph has diameter 6, which implies that there not exists a trivial perfect dominating set for $t = 5$, since there are, at least, one vertex at a distance greater than 5.*

Now, the next Theorem states a sufficient condition for the existence of a perfect t-dominating set in an EJ-graph containing vertex zero.

Theorem 56 *Let $0 \neq \alpha = a + b\rho \in \mathbb{Z}[\rho]$ and t be a positive integer.*

i) If $\beta = t + (2t+1)\rho$ divides α then the ideal $S = (\beta) \subseteq \mathbb{Z}[\rho]_\alpha$ is a perfect t-dominating set in EJ_α.

ii) If $-\overline{\beta} = (t+1) + (2t+1)\rho$ divides α then the ideal $S = (-\overline{\beta}) = (\overline{\beta}) \subseteq \mathbb{Z}[\rho]_\alpha$ is a perfect t-dominating set in EJ_α.

Proof.– We are going to prove the first item of the Theorem. The second one follows the same procedure.

Due to Corollary 50, the ideal (β) has $\dfrac{\mathcal{N}(\alpha)}{\mathcal{N}(\beta)}$, whit $\mathcal{N}(\beta) = 3t^2 + 3t + 1$.

First of all, we prove that $\beta = t + (2t+1)\rho$ is such that $D_\alpha(\beta, 0) = 2t+1$. Obviously, since $\beta \equiv (t+1)\rho + t(1+\rho) \pmod{\alpha}$ with $|t+1| + |t| = 2t+1$ we have that $D_\alpha(\beta, 0) \leq 2t+1$. Next, we show that this distance is exactly $2t+1$. If not, $\beta \equiv x + y\rho + z\rho^2 \pmod{\alpha}$ such that $|x| + |y| + |z| \leq 2t$. Therefore, there exists $\eta \in \mathbb{Z}[\rho]$ such that $\eta\beta = x + y\rho + z\rho^2$ in $\mathbb{Z}[\rho]$. Since $\mathcal{N}(\beta) > 3t^2$ and $\mathcal{N}(x + y\rho + z\rho^2) \leq 24t^2$ we have that $\mathcal{N}(\eta) < 8$. Now, if $\eta = c + d\rho$ with $c, d \in \mathbb{Z}$ we have that $\eta\beta = (ct - d(2t+1)) + (c(2t+1) - d(t+1))\rho$ and therefore

$$\left\{ \begin{array}{rcl} x - z & = & ct - d(2t+1), \\ y - z & = & c(2t+1) - d(t+1). \end{array} \right. \tag{4.3}$$

From where we get:

$$\left\{ \begin{array}{rcl} |x| + |z| & \geq & |ct - d(2t+1)|, \\ |y| + |z| & \geq & |c(2t+1) - d(t+1)|. \end{array} \right. \tag{4.4}$$

Now, since $\mathcal{N}(\eta) \leq 7$ we have three different cases that we study separately.

- If $0 \leq |c| < |d|$ we have that $|x| + |z| \geq |ct - d(2t+1)| \geq |d||2t+1| > 2t$.
- If $0 \leq |d| < |c|$ we have that $|y| + |z| \geq |c(2t+1) - d(t+1)| \geq |c|(2t+1) > 2t$.
- If $0 \neq |c| = |d|$ we have two possibilities. If $c = -d$, any of the preceding cases yields to $|x| + |z| > 2t$ or $|y| + |z| > 2t$. If $c = d$, from Equations (4.3) we get that $|x| + |y| \geq |c(t+1) + dt| = |2ct + c| = |c|(2t+1) > 2t$.

In any case we get that $|x| + |y| + |z| > 2t$, which is a contradiction.

Finally, we have to prove that all the elements in (β) are at a distance greater or equal to $2t+1$. To this aim, we suppose the contrary and show that it yields to a contradiction. Therefore, there exists $\eta' \in \mathbb{Z}[\rho]$ such that $D_\alpha(\eta'\beta, 0) < 2t+1$. Hence, $\eta'\beta \equiv x + y\rho + z\rho^2 \pmod{\alpha}$ with $|x| + |y| + |z| \leq 2t$, that is, there exists $\eta \in \mathbb{Z}[\rho]$ such that $\eta\beta = x + y\rho + z\rho^2$ in $\mathbb{Z}[\rho]$. We have just proved that this condition yields to a contradiction, which concludes the proof. □

Hence, for any $\alpha = a + b\rho \in \mathbb{Z}[\rho]$ such that $\beta = t + (2t+1)\rho$ divides α, we define $\mathcal{C} = (\beta)$, the ideal generated by β, which is a perfect code over $\mathbb{Z}[\rho]_\alpha$ respect to the metric D_α. Next, we provide an example of a perfect error-correcting code based on the results above:

Example 14 *Let $\alpha_1 = (1+3\rho)^2 = -8-3\rho$. By Theorem 56, the ideal generated by $1+3\rho$ gives us the vertices of a perfect 1-dominating set in $EJ_{-8-3\rho}$. In Figure 4.4 a plane representation of this graph and its perfect 1-dominating set can be seen. Now, let $\alpha_2 = (1+2\rho)(2+5\rho) = -8-\rho$. Hence, by Theorem 56, the ideal generated by $2+5\rho$ is a perfect 2-dominating set in $EJ_{-8-\rho}$. This set is represented in Figure 4.5. For the sake of clarity, wrap-around edges have been omitted in both Figures.*

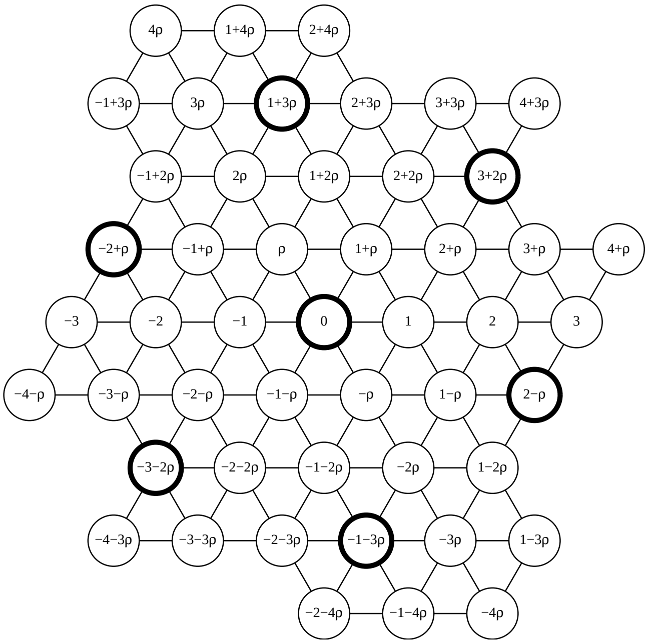

Figure 4.4: Perfect 1-Correcting Code over $\mathbb{Z}[\rho]_{-8-3\rho}$.

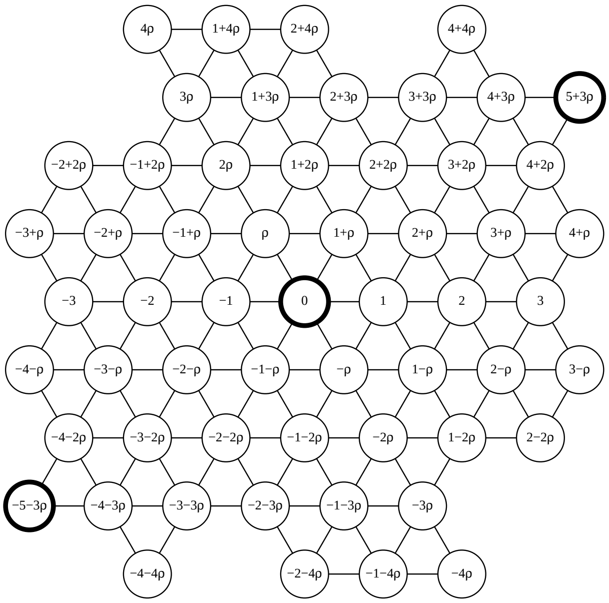

Figure 4.5: Perfect 2-Correcting Code over $\mathbb{Z}[\rho]_{-8-\rho}$.

Chapter 5

Graphs and Codes over Lipschitz Integers

Most of the previous ideas applied to integer rings of quadratic fields can be also considered over other algebraic structures. In this Chapter, our aim is to show that similar definitions and results can be obtained in the division algebra of the quaternions.

The rest of the Chapter is organized as follows. In Section 5.1, quotients of Lipschitz integers are considered. We introduce Cayley graphs over this structure and the perfect 1-dominating set problem is solved in Section 5.2. Section 5.3 is devoted to square representations of Lipschitz graphs. Some relations between these new quaternionic constellations and the ones considered for Gaussian graphs with the Lee metric will be shown in Section 5.4.

5.1 Quotients of Lipschitz Integers

In Section 1.3.2 we have introduced the quaternion algebra and its integer ring, the Lipschitz integers. Here, we consider quotients of this ring of integers by means of the following equivalence relation.

Definition 57 *Let $\alpha \neq 0$ be an integer quaternion. We say that $q_1, q_2 \in \mathbb{H}(\mathbb{Z})$ are* right congruent *modulo α if there exists $\beta \in \mathbb{H}(\mathbb{Z})$ such that*

$$q_1 - q_2 = \beta\alpha.$$

We will denote it as $q_1 \equiv_r q_2 \pmod{\alpha}$.

