Graphs with Large Girth based on Quaternions and Octonions

Novi Herawati Bong

Erasmus Mundus Master ALGANT

University of Bordeaux 1

Supervisor

Gilles Zemor

July 6, 2011

To Tjhai Po Lew and Bong Khiuk Tjin
for their love, patience, support and wisdom...

Acknowledgements

I would like to thank European Union for supporting the Erasmus Mundus ALGANT Master Program and thank the ALGANT consorsium for letting me to be a part of ALGANT.
I would like to thank to my advisor Prof. Gilles Zemor for the valuable knowledge that he shares to me, for his patience, encouragement and support in guiding me for completing this thesis.
I thank all professors both in Leiden and Bordeaux for valuable knowledge that they share and for showing me the beauty of Mathematics. In particular, my gratitude to Prof. Bas Edixhoven for the motivations, supports and helps, and especially for not giving up on me. Thanks to Prof. Hendrik Lenstra for being a great tutor and for the wise advices with bunch of supports. Thanks to Prof. Yuri Bilu for supports, helps during my second year in Bordeaux and for giving me hope that I am able to finish this program. Thanks to Prof. Qing Liu for being a wonderful tutor for me.
I would like to thank Nicolas Delfosse for the help in using Magma Computer Algebra.
My gratitude to Alberto Passuello for helping me with my Magma program and motivating me to finish my thesis on time.
I would like also to thank all friends in Leiden, in particular, to Dung, Liu, Angela, Valerio for all great time we share, to Katya for all joy and fun we share, to Ataulfo and Ariyan, for helps and supports, to Shoumin, Yujia for the encouraging supports and many thanks to 12G-ers for a warm environment at DUWO home.
To all friends in Bordeaux, it has been my pleasure to spend my second year with you all. In particular, thanks to Martin, Andrii, Olga, Nikola and Farhad for all great moments, thanks to my Indonesian

friends in Bordeaux: Afandi, Olivia and Agung for providing me a home-like environment abroad.
My gratitude to my bachelor advisor, Dr. Kiki Ariyanti Sugeng for keep motivating me, supporting me and encouraging me not to give up during my master program. Thank you very much for all helps and fruitful advices.
Thanks to Gianluigi Pasquinelli for reminding me that universe is always within me to support me.
I want to thank to all my friends, that I might not be able to mention one by one, for all the supports.
Last but not least, thanks to my late father, my mother and my family for the love, strength and endless support.

Deep bow in gratitude to universe that make all these things possible.

Talence, July 6, 2011
Novi Herawati Bong

Contents

List of Figures

Chapter 1

Introduction

The girth of a graph is the length of the smallest cycle in a graph. Given a graph G, there is an upper bound for the girth G (denoted $g(G)$)(see [4]), as follow:

$$\text{for } k \geq 3, \text{ any } k-\text{regular graph } G \text{ verifies: } g(G) \leq 2\log_{k-1}|G|,$$

where $|G|$ denotes the number of vertices of the graph. This motivates the definition of graph with large girth by Biggs [1], that is,
a family $\{G_i\}_i$ of k-regular graphs is of *large girth* if and only if there exists some positive constant c such that for any graph in this family, we have

$$g(G_i) \geq c\log_{k-1}|G_i|.$$

A question might arise in mind, "Why a graph with large girth is interesting?". From the point of view of combinatorics, graphs of large girth which satisfy (or come close to) the upperbound of the girth are extremal object. From the point of view of coding theory, for example: low-density parity-check codes (LDPC), the graph of large girth is needed in order to get a good decoding performance. Margulis [7] first proposed an algebraic construction of LDPC codes of unbounded minimum distance by providing explicit families of regular graphs of large girth.

The research for constructing the large girth graphs has been conducted since long time ago. However, for a long time, the best result was the non-constructive result of Erdos and Sachs [1963] and its improvement by Sauer and Walther which showed the existence of families of graphs with $c = 1$. The first explicit constructions were obtained by Margulis[7], with the constant c strictly smaller than 1.

There are some methods that we can use to construct a graph with large girth. One of them is by using random method to obtain random graph with large girth. In this thesis, we will only discuss about the algebraic approach, that is, the graph construction based on quaternions and octonions algebra. The construction based on quaternions is a result by A. Lubotzky, R. Phillips and P. Sarnak [6], where the construction is a $(p+1)$-regular Cayley graph on the group $\mathrm{PGL}_2(q)$ or $\mathrm{PSL}_2(q)$ depending on the Legendre symbol $\left(\frac{p}{q}\right)$, where p, q are prime numbers with $q > p$, congruent to one modulo 4. This result then improved to any prime numbers greater than 2 in [5]. This graph achieve $c = \frac{4}{3} > 1$ for the bound on the girth.

The idea of the construction is, firstly, we construct $(p+1)$-regular infinite tree in an arithmetic way using quaternion and then obtain the finite graph by taking suitable finite quotients of this tree which do not create small cycles. The regular infinite tree is obtained by constructing a Cayley graph with $p+1$ generators. Those $p+1$ generators are the four tuples (a_0, a_1, a_2, a_3) which are the integer solutions of the equations:

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p,$$

whose a_0 is a positive odd integer and a_j even for $j = 1, 2, 3$ ($p \equiv 1(\mathrm{mod} 4)$), or if $p \equiv 3(\mathrm{mod} 4)$, a_0 is a positive even integer and a_j odd for $j = 1, 2, 3$ together with one of each conjugate pair of the tuples where a_0 is zero and a_j odd for $j = 1, 2, 3$. These tuples are considered later on as an element of quaternion over integer ring, which has norm p.

The set of the vertices of the Cayley graph, which is a set containing those generators will be the set of quaternions α over integer of norm a power of p, such that $\alpha \equiv 1(\mathrm{mod} 2)$ or $\alpha \equiv i + j + k(\mathrm{mod} 2)$, but being quotient by a certain equivalence relation that make this set a group. The generators of the Cayley graph are then the image of those generators in this quotient.

Obtaining a $(p+1)$-regular infinite tree, now, we need to define a suitable finite quotient in order to obtain a finite graph. Taking quaternions over integers modulo a prime q, we arrive to quaternion over a finite field $\mathbb{F}_q$. This mapping is indeed a well-defined homomorphism from the set of vertices defined above to a quaternion over finite field $\mathbb{F}_q$ modulo the center of it. The finite graph will be the Cayley graph of the image of this homomorphism with the symmetric set is the image of the generators of previous Cayley graph under this homomorphism. The girth of this graph will achieve the constant $c = \frac{4}{3}$ if the Legendre symbol $\left(\frac{p}{q}\right) = -1$.

Furthermore, using the isomorphism between the quaternions over $\mathbb{F}_q$ and the set of 2×2 matrices over $\mathbb{F}_q$, we will develop a computer program, using MAGMA Computer Algebra, that will generate the graph and return the result the girth of the graph, given the prime numbers p and q by user. The graph is a Cayley graph over $\mathrm{PGL}_2(q)$ if $\left(\frac{p}{q}\right) = -1$ (bipartite graph) or over $\mathrm{PSL}_2(q)$ if $\left(\frac{p}{q}\right) = 1$ (non-bipartite graph). Unfortunately, due to the lack of the memory, the program is only applicable for small prime numbers.

We will continue the discussion with a result of a better bound. Recently, X. Dahan and J.-P. Tilich [4], succeedly improve the bound from $\frac{4}{3}$ to $\frac{12}{7}$, by mimicking the construction process by Lubotzky et.al, but replacing the quaternion algebra by the octonion algebra. The result is a $(p^3 + 1)$-regular graph, where p is a prime number. However, the construction based on octonions is more complicated than quaternions since it is not associative. The graph is a Cayley graph on loops, not on groups as in quaternions case. Moreover, the vertex-transitivity of the resulting graph is unknown.