Note that this equivalence relation is well-defined. Hence, we can consider the quotient ring of the integer quaternions modulo this equivalence relation, which we denote as:

$$\mathbb{H}(\mathbb{Z})_\alpha = \{q \pmod{\alpha} \mid q \in \mathbb{H}(\mathbb{Z})\}.$$

This set coincides with the quotient ring of the integer quaternions over the left ideal generated by α, which we denote as $\langle\alpha\rangle$. In the next result we give an expression for the cardinal of this set. We have addressed such a result and its proof since we have not found it in the literature.

Theorem 58 *Let $\alpha \in \mathbb{H}(\mathbb{Z})$. Then $\mathbb{H}(\mathbb{Z})_\alpha$ has $\mathcal{N}(\alpha)^2$ elements.*

Proof.– The guidelines of this proof were suggested in [32]. Let $\alpha \neq 0$ be an integer quaternion and $A = \mathbb{H}(\mathbb{Z})$. First of all, we are going to prove that the left A-module $\dfrac{\mathbb{H}(\mathbb{Z})}{\langle\mathcal{N}(\alpha)\rangle}$ has $\mathcal{N}(\alpha)^4$ elements. Let $N = \mathcal{N}(\alpha)$. If two elements $\beta = b_1 + b_2 i + b_3 j + b_4 k$ and $\beta' = b_1' + b_2' i + b_3' j + b_4' k$ are congruent modulo N, then there exists $\beta = b_1'' + b_2'' i + b_3'' j + b_4'' k$ such that

$$\beta - \beta' = \beta'' N.$$

Therefore, $b_i - b_i' = b_i'' N$ for $i = 1, \ldots, 4$, that is, $b_i \equiv b_i' \pmod{N}$, which implies that there exists N possibilities for each b_i and therefore, N^4 different equivalence classes modulo N.

Now, since $\mathcal{N}(\alpha) = \overline{\alpha}\alpha$ we have the following inclusions of left ideals:

$$\langle\mathcal{N}(\alpha)\rangle = \langle\overline{\alpha}\alpha\rangle \subseteq \langle\alpha\rangle.$$

By the Third Isomorphism Theorem for A-modules (see [40]), we have the following exact sequence of left A-modules:

$$0 \longrightarrow \frac{\langle\alpha\rangle}{\langle\overline{\alpha}\alpha\rangle} \longrightarrow \frac{A}{\langle\overline{\alpha}\alpha\rangle} \longrightarrow \frac{A}{\langle\alpha\rangle} \longrightarrow 0$$

We denote the number of elements of $\dfrac{A}{\langle\alpha\rangle}$ by n and the number of elements of $\dfrac{\langle\alpha\rangle}{\langle\overline{\alpha}\alpha\rangle}$ by m. Then, as a consequence of the Lagrange's Theorem (see [40]) we can consider the previous exact sequence as a sequence of abelian groups and we have that $\mathcal{N}(\alpha)^4 = nm$. If we prove that $n = m$ we can finally conclude that $n = \mathcal{N}(\alpha)^2$.

Now, just note that the mapping

$$f : \frac{A}{\langle\overline{\alpha}\rangle} \longrightarrow \frac{\langle\alpha\rangle}{\langle\overline{\alpha}\alpha\rangle}$$

defined as $f(\beta + \langle\overline{\alpha}\rangle) = \beta\alpha + \langle\overline{\alpha}\alpha\rangle$ is both well-defined and an isomorphism of left A-modules. As a consequence, m is exactly the cardinal number of $\dfrac{A}{\langle\overline{\alpha}\rangle}$.

Finally, the quaternion conjugation is an anti-automorphism which implies that $\frac{A}{\langle\overline{\alpha}\rangle}$ and $\frac{A}{\langle\alpha\rangle}$ have that same cardinal number, that is, $n = m$, as we wanted to proof.□

As a consequence of the previous result we have the following:

Corollary 59 *Let $0 \neq \alpha \in \mathbb{H}(\mathbb{Z})$. Let $\beta \in \mathbb{H}(\mathbb{Z})$ be such that β is a right-divisor of α. Then, the left-ideal generated by β, $\langle\beta\rangle \subseteq \mathbb{H}(\mathbb{Z})_\alpha$ has $\frac{\mathcal{N}(\alpha)^2}{\mathcal{N}(\beta)^2}$ elements.*

5.2 Lipschitz Graphs, Perfect Dominating Sets and Codes

As in the cases of Gaussian integers and Eisenstein-Jacobi integers, we can define Cayley graphs over the quaternion integers or Lipschitz integers in an analogous way. For any $\alpha \in \mathbb{H}(\mathbb{Z})$ we can define a degree eight graph which has $\mathbb{H}(\mathbb{Z})_\alpha$ as its set of vertices. The definition is as follows:

Definition 60 *Let $0 \neq \alpha \in \mathbb{H}(\mathbb{Z})$ be an integer quaternion. We define the* Lipschitz graph *generated by α, $L_\alpha = (V, E)$, as follows:*

i) $V = \mathbb{H}(\mathbb{Z})_\alpha$ *is the set of vertices.*

ii) $E = \{(\eta, \beta) \in V \times V \mid \beta - \eta \equiv_r \pm 1, \pm i, \pm j, \pm k \pmod{\alpha}\}$ *is the set of edges.*

According to Theorem 58, this graph has order $\mathcal{N}(\alpha)^2 = (a_1^2 + a_2^2 + a_3^2 + a_4^2)^2$ and degree eight since every vertex is connected with other eight different ones. It is also connected and vertex-symmetric by definition. Figure 5.1 shows a representation of the Lipschitz graph generated by $1 + i + j + 2k$.

Now, we study the existence of perfect 1-dominating sets for Lipschitz graphs. In Theorem 61 a sufficient condition for the existence of such a set and its construction is detailed.

First of all, for any two vertices $\beta, \gamma \in \mathbb{H}(\mathbb{Z})_\alpha$ of the graph L_α, we will denote their distance in the graph as $D_\alpha(\beta, \gamma)$. Note that this distance can be computed as follows:

$$D_\alpha(\beta, \gamma) = \min\{|x_1| + |x_2| + |x_3| + |x_4| \mid \beta - \gamma \equiv_r x_1 + x_2 i + x_3 j + x_4 k \pmod{\alpha}\}.$$

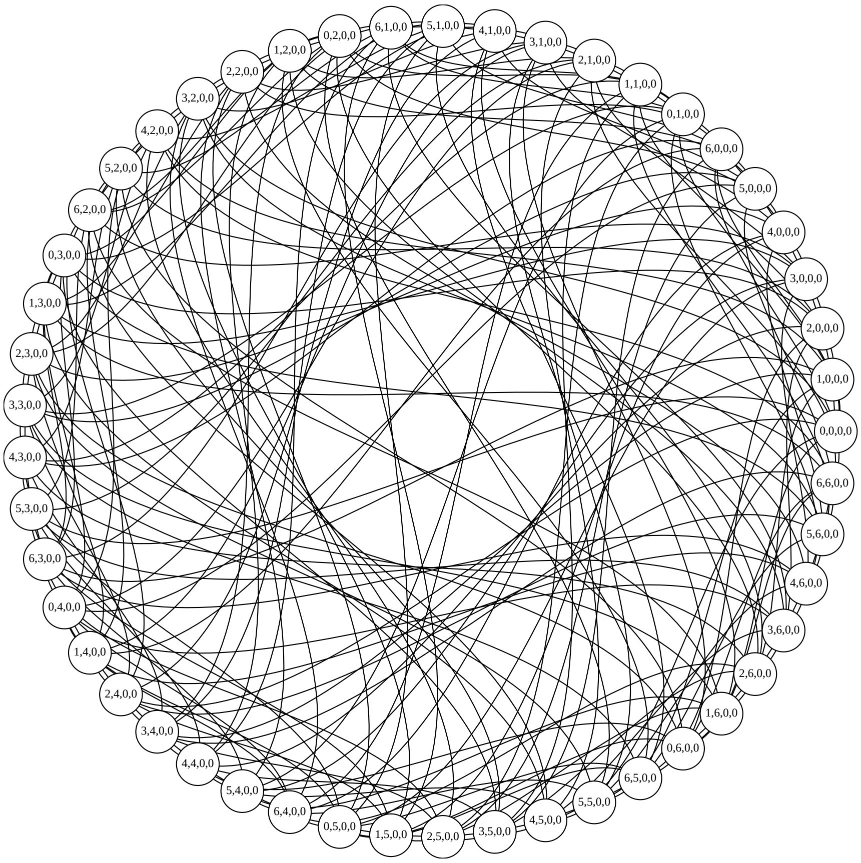

Figure 5.1: A Representation of the Lipschitz Graph Generated by $1+i+j+2k$.

Theorem 61 *Let $0 \neq \alpha \in \mathbb{H}(\mathbb{Z})$ be an integer quaternion.*

- *If $1+i+j$ is a right divisor of α then the left-ideal generated by $1+i+j$ is a perfect 1-dominating set over L_α.*

- *If $1+i+k$ is a right divisor of α then the left-ideal generated by $1+i+k$ is a perfect 1-dominating set over L_α.*

- *If $1+j+k$ is a right divisor of α then the left-ideal generated by $1+j+k$ is a perfect 1-dominating set over L_α.*

- *If $i+j+k$ is a right divisor of α then the left-ideal generated by $i+j+k$ is a perfect 1-dominating set over L_α.*

Proof.– We just proof the first item, since the other ones proceed in an analogous way.