The thesis is organized as follows: In Chapter 2, we will give detail construction of the graph based on quaternions, determine the lower bound for the girth, and provide an algorithm of graph construction using Magma computer algebra. In Chapter 3, we will give the detail construction of the finite graph based on octonions that achieve the constant $c = \frac{12}{7}$ for the bound. We will give a short conclusion in Chapter 4. Appendix A is provided to recall about the quaternions and octonions algebra, while Appendix B gives an introduction to Cayley graph, both on groups and on loops. The full Magma program will be provided in Appendix C.

Chapter 2

Construction of Graph with Large Girth Based on Quaternions

In this chapter, we will study the construction of graph with large girth based on quaternions by Davidoff et. al. [5] which is the generalization of the construction by Lubotzky et. al [6].

Given two primes $p = 3$ and $q = 5$. Let the group G be $\mathrm{PGL}_2(\mathbb{F}_5)$ and define a symmetric set

$$S := \{ \begin{bmatrix} 3 & 1 \\ 3 & 2 \end{bmatrix}, \begin{bmatrix} 3 & 2 \\ 4 & 2 \end{bmatrix}, \begin{bmatrix} 3 & 3 \\ 1 & 2 \end{bmatrix}, \begin{bmatrix} 3 & 4 \\ 2 & 2 \end{bmatrix} \}.$$

Consider the Cayley graph $\mathcal{G}(G, S)$ (see Appendix B) which is shown in Figure 2.1.

The graph should be continuosly extended until the number of vertices equal to $|G| = |PGL_2(\mathbb{F}_5)| = 120$ (see that this is a finite graph). However, since we are interested only on the girth, which is the length of the smallest cycle, to simplifiy the picture, we stop drawing the Cayley graph after we find cycles. In Figure 2.1, at that point, there are some vertices appear twice as leaves of the tree, which means, the graph has contained a cycle. The same vertices are denoted by the circle of the same colour. Note that there are 2 pairs of dash circles. The matrices

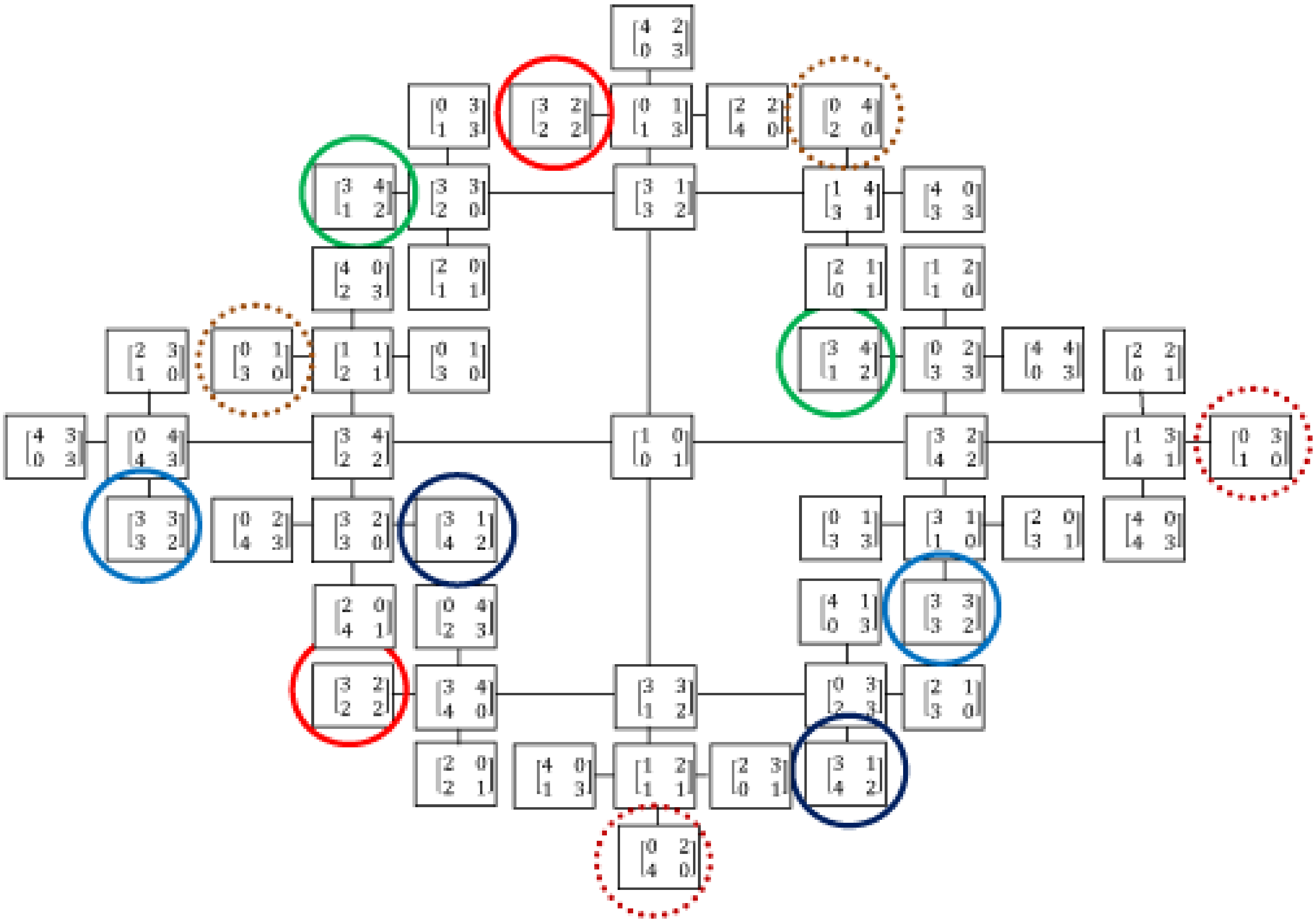

Figure 2.1: Cayley graph $\mathcal{G}(PGL_2(\mathbb{F}_5), S)$

in each pair looks different, but they actually differ only by a scalar matrix. Since we are dealing with $\mathrm{PGL}_2(\mathbb{F}_5)$, matrices that differ by scalar matrices lie in the same equivalence class, thus they coincide. The graph contains 6 cycles of length 6 and there is no smaller cycle, thus, the girth of the graph is 6. Since

$$6 \geq \frac{4}{3}\log_3 120 - \log_3 4 \approx 4.55,$$

this Cayley graph is the graph with large girth that we want (achieving the constant $c = \frac{4}{3}$).

If we replace $\mathbb{F}_5$ by $\mathbb{Z}$, the determinant of matrices in each depth is increasing by the factor of the determinant of the generator and therefore, we will obtain all different vertices. The resulting graph will be a 4-regular infinite tree. Hence, we can say that the graph in Figure 2.1 is actually a quotient of an infinite regular tree.

If we observe further, the set of generators S is not arbitrarily chosen. It is a symmetric set, $S = S^{-1}$, and each element of the set S has determinant $p = 3$. Moreover, we can write elements in the set of generator S in the form:

$$\begin{bmatrix} a_0 + a_1x + a_3y & -a_1y + a_2 + a_3x \\ -a_1y - a_2 + a_3x & a_0 - a_1x - a_3y \end{bmatrix}$$

where $x = 3, y = 0$ satisfying $x^2 + y^2 + 1 = 0$ in $\mathbb{F}_5$. The determinant of the matrices becomes:

$$a_0^2 + a_1^2 + a_2^2 + a_3^2.$$

Hence, to obtain the set of generators, we need to find x, y such that $x^2+y^2+1 \equiv 0(\mathrm{mod} 5)$ and solve the equation:

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = 3.$$

If we see the tuple (a_0, a_1, a_2, a_3) as a quaternion $a_0 + a_1i + a_2j + a_3k$, then the problem of solving the equation above turns to a problem of finding a quaternion with norm 3.

More generally, to construct the desired Cayley graph with large girth, we need to have two different primes p and q, find integers x, y satisfying $x^2 + y^2 + 1 \equiv$

$0(\text{mod} q)$, then solve the equation $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$. By Jacobi's Theorem, there are $8(p+1)$ solutions $\alpha = (a_0, a_1, a_2, a_3)$. Among them (see next section) there are $p+1$ solutions satisfying: a_0 is a positive odd integer and a_j even for $j = 1, 2, 3$ ($p \equiv 1(\text{mod} 4)$), or if $p \equiv 3(\text{mod} 4)$, a_0 is a positive even integer and a_j odd for $j = 1, 2, 3$ together with one of each conjugate pair of the tuples where a_0 is zero and a_j odd for $j = 1, 2, 3$. To each solution α, we associate the matrix $\tilde{\alpha}$ in $\text{PGL}_2(\mathbb{F}_q)$

$$\begin{bmatrix} a_0 + a_1 x + a_3 y & -a_1 y + a_2 + a_3 x \\ -a_1 y - a_2 + a_3 x & a_0 - a_1 x - a_3 y \end{bmatrix}$$

Form the Cayley graph of $\text{PGL}_2(\mathbb{F}_q)$ relative to the above $p+1$ elements. This is a $(p+1)$-regular graph with $n = q(q^2-1)$ vertices. This graph will achieve the constant $c = \frac{4}{3}$ for the bound of the girth whenever $\left(\frac{p}{q}\right) = -1$, i.e. when p is not a square modulo q.

We will elaborate in more detail the construction of the graph in the following sections in this chapter. We will do it in the language of quaternions, since there is an isomorphism between the quaternions $\mathbb{H}(\mathbb{F}_q)$ and the set of 2-by-2 matrices $M_2(\mathbb{F}_q)$. We will start this chapter by constructing the $(p+1)$-regular infinite tree in Section 2.1 and we will show how to define the finite quotients to obtain the desired finite graph in Section 2.2. In Section 2.3, we will determine the lower bound on the girth. In Section 2.4, we will provide an algorithm that deal with the construction of the graph and return the girth of the graph for the given p and q.

2.1 The Construction of the $(p+1)$-Regular Infinite Tree

The $(p+1)$-regular infinite tree is obtained by constructing a Cayley graph on group (see Appendix B) with $p+1$ generators. Hence, we need to define a group (that will be the set of vertices of the graph) and determine the $p+1$ elements of the group to be the generators. Initially, those $p+1$ generators are the four tuples (a_0, a_1, a_2, a_3) which are the integer solutions of the equations:

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p,$$

whose a_0 is a positive odd integer and a_j even for $j = 1, 2, 3$ if $p \equiv 1(\text{mod}4)$, or for the case $p \equiv 3(\text{mod}4)$, it is a tuple where a_0 is a positive even integer and a_j odd for $j = 1, 2, 3$ together with one of each conjugate pair of the tuples where a_0 is zero and a_j odd for $j = 1, 2, 3$.

These solutions exist due to the following theorem of Jacobi [5], that is known in number theory.

Theorem 2.1.1. *Let n be an odd positive integer. Then the number of possible ways to write n as sum of four squares is*

$$8 \sum_{d|n} d$$

Now, let p be an odd prime. Then, by Jacobi's Theorem, the equation:

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$$

has $8(p + 1)$ solutions, where:

- If $p \equiv 1(\text{mod}4)$: Only one of the a_i can be odd and the rest are even.
- If $p \equiv 3(\text{mod}4)$: Only one of the a_i can be even and the rest are odd.

Since the solutions are four tuples (a_0, a_1, a_2, a_3) of integers satisfying $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$, we can consider them as quaternions over integers of norm p (see Appendix A to recall about quaternions). From the $8(p + 1)$ solutions, we need to choose $p + 1$ of them to be generators that satisfied the given criterion. We can do it as follows: denote the distinguished a_i in each case as: a_i^0.
For $p \equiv 1(\text{mod}4)$, the distinguished one, a_i^0 is odd, and hence $a_i^0 \neq 0$. Among the 8 associates $\epsilon\alpha$ of α (ϵ is the unit quaternion), exactly one will have $|a_i^0|$ as its zero-th component. We named this as "distinguished" solution.
For $p \equiv 3(\text{mod}4)$, if $a_i^0 \neq 0$, we define the distinguished solution as in the case $p \equiv 1(\text{mod}4)$. If $a_i^0 = 0$, then two associates, $\epsilon\alpha$ and $-\epsilon\alpha$, will each has $a_0 = 0$.

In this case, we may choose either one as distinguished solution.

Now, among $8(p+1)$ solutions, we have found $(p+1)$ distinguished solutions of

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$$

such that each corresponding quaternion solution α satisfies either $\alpha \equiv 1(\bmod 2)$ or $\alpha \equiv i+j+k(\bmod 2)$. If the distinguished coordinate $a_i^0 \neq 0$, then both α and $\bar{\alpha}$ will appear as distinguished solution, but if $a_i^0 = 0$ (which can only appear in the case $p \equiv 3(\bmod 4)$), only one of the pair is included.

Define S_p, the set of all distinguished solutions. Therefore,

$$S_p = \{\alpha_1, \bar{\alpha_1}, \ldots, \alpha_r, \bar{\alpha_r}, \beta_1, \ldots, \beta_s\}$$

where α_i has $a_0^{(i)} > 0, \beta_j$ has $b_0^{(j)} = 0, \alpha_i \bar{\alpha_i} = -\beta_j^2 = p$ and $2r + s = |S_p| = p + 1$.

Having the $p+1$ generators in the form of quaternions over integers, we can move forward to construct the Cayley graph. Now, we need to have the set of quaternions, that will be used as vertices of the graph. The set must contain those generators. In order to do so, define a set of quaternions α over integers of norm a power of p such that $\alpha \equiv 1(\text{mod}2)$ or $\alpha \equiv i+j+k(\text{mod}2)$. This set (denoted by Λ') clearly contains all the $p+1$ generators in S_p. Hence, for a given prime number p,

$$\Lambda' = \{\alpha \in \mathbb{H}(\mathbb{Z}) : \alpha \equiv 1(\text{mod}2)\text{or} \quad \alpha \equiv i+j+k(\text{mod}2), N(\alpha) \quad \text{a power of} \quad p\}.$$

A problem arises because Λ' is not a group. This problem can be overcomed by reducing Λ' modulo the following equivalence relation:

$$\text{for } \alpha, \beta \in \Lambda', \alpha \sim \beta \text{ if there exist } m, n \in \mathbb{N} \text{ such that } p^m\alpha = \pm p^n\beta.$$

We denote $[\alpha]$ the equivalence class of $\alpha \in \Lambda'$. Define

$$\Lambda = \Lambda' / \sim$$

the set of equivalence classes, and

$$Q : \Lambda' \to \Lambda$$

the quotient map $Q(\alpha) = [\alpha]$. Note that $\sim$ is compatible with multiplication, that is, $\alpha_1 \sim \beta_1, \alpha_2 \sim \beta_2$, then $\alpha_1\alpha_2 \sim \beta_1\beta_2$. This shows that Λ comes equipped with an associative product with unit. Therefore, to prove that Λ is a group, it is sufficient to show that every element of Λ has an inverse. This is indeed true because for $\alpha \in \Lambda' : \alpha\bar{\alpha} = \bar{\alpha}\alpha \sim 1$; hence, $[\alpha]^{-1} = [\alpha]$.

With this group, we have to modify our set of generators, since the set of generators should be a subset of the group. Therefore, take the generators to be the image of S_p under the quotient map Q. Note that, for all $\alpha, \beta \in S_p, \alpha \sim \beta$ implies $\alpha = \beta$. So, again, $|Q(S_p)| = p + 1$.