Let $\alpha = a_1 + a_2 i + a_3 j + a_4 k$. First of all, since $1+i+j$ is a right-divisor of α, by Corollary 59, we have that the left-ideal generated by $1+i+j$, $\langle 1+i+j \rangle \subseteq \mathbb{H}(\mathbb{Z})_\alpha$ has cardinal number

$$\frac{\mathcal{N}(\alpha)^2}{\mathcal{N}(1+i+j)^2} = \frac{(a_1^2 + a_2^2 + a_3^2 + a_4^2)^2}{9}.$$

Now, we have to prove that for any two elements $\beta, \beta' \in \langle 1+i+j \rangle$, its distance fulfils $D_\alpha(\beta, \beta') \geq 3$. Note that it is enough to show that for any $\gamma \in \mathbb{H}(\mathbb{Z})$ such that $\gamma(1+i+j) \not\equiv 0 \pmod{\alpha}$, $D_\alpha(\gamma(1+i+j), 0) \geq 3$.

The proof is done by *reductio to absurdum*, that is, we suppose that there exist $0 \neq \gamma_1 \in \mathbb{H}(\mathbb{Z})$ such that $\gamma_1(1+i+j) \not\equiv 0 \pmod{\alpha}$ and $D_\alpha(\gamma_1(1+i+j), 0) < 3$. Therefore, $\gamma_1(1+i+j) \equiv_r x_1 + x_2 i + x_3 j + x_4 k \pmod{\alpha}$ with $|x_1| + |x_2| + |x_3| + |x_4| < 3$. We denote $x = x_1 + x_2 i + x_3 j + x_4 k$. Therefore, we have three possible cases cases:

i) One of the components of x is equal to 1 and the others are equal to 0.

ii) One of the components of x is equal to 2 and the others are equal to 0.

iii) Two components are equal to zero and the others equal to one.

The first case leads obviously to a contradiction. Hence, we just check in detail the other ones.

The second case implies that $\mathcal{N}(x) = 2^2 = 4$. On the other hand, since $1+i+j$ is a right divisor of α, there exists $\gamma_2 \in \mathbb{H}(\mathbb{Z})$ such that

$$\alpha = \gamma_2(1+i+j).$$

Now, since $\gamma_1(1+i+j) \equiv_r x_1 + x_2 i + x_3 j + x_4 k \pmod{\alpha}$, there exists $\gamma_3 \in \mathbb{H}(\mathbb{Z})$ such that

$$x_1 + x_2 i + x_3 j + x_4 k = \gamma_3 \alpha.$$

Finally, we obtain that

$$x_1 + x_2 i + x_3 j + x_4 k = (\gamma_1 - \gamma_2\gamma_3)(1+i+j).$$

If we take norms on both sides of the previous equality we obtain that

$$4 = \mathcal{N}(\gamma_1 - \gamma_2\gamma_3)\mathcal{N}(1+i+j) = \mathcal{N}(\gamma_1 - \gamma_2\gamma_3)3,$$

which is clearly a contradiction.

Finally, the third case implies that $\mathcal{N}(x) < 3$. According to the previous reasoning, which is correct also in this case we obtain that:

$$3 > \mathcal{N}(x_1 + x_2 i + x_3 j + x_4 k) = \mathcal{N}(\gamma_1 - \gamma_2\gamma_3)\mathcal{N}(1 + i + j) \geq 3,$$

which concludes the proof. □

Remark 62 *Note that in this case, the right-division of α by any of the candidates in Theorem 61 is equivalent to the fact that the cardinal of the ball of radius 1, which is 9, divides $N^2 = \mathcal{N}(\alpha)^2$; that is, 3 divides N. This is a consequence of the fact that $1 + i + j$ and its associates are the only ones with norm equal to 3. However, we have chosen to write the Theorem in an analogous way to the ones presented for Gaussian and Eisenstein-Jacobi graphs.*

Example 15 *Let $\alpha = 1 + i + 2j + 3k$. Since $i + j + k$ is a right divisor of α, then the left-ideal generated by $i + j + k$ is a perfect 1-dominating set in L_α.*

5.3 Square Representations of Lipschitz Graphs

In both the Gaussian and Eisenstein-Jacobi cases we have seen that there are some graphs which are or embed a square tours graph. Hence, there is some interest in studying the cases in which the elements of $\mathbb{H}(\mathbb{Z})_\alpha$ can be considered as two-dimensional sets. We will say that the basis $\{e_1, e_2\} \subset \{1, i, j, k\}$ *generates* $\mathbb{H}(\mathbb{Z})_\alpha$ if

$$\mathbb{H}(\mathbb{Z})_\alpha = \{me_1 + ne_2 \pmod{\alpha} \mid m, n \in \mathbb{Z}\}.$$

That is, for any $\beta \in \mathbb{H}(\mathbb{Z})_\alpha$ there exist $m, n \in \mathbb{Z}$ such that

$$\beta \equiv_r me_1 + ne_2 \pmod{\alpha}.$$

From here onwards, we discuss the cases in which any of the six possible bases generates $\mathbb{H}(Z)_\alpha$. Moreover, in the following result we state a particular case in which any of the bases always generates $\mathbb{H}(\mathbb{Z})_\alpha$. In this way, we can see the Lipschitz integers modulo α as $\mathbb{Z}_{\mathcal{N}(\alpha)} \times \mathbb{Z}_{\mathcal{N}(\alpha)}$.

Lemma 63 *Let $\alpha \in \mathbb{H}(Z)$ be an integer quaternion such that $\mathcal{N}(\alpha) = p$ is prime and $p \equiv 3 \pmod{4}$. Then, each one of the bases $\{e_1, e_2\} \subset \{1, i, j, k\}$ generates $\mathbb{H}(\mathbb{Z})_\alpha$.*

Proof.– We just prove that the basis $\{1, i\}$ generates $\mathbb{H}(\mathbb{Z})_\alpha$ since the other cases follow the same reasoning. Hence, we have to prove that there exist $m, n \in \mathbb{Z}$ such that $m + ni \equiv_r \beta \pmod{\alpha}$ for every $\beta \in \mathbb{H}(\mathbb{Z})$. Suppose that $m + ni \equiv_r m' + n'i \pmod{\alpha}$, with $0 \leq m, n, m', n' < p$. Then, there exists $\gamma \in \mathbb{H}(\mathbb{Z})$ such that

$$(m - m') + (n - n')i = \gamma\alpha.$$

If we take norms on both sides of the equation, we obtain that:

$$(m-m')^2+(n-n')^2=\mathcal{N}((m-m')+(n-n')i)=\mathcal{N}(\gamma\alpha)=\mathcal{N}(\gamma)\mathcal{N}(\alpha)=\dot{p},$$

where $\dot{p}$ denotes a multiple of p. Therefore, there exist $a, b \in \mathbb{Z}$ with $0 \leq a, b < p$ such that $a^2+b^2=\dot{p}$. Then, $(a+bi)(a-bi)=\dot{p}$ and p prime in $\mathbb{Z}[i]$ (Lemma 7) imply that p divides $a+bi$ or p divides $a-bi$ in $\mathbb{Z}[i]$. If p divides $a+bi$ in $\mathbb{Z}[i]$ then, $a+bi=(g_1+g_2i)p$ which implies $a=g_1p$ and $b=g_2p$ with both $a, b < p$, that is $a=b=0$. The same happens if p divides $a-bi$.

We have seen that $m=m'$ and $n=n'$. Now, since there are p^2 possibilities for obtaining $m+ni$ different classes. According to Theorem 58, $\mathbb{H}(\mathbb{Z})_\alpha$ has $\mathcal{N}(\alpha)^2=p^2$ elements. In consequence, we have proved that the family $\{m+ni \mid m, n \in \mathbb{Z}_p\}$ is a reduced residue system of the quotient ring. □

The next Theorem is a direct consequence of the previous Lemma.

Theorem 64 *Let $\alpha \in \mathbb{H}(Z)$ be an integer quaternion such that $\mathcal{N}(\alpha)=p$ prime and $p \equiv 3 \pmod 4$. Then, the square torus of side N is embedded in L_α.*

Proof.– The proof is based on Lemma 63 and the definition of the adjacency among vertices of the graph. □

Therefore, since the graph metric of a torus is the Lee metric, the Lee metric over the Lipschitz integers gives us an upper bound for the Lipschitz distance.