At this point, we have a group Λ and set of generators $Q(S_p) \subset \Lambda$ with cardinality $p+1$. According to Appendix B, we can have a well-defined Cayley graph $\mathcal{G}(\Lambda, Q(S_p))$ if $Q(S_p)$ is symmetry. To see its symmetricity, let $[\delta] \in Q(S_p)$. It corresponds to a $\delta \in S_p$. In the notation of S_p, δ can be either α_i or β_j. If $\delta = \alpha_i$, then we know that there also exists $\bar{\alpha_i} \in S_p$, which means $[\bar{\alpha_i}] \in Q(S_p)$. Since $\alpha_i\bar{\alpha_i} = p$, then $[\bar{\alpha_i}] \in Q(S_p)$ is the inverse of $[\delta] = [\alpha_i]$, because $[\alpha_i][\bar{\alpha_i}] = [p] = [1]$ in Λ. Now, consider the case $\delta = \beta_j$. Since

$$-\beta_j = -1(\beta_j) = -p^0\beta_j,$$

this implies that $[\beta_j] = [-\beta_j]$ in Λ. And since $-\beta_j^2 = p$, then $[\delta]^2 = [\beta_j][-\beta_j] = [p] = [1]$ in Λ. For every element $[\delta] \in Q(S_p)$, we can find its inverse in $Q(S_p)$, this shows that $Q(S_p)$ is symmetry.

Now, we have constructed the Cayley graph $\mathcal{G}(\Lambda, Q(S_p))$. This graph is the $(p+1)$-regular tree that we want. However, in order to prove that it is a regular tree, we need to study the factorization of quaternions over integers into primes.

We know that there is no unique factorization into primes in $\mathbb{H}(\mathbb{Z})$ (not even up to associate), for example, we can write

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

Fortunately, for the set of integral quaternions α with $N(\alpha) = p^k$, where p is an odd rational prime (hence, for α in Λ'), we can recover a sort of unique factorization for these α's. Before we go on for the factorization, we need to have the following definition.

Definition 2.1.2. A *reduced word* over S_p is a word over the alphabet S_p, which has no subword of the form $\alpha_i\bar{\alpha}_i, \bar{\alpha}_i\alpha_i, \beta_j^2 (i = 1, \dots, r, j = 1, \dots, s)$. The *length* of a word is the number of occuring symbols.

The following theorem will give the property of the factorization in quaternions over integers.

Theorem 2.1.3. *Let $k \in \mathbb{N}$; let $\alpha \in \mathbb{H}(\mathbb{Z})$ be such that $N(\alpha) = p^k$. Then α admits a unique factorization $\alpha = \epsilon p^r w_m$, where ϵ is a unit in $\mathbb{H}(\mathbb{Z}), w_m$ is a reduced word of length m over S_p, and $k = 2r + m$.*

Proof. We will prove this in two parts.

- Existence
  Let α be a fixed element of $\mathbb{H}(\mathbb{Z})$ with $N(\alpha) = p^k$. As stated in Proposition A.0.9, α is a product of primes in $\mathbb{H}(\mathbb{Z})$:

  $$\alpha = \delta_1\delta_2 \dots \delta_n.$$

  δ_i are all prime quaternions, then by Lemma A.0.8, we have $N(\delta_i) = p \quad (i = 1, \dots n)$. Since norm is multiplicative, then we should have $n = k$. For $N(\delta_i) = p$, we find a unit ϵ_i and $\gamma_i \in S_p$, such that $\delta_i = \epsilon_i\gamma_i$; hence

  $$\alpha = \epsilon_1\gamma_1\epsilon_2\gamma_2 \dots \epsilon_k\gamma_k.$$

  Since for every $\gamma \in S_p$ and every unit ϵ of $\mathbb{H}(\mathbb{Z})$, we can find some $\gamma' \in S_p$ and some unit ϵ', such that $\gamma\epsilon = \epsilon'\gamma'$, then the previous factorization of α can be rewritten in the form:

  $$\alpha = \varepsilon\gamma'_1 \dots \gamma'_k,$$

  with $\gamma'_i \in S_p$ and ϵ unit in $\mathbb{H}(\mathbb{Z})$. Now we found that we have written α as a product of a unit and a word in S_p. However, the word is not necessarily reduced. If it is not reduced, then we can replace each of the factors $\alpha_i\bar{\alpha}_i, \bar{\alpha}_i\alpha_i, \beta_j^2$ that occur in the factorization by p. Moving all p's to the left, we will obtain $\alpha = \epsilon p^r w_m$, where w_m is a reduced word over S_p. This proves the existence.

- Uniqueness

  We will prove uniqueness by a counting argument. From one side, we know that by Jacobi's Theorem, there are exactly

$$8\sum_{i=0}^{k} p^i = 8(\frac{p^{k+1}-1}{p-1})$$

quaternions $\alpha \in \mathbb{H}(\mathbb{Z})$ with $N(\alpha) = p^k$.

From another side, we need to count how many possibility to have α in the form $\alpha = \epsilon p^r w_m$. There are 8 units in $\mathbb{H}(\mathbb{Z})$, hence there are 8 choices for ϵ. For w_m, a reduced word of length m, over S_p, we have 1 choice if $m = 0$ and for $m > 1$, we have $p+1$ choices for the first letter (since $|S_p| = p+1$) and p choices for each of the following letter (since we need to avoid subwords of the form $\alpha_i\bar{\alpha}_i, \bar{\alpha}_i\alpha_i$ and β_j^2). Hence, the number of reduced words of length m can be summarized as:

$$\text{Number of reduced word of length} \quad m = \begin{cases} 1 & \text{if } m = 0, \\ (p+1)p^{m-1} & \text{if } m \geq 1. \end{cases}$$

Hence, the total number of α expressed in this form, is,

$$\begin{cases} 8\left(1 + (p+1)\sum_{r=0}^{\frac{k}{2}-1} p^{k-2r-1}\right) & \text{if } k \quad \text{is even,} \\ 8\left((p+1)\sum_{r=0}^{\frac{k-1}{2}} p^{k-2r-1}\right) & \text{if } k \quad \text{is odd.} \end{cases}$$

In both cases, we find $8\left(\frac{p^{k+1}-1}{p-1}\right)$ expressions. This number coincide with the number that we get from Jacobi's Theorem. Since, by existence part, every such α can be written in such a from, this factorization must be unique.

□

If we restrict our attention only to Λ', not to $\mathbb{H}(\mathbb{Z})$ in general, then Theorem 2.1.3 gives the following corollary:

Corollary 2.1.4. *Every element $\alpha \in \Lambda'$ with $N(\alpha) = p^k$ has a unique factorization $\alpha = \pm p^r w_m$, where $r \in \mathbb{N}, w_m$ is a reduced word of length m over S_p, and $k = 2r + m$.*

Proof. By Theorem 2.1.3, α can be written in a unique way as $\alpha = \epsilon p^r w_m$, with r and w_m having the desired properties and ϵ as a unit in $\mathbb{H}(\mathbb{Z})$. Reducing modulo 2, we get $\alpha \equiv \epsilon w_m (\text{mod} \quad 2)$. Any $\alpha_i, \beta_j \in S_p$ that appears in w_m has $\alpha_i, \beta_j \equiv 1 (\text{mod} \quad 2)$ or $\alpha_i, \beta_j \equiv i + j + k (\text{mod} \quad 2)$. For the moment, denote the latter as γ. Then, in modulo 2, we have the congruences:

$$\alpha \equiv \begin{cases} \epsilon & \text{if an even number of} \quad \gamma\text{'s appears in} \quad w_m, \\ \epsilon(i+j+k) & \text{if an odd number of} \quad \gamma\text{'s appears in} \quad w_m. \end{cases}$$

On the other hand, since $\alpha \in \Lambda', \alpha$ itself must satisfy $\alpha \equiv 1 (\text{mod} \quad 2)$ or $\alpha \equiv i + j + k (\text{mod} \quad 2)$. Therefore , we see that in every case we must have $\epsilon \equiv 1 (\text{mod} \quad 2)$; in other words, $\epsilon = \pm 1$. □

With this knowledge of factorization, now we can prove the following proposition.

Proposition 2.1.5. *The Cayley graph $\mathcal{G}(\Lambda, Q(S_p))$ is the $(p+1)$-regular tree.*

Proof.
- Regularity of the graph.
  By Proposition B.0.18, it is sufficient to prove that $Q(S_p)$ generates Λ. This is true since by the existence part of Corollary 2.1.4, any $\alpha \in \Lambda'$ is equivalent to a reduced word over S_p. Hence, the graph $\mathcal{G}(\Lambda, Q(S_p))$ is $(p+1)$-regular and connected.

- The resulting Cayley graph is a tree.
  To prove that it is a tree, we have to show that it does not contain any circuit. So suppose by contradiction that it does contain a circuit

$$x_0, x_1, x_2, \cdots, x_{g-1}, x_g = x_0$$

of length $g \geq 3$. By vertex-transitivity, we may assume $x_0 = [1]$. By definition of Cayley graph, we have $x_1 = [\gamma_1], x_2 = [\gamma_1\gamma_2], \cdots, x_g = [\gamma_1\gamma_2 \cdots \gamma_g]$ for some $\gamma_1, \gamma_2, \cdots, \gamma_g \in S_p$. Since $x_{k-1} \neq x_{k+1}$ for $1 \leq k \leq n-1$, the word $\gamma_1\gamma_2 \cdots \gamma_g$ over S_p is reduced, i.e. it contains no occurrence of $\alpha_i\bar{\alpha}_i, \bar{\alpha}_i\alpha_i$ or $\beta_j^2 (1 \leq i \leq s; 1 \leq j \leq t)$. The equality $[1] = [\gamma_1\gamma_2 \cdots \gamma_g]$ in Λ becomes, in Λ',

$$p^m = \pm p^n \gamma_1\gamma_2 \cdots \gamma_g.$$

However, since $\gamma_1\gamma_2 \cdots \gamma_g$ is a nontrivial reduced word over S_p, this contradicts the uniqueness part in Corollary 2.1.4, and the proof is complete.

□

2.2 Finite Graph $Y^{p,q}$

Having the infinite $(p+1)$-regular tree, we are now going to define the finite quotient for it. Let q be a prime and we consider reduction modulo q:

$$\tau_q : \mathbb{H}(\mathbb{Z}) \to \mathbb{H}(\mathbb{F}_q)$$

which sends Λ' to the group $\mathbb{H}(\mathbb{F}_q)^\times$ of invertible elements in $\mathbb{H}(\mathbb{F}_q)$. Let Z_q be the following central subgroup of $\mathbb{H}(\mathbb{F}_q)^\times$:

$$Z_q = \{\alpha \in \mathbb{H}(\mathbb{F}_q)^\times : \alpha = \bar{\alpha}\}.$$

Let $\alpha, \beta \in \Lambda'$: if $\alpha \sim \beta$, then $\tau_q(\alpha)^{-1}\tau_q(\beta) \in Z_q$. This means that $\tau_q : \Lambda' \to \mathbb{H}(\mathbb{F}_q)^\times$ descends to a well-defined group homomorphism

$$\Pi_q : \Lambda \to \mathbb{H}(\mathbb{F}_q)^\times / Z_q.$$

We denote the kernel of Π_q by $\Lambda(q)$ and we identify the image of Π_q with the quotient group $\Lambda/\Lambda(q)$. We set

$$T_{p,q} = (\Pi_q \circ Q)(S_p).$$

We define the graph $Y^{p,q}$ as the Cayley graph of $\Lambda/\Lambda(q)$ with respect ot $T_{p,q}$:

$$Y^{p,q} = \mathcal{G}(\Lambda/\Lambda(q), T_{p,q}).$$

The graph $Y^{p,q}$ is the $(p+1)$-regular finite graph as desired. This is true since by Proposition 2.1.5, Λ is generated by $Q(S_p)$ and it follows from Proposition B.0.18 that for $q > 2\sqrt{p}$, the graph $Y^{p,q}$ is regular and connected. The graph $Y^{p,q}$ will be $p+1$-regular if we can show that the cardinality of $T_{p,q}$ is $p+1$. This is given by the following lemma:

Lemma 2.2.1. *If q is large enough with respect to p (for example, if $q > 2\sqrt{p}$), then $|T_{p,q}| = p+1$.*

Proof. We have

$$\Pi_q : \Lambda \to \mathbb{H}(\mathbb{F}_q)^{\times}/Z_q.$$

Since $T_{p,q} = (\Pi_q \circ Q)(S_p)$ and we have already known that $|Q(S_p)| = p+1$, it is sufficient to prove that the map Π_q restricted to $Q(S_p)$ is injective. For simplicity, denote by Π'_q the map Π_q restricted to $Q(S_p)$, that is,

$$\Pi'_q : Q(S_p) \to \mathbb{H}(\mathbb{F}_q)^{\times}/Z_q.$$

Let $[\alpha], [\beta]$ be two different elements in $Q(S_p)$, then they correpond to $\alpha = a_0 + a_1 i + a_2 j + a_3 k, \beta = b_0 + b_1 i + b_2 j + b_3 k \in S_p$, where $a_i \neq b_i$ for some i. By definition, $N(\alpha) = N(\beta) = p$, we have $a_j, b_j \in (-\sqrt{p}, \sqrt{p})$ for $j \in \{0,1,2,3\}$. Thus, if $q > 2\sqrt{p}$, we have $a_i \not\equiv b_i (\text{mod} q)$. Therefore, $[\alpha]$ and $[\beta]$ have different image in $\mathbb{H}(\mathbb{F}_q)^{\times}$. Now, suppose

$$\Pi'_q([\alpha]) = \Pi'_q([\beta])$$

in $\mathbb{H}(\mathbb{F}_q)^{\times}/Z_q$, it means that there exists $\delta \in Z_q$ such that $\Pi'_q([\alpha]) = \delta.\Pi'_q([\beta])$. The δ corresponds to an element $\gamma = c_0 + c_1 i + c_2 j + c_3 k \in \mathbb{H}(\mathbb{Z})$ such that $q | c_1, c_2, c_3$. This implies, $[\alpha] = [\gamma][\beta]$. Since $N(\alpha) = N(\beta) = p$, then $N(\gamma) = 1$, and the fact that $q | c_1, c_2, c_3$ implies $\gamma = \pm 1$. Hence

$$\alpha = \pm\beta \Rightarrow [\alpha] = [\beta].$$

This contradicts to our assumption that $[\alpha], [\beta]$ are two different elements in $Q(S_p)$. □

2.3 Bound on the Girth

Before we are able to determine the lower bound for the girth of $Y^{p,q}$, we need to identify the "congruence subgroup" $\Lambda(q)$.

Lemma 2.3.1. $\Lambda(q) = \{[\alpha] \in \Lambda : \alpha = a_0 + a_1 i + a_2 j + a_3 k, q | a_1, a_2, a_3\}$.

Proof.

$$\begin{aligned} [\alpha] \in \Lambda(q) \quad &\Leftrightarrow \quad \tau_q(\alpha) \in Z_q \\ &\Leftrightarrow \quad q \quad \text{does not divide} \quad a_0 \quad \text{and} \quad q|a_1, a_2, a_3 \\ &\Leftrightarrow \quad q|a_1, a_2, a_3, \end{aligned}$$

where the equivalence between the second and third lines follows from the fact that $N(\alpha)$ is a power of p and $p \neq q$. □

We can now give a lower bound for the girth of $Y^{p,q}$.

Proposition 2.3.2. *One has* $g(Y^{p,q}) \geq 2 \log_p q$*. If* $\left(\frac{p}{q}\right) = -1$*, we have the better inequality* $g(Y^{p,q}) \geq 4 \log_p q - \log_p 4$.