Example 16 *Figure 5.2 shows another representation of the Lipschitz graph generated by $1+i+j+2k$ previously shown in Figure 5.1. Note that $\mathcal{N}(1+i+j+2k)=7 \equiv 3 \pmod 4$. It can be observed a torus of side 7 embedded on the Lipschitz graph.*

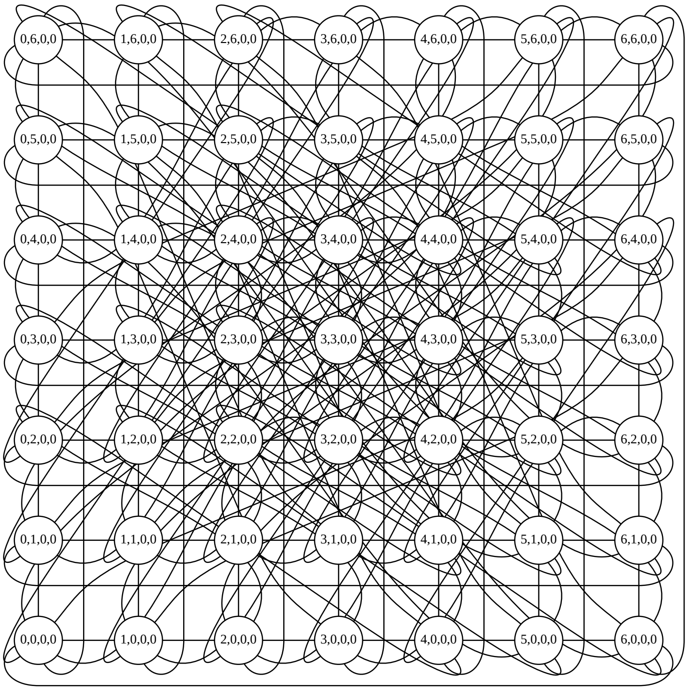

Figure 5.2: Square Representation of the Lipschitz Graph Generated by $1+i+j+2k$.

However, there are many more cases in which we can find a reduced residue system, in which any class of the quotient can be represented by an element with two coefficients equal to zero. Next, we state a general method to find such a reduced residue system and detail some guidelines for the proof. Finally, we show one example for an integer quaternion with non-prime norm in which we can find such a family of representants.

Lemma 65 *Let $0 \neq \alpha = a_1 + a_2 i + a_3 j + a_4 k \in \mathbb{H}(Z)$ be an integer quaternion and $N = \mathcal{N}(\alpha)$. Let $\gcd(a_1^2 + a_2^2, N) = 1$ and $\gcd(a_3^2 + a_4^2, N) = 1$. Then the following linear system over $\mathbb{Z}_N$ in variables $\{m, n\}$:*

$$(S1)\begin{cases} a_1 m + a_2 n = a_1 b_1 + a_2 b_2 + a_3 b_3 + a_4 b_4 \\ -a_2 m + a_1 n = -a_2 b_1 + a_1 b_2 - a_4 b_3 + a_3 b_4 \\ -a_3 m + a_4 n = -a_3 b_1 + a_4 b_2 + a_1 b_3 - a_2 b_4 \\ -a_4 m - a_3 n = -a_4 b_1 - a_3 b_2 + a_2 b_3 + a_1 b_4 \end{cases}$$

has a solution in $\mathbb{Z}_N$ for any $b_1, b_2, b_3, b_4 \in \mathbb{Z}$ and the family $\{m + ni \mid m, n \in \mathbb{Z}_N\}$ is a reduced residue system of the quotient ring $\mathbb{H}(\mathbb{Z})_\alpha$.

Proof.– Given any $\beta = b_1 + b_2 i + b_3 j + b_3 k \in \mathbb{H}(\mathbb{Z})$ we have to prove that there exist $m, n \in \mathbb{Z}$ and $\gamma \in \mathbb{H}(\mathbb{Z})$ such that:

$$m + ni - (b_1 + b_2 i + b_3 j + b_4 k) = \gamma\alpha.$$

A general expression for γ would be $\gamma = g_1 + g_2 i + g_3 j + g_4 k$ with $g_1, g_2, g_3, g_4 \in \mathbb{Z}$. The product of γ and α is computed as:

$$\begin{array}{rcl} \gamma\alpha & = & (g_1 a_1 - g_2 a_2 - g_3 a_3 - g_4 a_4) \\ & + & (g_1 a_2 + g_2 a_1 + g_3 a_4 - g_4 a_3) i \\ & + & (g_1 a_3 - g_2 a_4 + g_3 a_1 + g_4 a_2) j \\ & + & (g_1 a_4 + g_2 a_3 - g_3 a_2 + g_4 a_1) k. \end{array}$$

It can be verified that this product can be obtained operating the the next matrix product:

$$\begin{pmatrix} 1 & i & j & k \end{pmatrix} \begin{pmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & a_4 & -a_3 \\ a_3 & -a_4 & a_1 & a_2 \\ a_4 & a_3 & -a_2 & a_1 \end{pmatrix} \begin{pmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \end{pmatrix}$$

Thus, if we represent the quaternions as vector columns we obtain the following equation:

$$\begin{pmatrix} m - b_1 \\ n - b_2 \\ -b_3 \\ -b_4 \end{pmatrix} = \begin{pmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & a_4 & -a_3 \\ a_3 & -a_4 & a_1 & a_2 \\ a_4 & a_3 & -a_2 & a_1 \end{pmatrix} \begin{pmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \end{pmatrix}$$

Note that the determinant of the square matrix is equal to $\mathcal{N}(\alpha)^2$, which is non-zero, that is the system always has solution. Hence, if we multiply by its inverse on both sides we obtain:

$$\begin{pmatrix} g_1 \\ g_2 \\ g_3 \\ g_4 \end{pmatrix} = \frac{1}{N} \begin{pmatrix} a_1(m - b_1) + a_2(n - b_2) - a_3 b_3 - a_4 b_4 \\ -a_2(m - b_1) + a_1(n - b_2) + a_4 b_3 - a_3 b_4 \\ -a_3(m - b_1) + a_4(n - b_2) - a_1 b_3 + a_2 b_4 \\ -a_4(m - b_1) - a_3(n - b_2) - a_2 b_3 - a_1 b_4 \end{pmatrix}$$

Now, g_1, g_2, g_3, g_4 have to be integers. Note that the first component of the vector is

$$\frac{1}{N}(a_1(m - b_1) + a_2(n - b_2) - a_3 b_3 - a_4 b_4),$$

which is an integer if and only if it is fulfilled that

$$a_1(m - b_1) + a_2(n - b_2) - a_3 b_3 - a_4 b_4 \equiv 0 \pmod{N}.$$

If we operate in this way, we obtain the following linear system over $\mathbb{Z}_N$:

$$(S1)\begin{cases} a_1m + a_2n = a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4 \\ -a_2m + a_1n = -a_2b_1 + a_1b_2 - a_4b_3 + a_3b_4 \\ -a_3m + a_4n = -a_3b_1 + a_4b_2 + a_1b_3 - a_2b_4 \\ -a_4m - a_3n = -a_4b_1 - a_3b_2 + a_2b_3 + a_1b_4 \end{cases}$$

Now, we are going to verify that the conditions $\gcd(a_1^2 + a_2^2, N) = 1$ and $\gcd(a_3^2 + a_4^2, N) = 1$ imply that the previous system has solution over $\mathbb{Z}_N$.

Straightforwardly, the condition $\gcd(a_1^2 + a_2^2, N) = 1$ implies that the subsystem:

$$(E1)\begin{cases} a_1m + a_2n = a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4 \\ -a_2m + a_1n = -a_2b_1 + a_1b_2 - a_4b_3 + a_3b_4 \end{cases}$$

has solution in $\mathbb{Z}_N$, which by Cramer's rule is:

$$m_1 := \frac{(a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)a_1 - (-a_2b_1 + a_1b_2 - a_4b_3 + a_3b_4)a_2}{a_1^2 + a_2^2},$$

$$n_1 := \frac{a_1(-a_2b_1 + a_1b_2 - a_4b_3 + a_3b_4) - (-a_2)(a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)}{a_1^2 + a_2^2}.$$

Analogously, the condition $\gcd(a_3^2 + a_4^2, N) = 1$ implies that the subsystem:

$$(E2)\begin{cases} -a_3m + a_4n = -a_3b_1 + a_4b_2 + a_1b_3 - a_2b_4 \\ -a_4m - a_3n = -a_4b_1 - a_3b_2 + a_2b_3 + a_1b_4 \end{cases}$$

has solution in $\mathbb{Z}_N$, which by Cramer's rule is:

$$m_2 := \frac{(-a_3b_1 + a_4b_2 + a_1b_3 - a_2b_4)(-a_3) - (-a_4b_1 - a_3b_2 + a_2b_3 + a_1b_4)a_4}{a_3^2 + a_4^2},$$

$$n_2 := \frac{(-a_3)(-a_4b_1 - a_3b_2 + a_2b_3 + a_1b_4) - (-a_4)(-a_3b_1 + a_4b_2 + a_1b_3 - a_2b_4)}{a_3^2 + a_4^2}.$$

Now, we show that $m_1 \equiv m_2 \pmod N$ and $n_1 \equiv n_2 \pmod N$, which concludes the proof. Note that $a_1^2 + a_2^2 \equiv -(a_3^2 + a_4^2) \pmod N$. Therefore, $m_1 \equiv m_2$ $\pmod N$ if and only if the sum of their numerators is congruent to zero modulo N and $n_1 \equiv n_2 \pmod N$ if and only if the sum of their numerators is congruent to zero modulo N. If we operate, we obtain the following expressions

$$b_1(a_1^2 + a_2^2 + a_3^2 + a_4^2) \equiv 0 \pmod N,$$

$$b_2(a_1^2 + a_2^2 + a_3^2 + a_4^2) \equiv 0 \pmod N,$$

which are obviously true, which concludes the proof. □

Note that similar conditions can be formulated for each of bases $\{e_1, e_2\} \subset \{1, i, j, k\}$ by just permutating the order of the indices. In fact, since $a_3^2 + a_4^2 = N - (a_1^2 + a_2^2)$, this implies that $\gcd(a_1^2 + a_2^2, N) = 1$ if and only if $\gcd(a_3^2 + a_4^2, N) = 1$. Therefore, we can state the following result.