Proof. For simplicity's sake, write g for $g(Y^{p,q})$. Let $x_0, x_1, \cdots, x_{g-1}, x_g = x_0$ be the vertices of a circuit of length g in $Y^{p,q}$. By vertex-transitivity of $Y^{p,q}$ (see Proposition B.0.18), we may assume that $x_0 = x_g = 1$ in $\Lambda/\Lambda(q)$. Since $Y^{p,q}$ is a Cayley graph, we find $t_1, \cdots, t_g \in T_{p,q}$, such that

$$x_i = t_1 t_2 \cdots t_i \quad (1 \leq i \leq g).$$

Now, $t_i = \Pi_q([\gamma_i])$ for a unique $\gamma_i \in S_p \quad (i = 1, \cdots, g)$. Write $\alpha = \gamma_1 \cdots \gamma_g \in \Lambda'$ with $\alpha = a_0 + a_1 i + a_2 j + a_3 k$. Note that α is a reduced word over S_p, and $[\alpha] = [\gamma_1] \cdots [\gamma_g]$ is distinct from $[1]$ in Λ, by Proposition 2.1.5(b). Thus, α is not equivalent to 1 in Λ', which implies that at least one of a_1, a_2, a_3 is nonzero. On the other hand,

$$\Pi_q([\alpha]) = t_1 t_2 \cdots t_g = x_g = 1,$$

so that $[\alpha] \in \Lambda(q)$. By Lemma 2.3.1, the prime q must divide a_1, a_2, a_3. Since one of them is nonzero, we get

$$p^g = N(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2 \geq q^2$$

Taking logarithms in base p, we get the first statement. Suppose now that $\left(\frac{p}{q}\right) = -1$. Since $p^g \equiv a_0^2(\mod q)$, we have

$$1 = \left(\frac{p^g}{q}\right) = \left(\frac{p}{q}\right)^g = (-1)^g,$$

so that g is even, say $g = 2h$. Now actually

$$p^{2h} \equiv a_0^2(\text{mod} q^2).$$

Lemma 2.3.3. *Let q be an odd prime; let a, b be integers, not divisible by q, such that $a^2 \equiv b^2(\text{mod} q^2)$. Then $a \equiv \pm b(\text{mod} q^2)$*

Proof.

$$\begin{aligned} a^2 \equiv b^2(\text{mod} q^2) &\Leftrightarrow a^2 - b^2 \equiv 0(\text{mod} q^2) \\ &\Leftrightarrow (a-b)(a+b) \equiv 0(\text{mod} q^2) \\ &\Leftrightarrow q^2|(a-b)(a+b) \end{aligned}$$

Since $q|q^2|(a-b)(a+b)$ and q is prime, then $q|(a-b)$ or $q|(a+b)$. However, in our case, q cannot divide both in the same time, otherwise

$$q|(a-b) + (a+b) \Rightarrow q|2a \Rightarrow q|a$$

(q is an odd prime, so $q \nmid 2$). This contradicts to the fact that a is not divisible by q. Hence, only one of these holds, $q|(a-b)$ or $q|(a+b)$. We may assume that $q|(a-b)$. This together with the fact that $q^2|(a-b)(a+b)$ implies that $q^2|(a-b)$. Thus, we obtain $a \equiv b(\text{mod} q^2)$. Similarly, for $q|(a+b)$, we obtain

$a \equiv -b (\mathrm{mod} q^2)$. This complete the proof. □

By Lemma 2.3.3 above, it follows that

$$p^h \equiv \pm a_0 (\mathrm{mod} q^2).$$

On the other hand, $a_0^2 \leq p^g$, so $|a_0| \leq p^h$. Assume by contradiction that $g < 4 \log_p q - \log_p 4 = \log_p \frac{q^4}{4}$, so $p^h < \frac{q^2}{2}$ and implies $|p^h \mp a_0| < q^2$. From the previous congruence, we get $p^h = \pm a_0$, then $p^g = a_0^2$, which forces $a_1 = a_2 = a_3 = 0$. This leads to contradiction. □

2.4 Construction of the Graph using Magma Computer Algebra

The idea of developing a computer program is the same as the general abstract construction, except that in the computer program, we represent the quaternions over the finite field $\mathbb{F}_q$ in the form of matrices. This is possible since the following isomorphism exists.

Proposition 2.4.1. *Let K be a field, not of characteristic 2. Assume that there exists $x, y \in K$, such that $x^2 + y^2 + 1 = 0$. Then $\mathbb{H}(K)$ is isomorphic to the algebra $M_2(K)$ of 2×2 matrices over K.*

Proof. Define

$$\begin{array}{rcl} \psi : \mathbb{H}(K) & \to & M_2(K) \\ a_0 + a_1 i + a_2 j + a_3 k & \mapsto & \begin{pmatrix} a_0 + a_1 x + a_3 y & -a_1 y + a_2 + a_3 x \\ -a_1 y - a_2 + a_3 x & a_0 - a_1 x - a_3 y \end{pmatrix} \end{array}$$

By a little calculation, we check that $\psi(q_1 q_2) = \psi(q_1)\psi(q_2)$ for $q_1, q_2 \in \mathbb{H}(K)$. Since ψ is a K-linear map between two K-vector spaces of the same dimension 4, to prove that ψ is an isomorphism it is enough to show that ψ is injective. But $\psi(a_0 + a_1 i + a_2 j + a_3 k) = 0$ leads to a 4-by-4 homogeneous linear system in the variables a_0, a_1, a_2, a_3, with determinant

$$\begin{vmatrix} 1 & x & 0 & y \\ 0 & -y & 1 & x \\ 0 & -y & -1 & x \\ 1 & -x & 0 & -y \end{vmatrix} = -4(x^2 + y^2) = 4 \neq 0.$$

(since char $K \neq 2$). □

The isomorphism exists for $K = \mathbb{F}_q$ because q is an odd prime and the following proposition.

Proposition 2.4.2. *Let q be an odd prime power. There exists $x, y \in \mathbb{F}_q$, such that $x^2 + y^2 + 1 = 0$.*

Proof. Counting 0, there are $\frac{q+1}{2}$ squares in $\mathbb{F}_q$. Define then

$$A_+ = \{1 + x^2 : x \in \mathbb{F}_q\}; A_- = \{-y^2 : y \in \mathbb{F}_q\}.$$

Since $|A_+| = |A_-| = \frac{q+1}{2}$, we have

$$A_+ \cap A_- \neq \emptyset,$$

hence the result. □

The algorithm of the program is as follow:

Algorithm 1 Constructing the Cayley graph and determining the girth

```
Require: $p, q$ prime numbers, $q > 2\sqrt{p}$
Ensure: The girth of finite graph $Y^{p,q}$
  1. (Defining the set $S_p$) Compute the solutions of the equations: $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$.
  if $p \equiv 1(\text{mod} 4)$ then
    include the solutions with $a_0$ an odd positive integer to the set $S_p$
  else
    include the solutions with $a_0$ an odd positive integer and the solutions with $a_0 = 0$ but $a_1 > 0$ to the set $S_p$
  end if
  2. (The generators of the graph that associate to $S_p$ in the form of element of $\text{GL}_2(\mathbb{F}_q)$ ) Find $x, y \in \mathbb{F}_q$ that satisfy $x^2 + y^2 + 1 = 0$. Apply isomorphism in the Proposition 2.4.1 to $S_p$, reduce each entry modulo $q$, to obtain the set of generators in the form matrices in $\text{GL}_2(\mathbb{F}_q)$.
  3. (Initializing set of vertices) Define an array SET of sets of matrices, with SET[0] is the set of Identity matrix of $\text{GL}_2(\mathbb{F}_q)$. Set[$i$] := Set of vertices that has distance $i$ from the identity matrix.
  4. (Constructing the graph) Multiply all elements in SET[$i-1$] with all generators and modulo scalar matrices. SET[$i$] will be the set of the resulting matrices which are not contained in SET[$i-2$].
  5. (Checking girth)
  if SET[$i$]$\cap$ SET[$i-1$] $\neq \emptyset$ then
    STOP
    Output : $2i - 3$.
  else if $|\text{SET}[i]| < (p+1) * p^{(i-1)}$ then
    STOP
    Output: $2i$
  else
    Repeat step 4 with new $i := i + 1$
  end if
```

Chapter 3

Construction of Graph with Large Girth Based on Octonions

We have seen in Chapter 2, the construction of the finite graph based on quaternions that achieve the constant $c = \frac{4}{3}$. In this chapter, we will discuss the result of X. Dahan and J.-P. Tillich in their recent paper[4] about the construction of finite graph that achieve the constant $c = \frac{12}{7}$. The idea of this construction is the same as the construction by A. Lubotzky, R. Phillips and P. Sarnak, replacing the quaternions by octonions.

Given two different primes p, q with $q > p$, we will first construct the infinite regular tree of degree $p^3 + 1$. It will be obtained from the Cayley graph on loops (see Appendix B). Similarly to the Cayley graph on groups, the graph has a set of vertices and the set of generators. However, in this case, the set of vertices will be elements of a loop, instead of a group, and the generators will be the subset of it with the cardinality $(p^3 + 1)$.

In Appendix A, we have described the set of integral elements $\mathcal{C} \subset \mathbb{O}$. We define set of generators $\mathscr{P}(p)$ as follows

$$\mathscr{P}(p) := \{\alpha \in \mathbb{O}(\mathbb{Z}) : \alpha > 0, N(\alpha) = p, \alpha - 1 \in 2\mathcal{C}\}.$$

We will prove in the next section that the cardinality of $\mathscr{P}(p)$ is indeed $p^3 + 1$. The loop Λ that will be the set of vertices of the graph is the set of all irreducible products with elements in $\mathscr{P}(p)$ (with the convention that the void product belongs to it and is equal to 1). Finally, the infinite (p^3+1)- regular tree will be defined as the following Cayley graph

$$\mathcal{G}(\Lambda, \mathscr{P}(p)).$$

(For the detail construction, see Section 3.1.)

Having constructed the infinite (p^3+1)-regular tree, mimicking the construction for quaternions case, we will define finite quotient for the tree. Since all elements in Λ has norm a power of p which is therefore invertible modulo q, then reducting the octonions over integers by a prime q will gives us element is $\mathbb{O}(\mathbb{F}_q)^\times$.

Consider the reduction modulo q:

$$\tau_q : \mathbb{O}(\mathbb{Z}) \to \mathbb{O}(\mathbb{F}_q)^\times.$$

Let Z be the center of $\mathbb{O}(\mathbb{F}_q)^\times$, i.e.

$$Z = \{\alpha \in \mathbb{O}(\mathbb{F}_q)^\times : \alpha = \bar{\alpha}\}.$$

By definition of the product $*$ in the loop Λ (see Section 3.2), we will see that $\tau_q(\alpha * \beta)$ and $\tau_q(\alpha)\tau_q(\beta)$ differ only by element in the center. Hence, taking quotient of the codomain by the center, we obtain the following well-defined map:

$$\Pi_q : \Lambda \to \mathbb{O}(\mathbb{F}_q)^\times / Z.$$

If we denote the kernel of Π_q by $\Lambda(q)$ and set

$$S_{p,q} = \Pi_q(\mathscr{P}(p)),$$

then the finite graph will be:

$$\mathcal{G}(\mathrm{Im}(\Pi_q), S_{p,q}),$$

where $\mathrm{Im}(\Pi_q)$ denotes the image of Π_q. We will prove later in Section 3.3 that this graph achieve the constant $c = \frac{12}{7}$ as desired whenever $\left(\frac{p}{q}\right) = -1$, i.e. when p is not a square modulo q. However, before we are able to determine the girth, we need to know what the image and the kernel of the map Π_q are. This will be given in detail in Section 3.1.

Unfortunately, the actual replacement is not that direct, by just replacing all quaternions with octonions. It gives rise to some problems since octonions is not associative (see Appendix A). The vertex-transitivity of the resulted graph is also unknown, so it brings difficulty to determine the girth. In order to overcome those problems, we need to have some extra properties that will be found throughout this chapter.

3.1 The Construction of the (p^3+1)-Regular Infinite Tree

As mentioned earlier in this chapter, to construct the infinite tree, we will start by defining the set of generators $\mathscr{P}(p)$ that is given by

$$\mathscr{P}(p) := \{\alpha \in \mathbb{O}(\mathbb{Z}) : \alpha > 0, N(\alpha) = p, \alpha - 1 \in 2\mathcal{C}\}.$$

Recall that the set of vertices will be the loop Λ and the infinite (p^3+1)- regular tree will be defined as the following Cayley graph

$$\mathcal{G}(\Lambda, \mathscr{P}(p)).$$

Now, we will show step by step that the graph $\mathcal{G}(\Lambda, \mathscr{P}(p))$ is indeed a (p^3+1)-regular infinite tree and is a Cayley graph on loop (i.e to show that Λ is a loop). It is sufficient to show that the cardinality of $\mathscr{P}(p)$ is equal to p^3+1 and Λ is indeed a loop.

3.1.1 Cardinality of $\mathscr{P}(p)$

In order to determine the cardinality of the set $\mathscr{P}(p)$, we need the following two lemmas. Let us denote reduction modulo p by $\hat{}$ in order not to confuse with the conjugation $(\bar{})$.

Lemma 3.1.1. *If p is a prime number then there are $(p^4-1)(p^3+1)$ classes $\hat{\alpha} \in \hat{\mathcal{C}} = \mathcal{C}/\mathcal{C}p$ such that $\hat{\alpha} \neq 0$ and $\widehat{N(\alpha)} = 0$.*

Proof. Using the isomorphism between $\hat{\mathcal{C}}$ and the vector matrix algebra which respects norm and trace, it is enough to count the vector matrices $A \neq 0$ such that $N(A) = 0$ or the $0 \neq (a, d, \mathbf{b}, \mathbf{c}) \in \mathbb{F}_p^8$ such that $ad = -\mathbf{bc}$.
To count this, suppose

$$\mathbf{b} = (b_1, b_2, b_3), \mathbf{c} = (c_1, c_2, c_3) \in \mathbb{F}_p^3,$$

and write the vector matrix as:

$$\begin{pmatrix} a & b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 & d \end{pmatrix}.$$

In order to satisfy $ad = -\mathbf{bc}$, we can choose the elements of the matrix in two ways:

- There are $p^4 - 1$ ways of choosing the first row to be nonzero, but for second row, we can only choose 3 elements arbitrarily, and the last one depends on all chosen elements. So, there are only p^3 ways to choose the second row.
- If the first row is $\mathbf{0}$ (only one way to do this), then we can choose second row arbitrarily, as long as it is not equal to $\mathbf{0}$. Hence, there are $p^4 - 1$ ways of doing so.

Hence, the total number of the vector matrices that satisfies $0 \neq (a, d, \mathbf{b}, \mathbf{c}) \in \mathbb{F}_p^8$ such that $ad = -\mathbf{bc}$ is:

$$(p^4-1)p^3 + 1(p^4-1) = (p^4-1)(p^3+1).$$

□

Lemma 3.1.2. *If $m \in \mathbb{N}, m > 4$ and $M := \{\alpha \in M | N(\alpha) = m\}$, then the reduction map $M \to \mathcal{C}/\mathcal{C}m$ is injective.*

Now, the following proposition will give the cardinality of $\mathscr{P}(p)$.

Proposition 3.1.3. *If p is an odd prime number then there are exactly p^3+1 prime octonions π such that $n(\pi)=p, \pi \equiv 1(\mathrm{mod}2), \pi > 0$. In other word, the cardinality of $\mathscr{P}(p)$ is equal to p^3+1.*

Proof. For $p=2,3$, this can be established easily by explicit enumeration. Let $p>3$, then $\mathscr{P}(p)=\mathscr{P}$ can be identified (by Lemma 3.1.2) with the subset $\hat{\mathscr{P}}$ of N, where

$$N := \{\hat{\alpha} \in \widehat{\mathfrak{C}} | \widehat{N(\alpha)} = 0, \hat{\alpha} \neq 0\}.$$

For $\hat{\alpha}$ and $\hat{\beta}$ define an equivalence relation as follow: $\hat{\alpha} \sim \hat{\beta}$ if there exists a $\pi \in \mathscr{P}$ such that

$$\widehat{\alpha\overline{\pi}} = 0 = \widehat{\beta\overline{\pi}}.$$

This means that π is a right divisor of representatives α, β of the classes $\hat{\alpha}$, respectively $\hat{\beta}$.