Theorem 66 *Let $\alpha = a_1 + a_2 i + a_3 j + a_4 k \in \mathbb{H}(\mathbb{Z})$. If at least one of the six integers $a_1^2 + a_2^2, a_1^2 + a_3^2, a_1^2 + a_4^2, a_2^2 + a_3^2, a_2^2 + a_4^2, a_3^2 + a_4^2$ is coprime to $\mathcal{N}(\alpha)$, then $\mathbb{H}(\mathbb{Z})_\alpha$ is generated by one of the six possible bases $\{e_u, e_v\} \subset \{1, i, j, k\}$.*

Finally, using previous result we can enunciate the following consequence.

Corollary 67 *Let $\alpha = a_1 + a_2 i + a_3 j + a_4 k \in \mathbb{H}(\mathbb{Z})$ be an integer quaternion such that at least one of the six integers $a_1^2 + a_2^2, a_1^2 + a_3^2, a_1^2 + a_4^2, a_2^2 + a_3^2, a_2^2 + a_4^2, a_3^2 + a_4^2$ is coprime to $\mathcal{N}(\alpha) = N$. Then, the additive group $(\mathbb{H}(\mathbb{Z})_\alpha, +)$ is isomorphic to $(\mathbb{Z}_N \times \mathbb{Z}_N, +)$.*

Proof.– Since at least one of the six integers $a_1^2+a_2^2, a_1^2+a_3^2, a_1^2+a_4^2, a_2^2+a_3^2, a_2^2+a_4^2, a_3^2+a_4^2$ is coprime to $\mathcal{N}(\alpha) = N$, then there exists at least one basis $\{e_u, e_v\} \subset \{1, i, j, k\}$ that generates $H(\mathbb{Z})_\alpha$. Let us consider the following mapping:

$$\begin{array}{rccc} f: & \mathbb{Z}_N \times \mathbb{Z}_N & \longrightarrow & \mathbb{H}(\mathbb{Z})_\alpha \\ & (m, n) & \longmapsto & m e_u + n e_v \pmod{\alpha} \end{array}$$

The mapping f is well-defined. If $(m_1, n_1), (m_2, n_2) \in \mathbb{Z}_N \times \mathbb{Z}_N$ such that $m_1 \equiv m_2 \pmod{N}$ and $n_1 \equiv n_2 \pmod{N}$ we have that there exist $c_1, c_2 \in \mathbb{Z}$ such that

$$m_1 - m_2 = c_1 N = c_1 \overline{\alpha}\alpha,$$
$$n_1 - n_2 = c_2 N = c_2 \overline{\alpha}\alpha,$$

which implies that $(m_1 - m_2)e_u + (n_1 - n_2)e_v = (c_1 e_u + c_2 e_v)\overline{\alpha}\alpha$, that is, $m_1 e_u + n_1 e_v \equiv_r m_2 e_u + n_2 e_v$.

The fact that f is a bijective mapping is a direct consequence of the existence of a solution in the corresponding system of equations in $\mathbb{Z}_N$. Also, it is straightforward that the mapping preserves the addition. Hence, f is a group isomorphism. □

Example 17 *Suppose $\alpha = 1 + i + 2j + 3k$ with $\mathcal{N}(\alpha) = 15$. Note that* $\gcd(2, 15) = 1$ *and* $\gcd(13, 15) = 1$. *Each of these conditions implies that the system of equations (S1):*

$$(S1) \begin{cases} m + n = b_1 + b_2 + 2b_3 + 3b_4 \\ m + n = -b_1 + b_2 - 3b_3 + 2b_4 \\ -2m + 3n = -2b_1 + 3b_2 + b_3 - b_4 \\ -3m - 2n = -3b_1 - 2b_2 + b_3 + b_4 \end{cases}$$

has solution. In fact, it is easy to prove that $m = b_1 + 10b_3 + 8b_4$ and $n = b_2 + 7b_3 + 10b_4$ is a solution to the system. Therefore, we can always find a representant of the form $m + ni$ for any class of $\mathbb{H}(\mathbb{Z})_\alpha$, with $(m, n) \in \mathbb{Z}_{15} \times \mathbb{Z}_{15}$.

5.4 Cayley Graphs over Different Complex Integer Rings

In this Section, we consider those values of N in which more than one of the graphs introduced in this memory, Gaussian, Eisenstein-Jacobi and Lipschitz graphs, can be built. In such cases we ask for the existence of perfect dominating sets. In order to illustrate the different relations between the three families of graphs, several examples are going to be shown. Finally, we conclude the Section with a particular case in which the Lee distance can also be applied over Lipschitz graphs.

First of all, if $N \in \mathbb{Z}$ can be written as a sum of two squares we can build a Gaussian graph with N vertices. In the case of an integer N that can be written as the norm of an Eisenstein-Jacobi integer ($N = a^2 + b^2 - ab$ for some integers a, b), we can build an Eisenstein-Jacobi graph of order N. Finally, for any integer N which is a perfect square, we can write its square root as the sum of four squares and therefore, we can build a Lipschitz graph with N vertices.

There are several cases in which we can define, for a given number of vertices N, the three different graphs as the next example shows.

Example 18 *Let* $N = 25$. *Clearly,* $25 = \mathcal{N}(5i)$ *if we consider the norm in the Gaussian integers. Also,* $25 = \mathcal{N}(5\rho)$ *if we consider the norm in the Eisenstein-Jacobi integers. Finally,* $N = \mathcal{N}(j + 2k)$ *if we consider the norm in the integer quaternions. Figures 5.3, 5.4, 5.5, show three examples of these graphs, all of them with the same number of vertices but with degrees four, six and eight, respectively.*

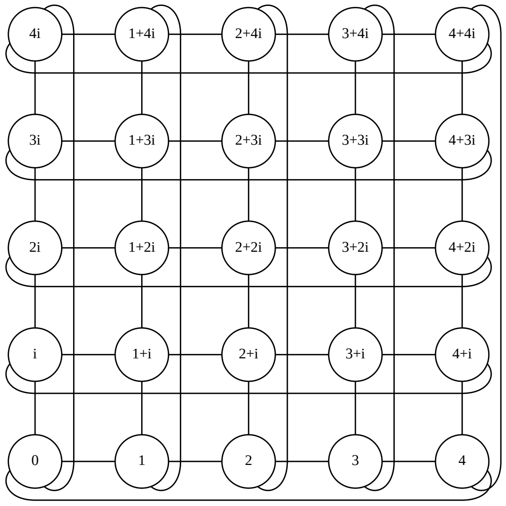

Figure 5.3: G_5.

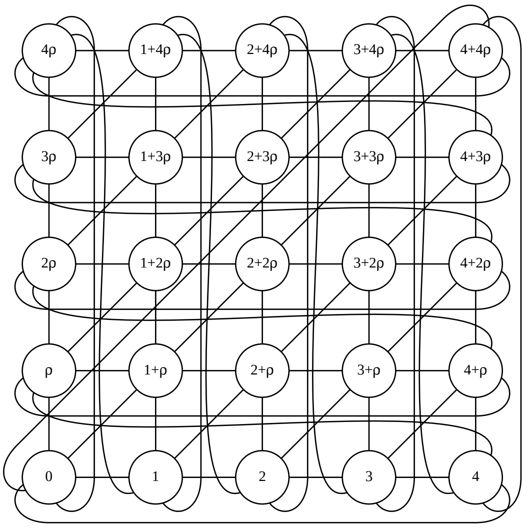

Figure 5.4: EJ_5.

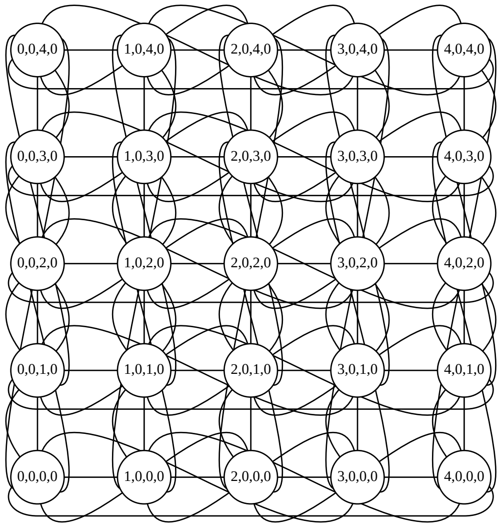

Figure 5.5: L_{j+2k}.

Now, we wonder if there are values of N such that there exist the three graphs and perfect t-dominating sets over each one of the them. Note that, if there exists a perfect 1-dominating set for the Lipschitz graph, then 9 must divide N^2, or equivalently $N \equiv 0 \pmod 3$. Also, if there exists a perfect t-dominating set for the Eisenstein-Jacobi graph, then $3t^2 + 3t + 1$ must divide N. In particular, if both sets exist, then

$$N \equiv 0 \pmod{3},$$
$$N \equiv 1 \pmod{3}.$$

Therefore, there are no Lipschitz and Eisenstein-Jacobi graphs with the same order having both a perfect t-dominating set. However, as the next example shows, there are Gaussian graphs and Eisenstein-Jacobi graphs with the same order, having both of them perfect t-dominating sets.

Example 19 *Let us consider* $N = 61$. $N = \mathcal{N}(6+5i)$ *when considering the norm in the Gaussian integers and* $N = \mathcal{N}(4+9\rho)$ *when considering the Eisenstein-Jacobi integer's norm. Both integers correspond to the Gaussian and Eisenstein-Jacobi divisors that we considered for the existence of a perfect* t*-dominating set in each case, that is, they form a ball for each metric. However, the first one,* $6+5i = i(5-6i)$ *corresponds to a a ball of radius* $t = 5$ *and* $4+9\rho$ *corresponds to radius* $t = 4$*. Figures 5.6 and 5.7 show both graphs.*

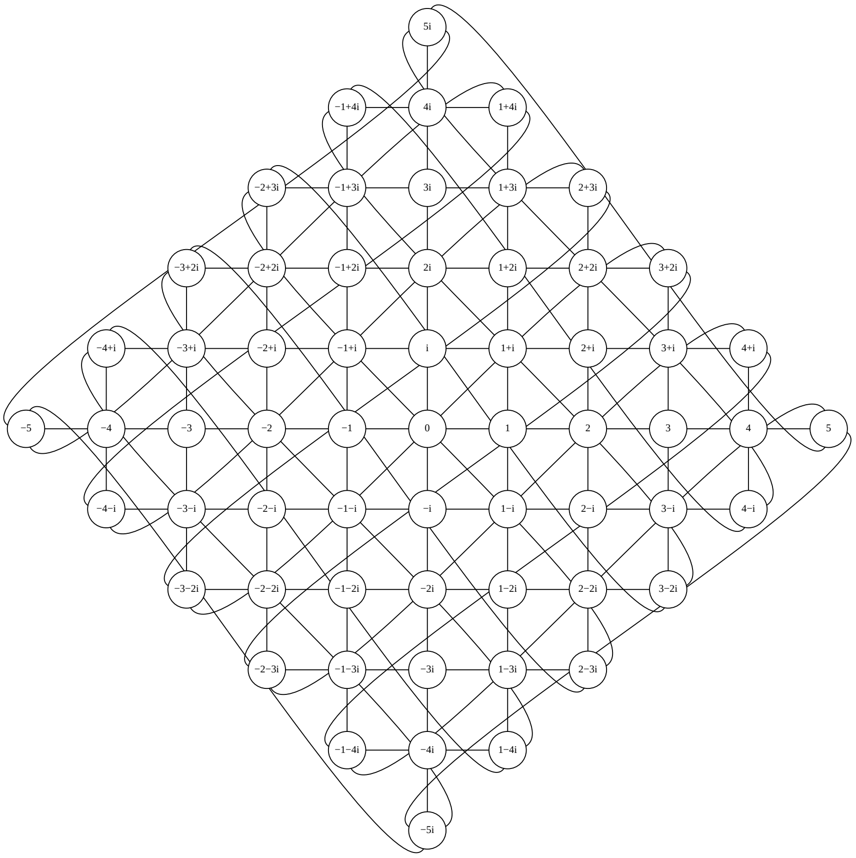

Figure 5.6: G_{5-6i}.

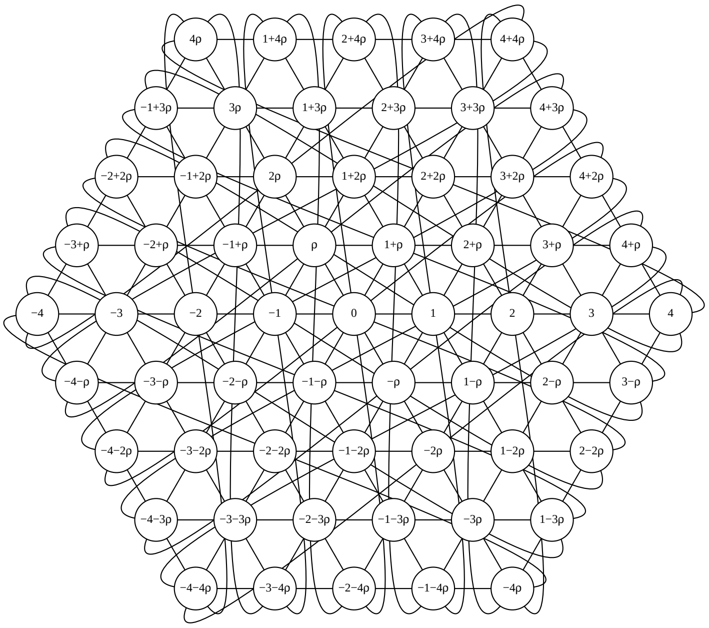

Figure 5.7: $EJ_{4+9\rho}$.

Finally, there are also cases in which for a given integer N being a sum of two squares and a perfect square we can consider Gaussian and Lipschitz graphs with perfect dominating sets. Suppose that we are considering a Lipschitz graph with N^2 vertices in which at least one of the bases $\{1, i\}$, $\{1, j\}$ or $\{1, k\}$ generates $\mathbb{H}(\mathbb{Z})_\alpha$. In this case, the associated constellation is a square with side N. Therefore, we can consider two different metrics coming from the graphs defined in this work: the Lee metric and the Lipschitz's graph metric. In both cases we can consider the construction of perfect 1-correcting codes which leads to some interesting examples of different codes over the same alphabet, $\mathbb{Z}_N \times \mathbb{Z}_N$, as the next example shows.

Example 20 *Let us have a look at the square constellation induced by the Lipschitz integer $1 + i + 2j + 3k$ represented as $\mathbb{Z}_{15} \times \mathbb{Z}_{15}$. For this space, we can consider two different metrics and two different 1-error correcting codes for both metrics.*

- *In the first case, we can see the signal points of the constellation as the vertices of the Lipschitz graph generated by $1 + i + 2j + 3k$. The integer quaternion $i + j + k$ is a right divisor of $1 + i + 2j + 3k$ and therefore, we have a perfect code which is represented in Figure 5.8.*

- *In the second case, we can also see the square constellation as the vertices of the Gaussian graph G_{15}. In this case, the distance induced by the graph coincides with the Lee metric. Also, since $1 + 2i$ divides 15, we can build a perfect code which is represented in Figure 5.9.*

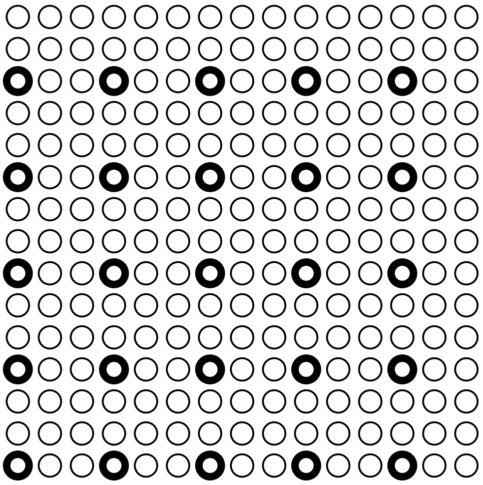

Figure 5.8: Perfect Code over $\mathbb{Z}_{15} \times \mathbb{Z}_{15}$ for the Lipschitz Distance.

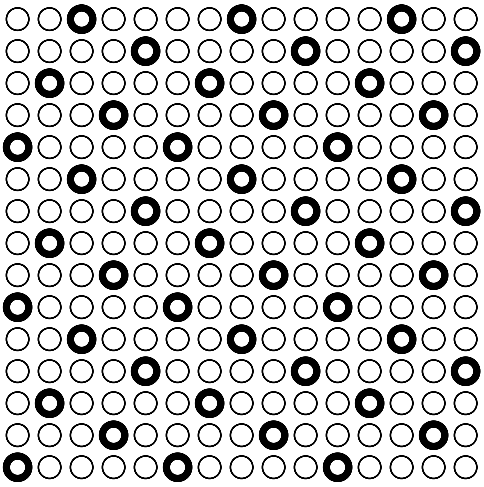

Figure 5.9: Perfect Code over $\mathbb{Z}_{15} \times \mathbb{Z}_{15}$ for the Lee Distance.

Chapter 6

Conclusions and Future Research

In this memory we have presented an original relationship among the fields of Number Theory, Graph Theory and Coding Theory. We have introduced three families of Cayley graphs whose vertices are the elements of quotient rings of the Gaussian integers, the Eisenstein-Jacobi integers and the Lipschitz integers, respectively. The degree of these graphs and their set of edges are determined by the set of units of the corresponding ring. Hence, such graphs constitute models of their underlying integer rings.

The motivation behind the study of these graphs has been the proposal of perfect error-correcting codes for multi-dimensional signal constellations. We have considered quadratic, hexagonal and four-dimensional constellations or lattices. Each signal point is represented by a vertex of the considered graph. The code structure and its error-correction capacity are determined by different properties of the graph modeling it.

Other approaches for the definition of metrics for this kind of signal constellations have failed and therefore, the techniques presented in this memory seem to be a correct alternative to use over these metric spaces. Moreover, the well-known perfect codes for the Lee metric are a subcase of the codes presented in this research which link this work with classical results in Coding Theory.

The problem of proposing perfect error-correcting codes over the alphabets considered in this work has a parallelism with the problem of finding sets of perfect domination over the graphs which model the constellation. We have been able to provide sufficient conditions for obtaining such perfect sets for each one of the graphs considered in this research: Gaussian, Eisenstein-Jacobi and Lipschitz graphs respectively. Consequently, we have been able to propose new perfect error-correcting codes for quadratic, hexagonal and four-dimensional signal spaces.

There are several topics related to the ones presented here that could be considered for future research. We summarize the most important ones in our opinion.

Code Performance. The characteristics of the codes proposed in this work depend on the distance-related properties of the graphs modeling them. Then, graph parameters as diameter and average distance should be obtained for Eisenstein-Jacobi and Lipschitz graphs. In the same way, the concept of quotient graph should be considered in these two cases. With this tools it would be straightforward to provide the basic performance figures of the proposed codes.

Longer Codes. The codes presented in Chapters 3 and 4 can be used to define longer codes over the Gaussian integers and Eisenstein-Jacobi integers. There are several ways for defining longer codes from shorter ones as it is considered in [15] for Hamming metric codes. These techniques could probably be adapted to the graph metrics that we have considered here. Also, known techniques from Graph Theory such as graph products or compositions could be considered to obtain longer codes over this type of alphabets.

Non-perfect or Quasi-perfect Codes. In [3] quasi-perfect codes for the Lee distance are considered for two reasons. The first one is that not always exists a perfect code over the two-dimensional Lee-space. The second one is that, as Welch and Golomb conjectured in [29] which is not proved yet, there is not perfect Lee codes for radii greater than 1 when the dimensions of the signal space is higher than 2 (respectively, the degree of the graph torus is higher than 4). We are under similar conditions: not always there are perfect dominating sets over the Gaussian and Eisenstein-Jacobi graphs so, quasi-perfect codes could be considered. Also, there are not perfect dominating sets for degree six circulant graphs in general (not necessarily having a jump which is a linear combination of the first two ones), so quasi-perfect codes may be discussed also in this cases.

Anticodes. An *anticode* $\mathcal{A}$ of diameter d is characterized by the property that the distance between any two distinct points of $\mathcal{A}$ is at most d. The perfect codes that we have considered in this work are anticodes whose diameter is a function of the diameter of the quotient graphs introduced in Section 3.4. A deeper study about their relation with other anticodes, even with *tristance optimal anticodes* presented in [25] could be done.

Codes over Octavian Integers. The *octonions* are expressions of the form

$$x_\infty + x_0 i_0 + x_1 i_1 + x_2 i_2 + x_3 i_3 + x_4 i_4 + x_5 i_5 + x_6 i_6,$$

(x_t real), which constitute the algebra over the reals generated by the units $i_0, \ldots, i_6$ that satisfy

$$\begin{aligned} i_n^2 &= -1, \\ i_{n+1}i_{n+2} &= i_{n+4} = -i_{n+2}i_{n+1}, \\ i_{n+2}i_{n+4} &= i_{n+1} = -i_{n+4}i_{n+2}, \\ i_{n+4}i_{n+1} &= i_{n+2} = -i_{n+1}i_{n+4}, \end{aligned}$$

where the subscripts are taken modulo 7.

Due to the celebrated Hurwitz's Theorem we know that the only composition algebras over $\mathbb{R}$ are $\mathbb{C}$, $\mathbb{H}$ and $\mathbb{O}$, that is, the complex numbers, the quaternions and the octonions. Therefore, it seems a natural extension of our work to see how the techniques presented in this thesis can be applied to the *octavian integers*, that is, the octonions with integer coefficients. Similar definitions of Cayley graphs, in this case of degree 16 since there are 8 units, can be used and the existence of perfect dominating sets could be studied.

Graph Theory. We think that other applications of the graphs presented in this thesis could imply new results in Graph Theory. Nowadays, graph products that conserve the degree have become very popular as they are a tool to look for families of good graph expanders. In particular, the recently defined *zig-zag product* in [61] is a new type of graph product which inherits the expansion properties from the operated graphs. In [4] semi-direct products in groups and zig-zag products in graphs have been connected by means of Cayley graphs. In this sense, the quotient graphs introduced in Section 3.4 could be used to define a graph product for Gaussian graphs which conserves the graph degree.

Bibliography

[1] A. Ádám. “Research problem 2-10”. Journal of Combinatorial Theory, 2:393, 1967.

[2] F. Aguiló, M.A. Fiol and C. García. “Triple Loop Networks with Small Transmission Delay”. Discrete Mathematics 167/168 (1997) pp. 3-16.

[3] B. F. AlBdaiwi and B. Bose. “Quasi-perfect Lee Distance Codes”. IEEE Transactions on Information Theory 49(6): 1535-1539 (2003).

[4] N. Alon, A. Lubotzky, A. Wigderson. “Semi-direct Product in Groups and Zig-zag Product in Graphs: Connections and Applications”. Proc. of the 42nd FOCS, pp. 630-637, 2001.

[5] R. Beivide, E. Herrada, J.L. Balcázar and A. Arruabarrena. “Optimal Distance Networks of Low Degree for Parallel Computers”. IEEE Transactions on Computers, Vol. C-40, No. 10, pp. 1109-1124, 1991.

[6] R. Beivide, C. Martínez, J. Gutierrez, J. A. Gregorio, C. Izu and J. Miguel-Alonso. “Chordal Topologies for Interconnection Networks”. Proc. of 5th International Symposium on High Performance Computing (ISHPC 2003), pp 385-393. Tokio-Odaiba, Japan, October 2003. Also in Lecture Notes in Computer Science, Springer-Verlag.

[7] J-C. Belfiore, G. Rekaya. “Quaternionic Lattices for Space-Time Coding” ITW2003, Paris, France, March 31- April 4, 2003.

[8] E. R. Berlekamp. “Algebraic Coding Theory”. Aegean Park Press, 1984.

[9] J.-C. Bermond, G. Illiades and C. Peyrat. “An Optimization Problem in Distributed Loop Computer Networks”. 3rd International Conference on Combinatorial Mathematics. New York Academy of Sciences, pp. 1-13, 1985.

[10] F. T. Boesch, R. Tindell. “Circulants and their Connectivities”. J. Graph Theory 8 (1984) pp. 487- 499.

[11] F. T. Boesch and J. Wang. “Reliable Circulant Networks with Minimum Transmission Delay”. IEEE Transactions on Circuit and Systems. Vol. 32, pp. 1286-1291, 1985.

[12] B. Bose, B. Broeg, Y. Known and Y. Ashir. “Lee Distance and Topological Properties of k-ary n-cubes”. IEEE Transactions on Computers, Vol. 44, No. 8, pp. 1021-1030, 1995.

[13] J.-Y. Cai, G. Havas, B. Mans, A. Nerurkar, J.-P. Seifert and I. Shparlinski. ”On Routing in Circulant Graphs”. Cocoon’99, Japan, 1999.

[14] J. M. Cámara, M. Moretó, E. Vallejo, R. Beivide, J. Miguel-Alonso, C. Martínez and J. Ridruejo. “Mixed-radix Twisted Torus Interconnection Network”. 21st IEEE International Parallel & Distributed Processing Symposium - IPDPS ’07, Long Beach, California, USA, 26-30 March 2007.

[15] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein. “Covering Codes”. Elsevier 1997.

[16] H. Cohn. “Advanced Number Theory”. Dover Publications, Inc. (1980). ISBN 0-486-64023-X.

[17] J. H. Conway and D. A. Smith. “On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry”. A K Peters, Ltd. (2003). ISBN 1-56881-134-9.

[18] G. Cooperman, L. Finkelstein, N. Sarawagi. “Applications of Cayley Graphs” AAECC: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes International Conference (AAECC-8, 1990). Springer-Verlag Lecture Notes in Comp. Sci. 508.

[19] S.I.R. Costa, M. Muniz, E. Agustini and R. Palazzo. “Graphs, Tessellations, and Perfect Codes on Flat Tori”. IEEE Transactions on Information Theory, Vol. 50, No. 10, pp. 2363-2377, October 2004.

[20] G. Davidoff, P. Sarnak and A. Valette. “Elementary Number Theory, Group Theory and Ramanujan Graphs”. London Mathematical Society Student Texts (No. 55). Cambridge University Press, 2003. ISBN: 0 521 82426 5.

[21] P. J. Davis. “Circulant Matrices”. John Wiley & Sons , New York. 1979.

[22] Xue-Dong Dong, Cheong Boon Soh, Erry Gunawan and Li-Zhong Tang. “Groups of Algebraic Integers Used for Coding QAM Signals”. IEEE Transactions on Information Theory 44(5), pp. 1848-1860 (1998).

[23] Xue-Dong Dong, Cheong Boon Soh and Erry Gunawan. “Codes over Finite Fields for Multidimensional Signals”. Journal of Algebra 233, 105-121 (2000).

[24] B. Elspas and J. Turner. “Graphs with Circulant Adjacency Matrices”. J. Combin. Theory, No.9, pp. 297-307, 1970.

[25] T. Etzion, M. Schwartz, A. Vardy. “Optimal Tristance Anticodes in Certain Graphs”. J. Comb. Theory, Ser. A 113(2), pp. 189-224 (2006).

[26] M.A. Fiol, J.L. Yebra, I. Alegre and M. Valero. “A Discrete Optimization Problem in Local Networks and Data Alignment”. IEEE Transactions on Computers, Vol. 36, No. 6, pp. 702-713, 1987.

[27] E. Gabidulin, C. Martínez, R. Beivide and J. Gutierrez. “On the Weight Distribution of Gaussian Graphs with an Application to Coding Theory”. Proceedings of the 8th International Symposium on Communication Theory and Applications (ISCTA’05). Ambleside, UK. 17-22 July 2005.

[28] J. C. George, R. S. Sanders. “When is a Tensor Product of Circulant Graphs Circulant?” . In eprint arXiv:math/9907119 (07/1999).

[29] S. W. Golomb and L.R. Welch. “Algebraic Coding and the Lee Metric”. Error Correcting Codes, edited by H.B. Mann, John Wiley & Sons, New York, (1968).

[30] S. W. Golomb and L. R. Welch. “Perfect Codes in the Lee Metric and the Packing of the Polyominoes”. SIAM Journal of Applied Mathematics, Vol. 18, No. 2, pp. 302-317. Mar 1970.

[31] D. Gómez, J. Gutierrez, A. Ibeas, C. Martínez, and R. Beivide. ”On Finding a Shortest Path in Circulant Graphs with Two Jumps”. Accepted for presentation at Cocoon’05, China, 2005.

[32] J. Gómez Torrecillas, Universidad de Granada, Spain. Personal communication.

[33] R.W. Hamming. “Error Detecting and Error Correcting Codes”. The Bell System Technical Journal, vol. XXVI, no. 2. April 1950.

[34] F. Harary. “Graph Theory”. Addison-Wesley Publishing Company. 1972.

[35] G.H. Hardy and E.M. Wright. “An Introduction to the Theory of Numbers”. Oxford University Press. Fourth Edition (1960). ISBN 0-19-853310-7.

[36] C. Heuberger. “On Planarity and Colorability of Circulant Graphs”. Discrete Mathematics, vol. 268, no. 1-3 (2003), pp. 153-169.

[37] K. Huber. “Codes Over Gaussian Integers”. IEEE Transactions on Information Theory, Vol. 40, No. 1, pp. 207-216, January 1994.

[38] K. Huber. “Codes over Tori”. IEEE Trans. on Information Theory, Vol. 43, No. 2, pp. 740-744, March 1997.

[39] K. Huber. “Codes over Eisenstein-Jacobi integers”. Finite fields: theory, applications, and algorithms (Las Vegas, NV, 1993), 165–179, Contemp. Math., 168, Amer. Math. Soc., Providence, RI, 1994.

[40] T. W. Hungerford. “Algebra”. Springer-Verlag New York Inc. 1974.

[41] K. Ireland, M. Rosen. “A Classical Introduction to Modern Number Theory”. 1990.

[42] P. K. Jha. “Perfect r-Domination in the Kronecker Product of Two Cycles, with an Application to Diagonal/Toroidal Mesh”. Information Processing Letters 87 (2003) 163-168.

[43] W. E. Klee. “Cristallographic Nets and Their Quotient Graphs”. Cryst. Res. Technol. 39, No 11, 959-968 (2004).

[44] C.Y. Lee. “Some Properties of Nonbinary Error-Correcting Codes”. IRE Trans. Inform. Theory, 4 (1958), 77-82.

[45] B. Litow and B. Mans. “A Note on the Adam Conjecture for Double Loops”. Information Processing Letters (Elsevier), 66(3), pp. 149-153, May 1998.

[46] J. Liu, A. R. Calderbank. “The Icosian Code and the E_8 Lattice: A New 4×4 Space-Time Code with Non-vanishing Determinant”. ISIT 2006, Seattle, USA, July 9-14 2006.

[47] M. Livingston, F. Quentin. “Perfect Dominating Sets”. In Congressus Numerantium 79 (1990), pp. 187-203.

[48] C. Martínez, R. Beivide, C. Izu and J. Gutierrez. “Distance-Hereditary Embeddings of Circulant Graphs”. Proc. of IEEE Int. Conf. on Information Technology: Coding and Computing (ITCC-2003), pp. 320-324. Las Vegas, April 2003.

[49] C. Martínez, E. Vallejo, R. Beivide, C. Izu and M. Moretó. “Dense Gaussian Networks: Suitable Topologies for On-Chip Multiprocessors”. International Journal of Parallel Programming (ISSN - 0885-7458) Vol: 34 pp. 193-211, June 2006. Springer Netherlands.

[50] C. Martínez, R. Beivide, J. Gutierrez and E. Gabidulin. “Perfect Codes from Circulant Graphs”. Submitted to IEEE Transactions on Information Theory.

[51] C. Martínez, M. Moretó, R. Beivide, E. Gabidulin and E. Stafford. “Mesh Interconnection Networks Modeling Through the Ring of the Gaussian Integers”. Submitted to IEEE Transanctions on Computers.

[52] C. Martínez, R. Beivide, J. Gutierrez and E. Gabidulin. “On the Perfect t-Dominating Set Problem in Circulant Graphs and Codes over Gaussian Integers”. Proceedings of the 2005 IEEE International Symposium on Information Theory (ISIT’05). Adelaide, Australia. September, 2005.

[53] C. Martínez, M. Moretó, R. Beivide and E. Gabidulin. “A Generalization of Perfect Lee Codes over Gaussian Integers”. Proc. 2006 IEEE International Symposium on Information Theory. July 9-14, 2006. The Westin Seattle. Seattle, Washington.

[54] C. Martínez, E. Stafford, R. Beivide and E. Gabidulin. “Perfect Codes over Eisenstein-Jacobi Graphs”. Proc.Thenth International Workshop on Algebraic and Combinatorial Coding Theory. Zvenigorod, Russia, September 03-09 2006.

[55] C. Martínez, E. Stafford, R. Beivide and E. Gabidulin. “Perfect Codes in Metrics Induced by Eisenstein-Jacobi Integers”. Submitted to Problemi Peredachi Informatsii (Problems of Information Transimission), Russian Publication.

[56] C. Martínez, E. Stafford, R. Beivide and E. Gabidulin. “Perfect Codes over Lipschitz Integers”. Submitted to 2007 IEEE International Symposium on Information Theory.

[57] M. E. Muzychuk. “dám’s Conjecture is True in the Square-Free Case”. J. Comb. Theory, Ser. A 72(1): 118-134 (1995).

[58] T. P. da Nóbrega, J. C. Interlando, O. Milaré, M. Eliaand R. Palazzo. “Lattice Constellations and Codes from Quadratic Number Fields”. IEEE Transactions on Information Theory, Vol 47, No 4, May 2001, pp 1514-1527.

[59] P. Lusina, S. Shavgulidze and M. Bossert. “Space-time Block Factorisation Codes over Gaussian Integers”. IEE Proceedings: Communications, vol. 151, no. 5, October, 2004, pp. 415-421.

[60] C. S. Raghavendra, M. Gerla, A. Avizienis. “Reliable Loop Topologies for Large Local Computer Networks”. IEEE Trans. Computers 34(1): 46-55 (1985).

[61] O. Reingold, S. Vadhan and A. Wigderson. “Entropy Waves, The Zig-Zag Graph Product, and New Constant-Degree Expanders and Extractors”. Annals of Mathematics 155, pages 157-187, (2002).

[62] J. Rifà.“Groups of Complex Integers Used as QAM Signals”. IEEE Transactions on Information Theory, vol. 41, no. 5, September 1995.

[63] J. Rifà and J. M. Villanueva. “Error Correcting Codes for QAM from Integer Rings of an Euclidean Complex Quadratic Field”. ISIT 1998, Cambridge, MA, USA, August 16-21.

[64] N. Robertson, D. Sanders, P. Seymour and R. Thomas. “The Four-colour Theorem”. Journal of Combinatorial Theory Series B, Vol 70, No 1, Pag. 2-44 (May 1997)

[65] B. Robic. “Optimal Routing in 2-jump Circulant Networks”. University of Cambridge Computer Laboratory, TR397, 1996.

[66] R. S. Sanders. “Products of Circulant graphs are Metacirculant”. Journal of Combinatorial Theory Series B, vol 85 (2) (2002).

[67] C. H. Sequin. “Doubly Twisted Torus Networks for VLSI Processor Arrays”. 8th Annual International Symposium on Computer Architecture, Minnesota, pp 471-480, 1981.

[68] C. E. Shannon. “A Mathematical Theory of Communication”. Bell System Technical Journal, vol. 27, pp. 379-423 and 623-656, July and October, 1948.

[69] K. G. Shin. “HARTS: A Distributed Real-Time Architecture.” IEEE Computer, vol. 24, no. 5, pp 25-35 (1991).

[70] R. M. Tanner. “A Recursive Approach to Low Complexity Codes”. IEEE Trans. Inform. Theory, Vol. IT-27, No. 5, September, 1981, pp.533-547.

[71] J. Turner. “Point-symmetric Graphs with a Prime Number of Points”. J. Combiantorial Theory Theory, vol. 3, pp. 136-145, 167.

[72] W. Ulrich. “Non-binary Error Correction Codes”. Bell Sys. Tech. J., vol. 36, no. 6 (1957), pp. 1341-1387.

[73] R. S. Wilkov. “Analysis and Design of Reliable Computer Networks”. IEEE Trans. Communications, vol. 20, pp. 660–678, Jun 1972.

[74] C. K. Wong and D. Coppersmith. “A Combinatorial Problem Related to Multimodule Memory Organizations”. Journal of the ACM, Vol. 21, No. 3, pp. 392-402, 1974.

[75] Y. Yang, A. Funashi, A. Jouraku, H. Nishi, H. Amano and T. Sueyoshi. “Recursive Diagonal Torus: An Interconnection Network for Massively Parallel Computers”. IEEE Transactions on Parallel and Distributed Systems, Vol. 12, No. 7, July 2001.