Since $p \nmid \alpha$ but $p \mid N(\alpha)$ we have, by definition of $\mathscr{P}(p)$, a unique $\pi \in \mathscr{P}$ which is a right divisor of α. This implies the transitivity of the relation $\sim$ which is therefore an equivalence relation. Obviously $\hat{\alpha} \sim \hat{\pi}$ hence we may take $\widehat{\mathscr{P}}$ as a full set of representatives of the equivalence classes. The classes are $\widehat{\mathfrak{C}\pi} \backslash \{0\}$ and contain p^4-1 elements because $|\widehat{\mathfrak{C}\pi}| = (\mathfrak{C}\pi : \mathfrak{C}p) = N(\pi)^4 = p^4$ (see Lemma 3.1 in [10]). Using the isomorphism between $\mathfrak{C}/\mathfrak{C}p$ and the Zorn algebra over $\mathbb{F}_p$ we conclude from Lemma 3.1.1 that N contains $(p^4-1)(p^3+1)$ elements. Hence $\hat{\mathscr{P}}$ and $\mathscr{P}$ contain p^3+1 elements. □

3.1.2 The Loop Λ

After proving the cardinality of $\mathscr{P}(p)$, we are going to study the set Λ, which is defined as the set of all irreducible products with elements in $\mathscr{P}(p)$. Consider the products of elements of $\mathfrak{C}$ of the following form

$$\underbrace{(\dots((}_{\text{open brackets}} \ \epsilon\alpha_1)\alpha_2)\alpha_3)\dots)\alpha_s.$$

with $\epsilon \in \mathfrak{C}^\times, \alpha_i \in \mathfrak{C} - \mathfrak{C}^\times$. This product is called *irreducible product* if $\alpha_i \neq \overline{\alpha_{i+1}}$ for $i = 1, \dots, s-1$. For the products of elements of $\mathfrak{C}$ which are not irreducible can be simplified by using Corollary A.0.12.

In order to show that Λ is a loop, we need the main result of Rehm [10], the property of irreducible product in $\mathscr{P}(p)$, and the unique factorization property for certain element in $\mathbb{O}(\mathbb{Z})$, which will be stated below. We will prove them in the next section, when we discuss about the unique factorization of integral octonions in detail.

Theorem 3.1.4. *(**Rehm**) Let $\alpha \in \mathcal{C}$ be primitive. Suppose that $N(\alpha) = p_1 \cdots p_s$ where the p_i's are prime integers, not necessarily distinct. There exists a unique $\epsilon \in \mathcal{C}^\times$ and unique $\pi_i \in \mathscr{P}(p_i)$ for $i = 1, \dots, s$, such that:*

$$\alpha = \underbrace{(\dots((}_{open\ brackets} \quad \epsilon\pi_1)\pi_2)\pi_3)\dots)\pi_s.$$

Lemma 3.1.5. *Any irreducible product $(\dots((\epsilon\pi_1)\pi_2)\pi_3)\dots)\pi_t$ of an invertible element ϵ in $\mathcal{C}^\times$ and elements $\pi_1, \dots, \pi_t$ of $\mathscr{P}(p)$ is primitive.*

Proposition 3.1.6. *Any element $\alpha \in \mathbb{O}(\mathbb{Z})$ of norm $N(\alpha) = p^t$ and with $\alpha \equiv 1(\mathrm{mod} 2\mathcal{C})$, can be uniquely written as:*

$$\alpha = \pm p^s((\dots(\pi_1\pi_2)\cdots\pi_{t-2s-1})\pi_{t-2s},$$

where $((\dots(\pi_1\pi_2)\cdots\pi_{t-2s-1})\pi_{t-2s}$ is an irreducible product with elements $\pi_i \in \mathscr{P}(p)$.

Moreover, we need to endow the set Λ with the following operation.

Definition 3.1.7. Let α, β be two elements of Λ. By Proposition 3.1.6 the element of Λ can be written in a unique way as irreducible products over $\mathscr{P}(p), \alpha = (\dots(\alpha_1\alpha_2)\dots)\alpha_s, \beta = (\dots(\beta_1\beta_2)\cdots)\beta_t$. By using Proposition 3.1.6 again, there exists a unique irreducible product γ in $\mathscr{P}(p)$ such that $\alpha\beta = \pm p^l\gamma$, with $N(\gamma) = p^{s+t-2l}$, that is γ is an irreducible product of length $s + t - 2l$. We define

$$\alpha * \beta = \gamma.$$

This operation implies

Proposition 3.1.8. *The set Λ endowed with the multiplicative law $*$, is a Moufang loop generated by $\mathscr{P}(p)$.*

Proof. Clearly $1 * \alpha = \alpha * 1 = \alpha$ for any $\alpha \in \Lambda$.
Let α be some element of Λ. It belongs to $1 + 2\mathcal{C}$ and is primitive by Lemma 3.1.5. Therefore, this is also the case for $\bar{\alpha}$. By Proposition 3.1.6, we know that either $\bar{\alpha}$ or $-\bar{\alpha}$ belongs to Λ. If $\bar{\alpha} \in \Lambda$, then since $\alpha\bar{\alpha} = p^s$ where $p^s = N(\alpha)$, we obtain $\alpha * \bar{\alpha} = 1$. Similarly for the case $-\bar{\alpha} \in \Lambda$. This show that Λ is a loop.

In order to prove that Λ is a Moufang loop, it is sufficient to show that $*$ satisfies one of the Moufang identities. From the definition of $*$, we can derive the following:

$$\begin{aligned}
(\alpha * (\beta * \alpha)) * \gamma &= (\alpha * (p^{-s_1}\beta\alpha)) * \gamma \\
&= p^{-s_1}(p^{-s_2}\alpha(\beta\alpha)) * \gamma \\
&= p^{-s_1 - s_2}p^{-s_3}(\alpha(\beta\alpha))\gamma
\end{aligned}$$

for some non-negative integers s_1, s_2 and s_3. From the Moufang identities, we have

$$(\alpha(\beta\alpha))\gamma = \alpha((\beta\alpha)\gamma),$$

it implies that

$$(\alpha * (\beta * \alpha)) = \alpha * ((\beta * \alpha) * \gamma).$$

□

The following subsection will provide the proofs for the tools that we used above.

Unique Factorization for Integral Octonions

An integral octonion $\mu \in \mathcal{C}, \mu \neq 0$, is called a *right (left) divisor* of $\alpha \in \mathcal{C}$ if $\alpha\mu^{-1} \in \mathcal{C}$ ($\mu^{-1}\alpha \in \mathcal{C}$, respectively).

Since we are dealing with nonassociative algebra, the usual division algorithm that computes common right divisors of 2 elements of maximal norm, as in associative Euclidean domains, is not applicable. Nevertheless, Rehm[10] provide an algorithm based on Corollary A.0.15 computing left or right factors of α and prescribed norm dividing $N(\alpha)$, as given in the proof of the following proposition.

Proposition 3.1.9. *Let $0 \neq \alpha \in \mathcal{C}, m \in \mathbb{N}$ such that $m|N(\alpha)$. Then there exist at least 240 right and 240 left divisors μ of α such that $N(\mu) = m$.*

(See [10] for the proof) The proposition (and the algorithm) can be used to factorize $\alpha \in \mathcal{C}$. Let us write

$$\prod_{i=0}^{n} \gamma_i = (\cdots((\gamma_0\gamma_1)\gamma_2)\ldots)\gamma_n.$$

Then by induction on n, we will have the following corollary:

Corollary 3.1.10. *Let $\alpha \in \mathcal{C}, N(\alpha) = m_1 \cdots m_n, m_1, \ldots, m_n \in \mathbb{N}$. Then there are integral octaves $\mu_1, \ldots, \mu_n$ such that*

$$\prod_{i=1}^{n} \mu_i \text{ and } N(\mu_i) = m_i \quad (i = 1, \ldots, m)$$

In order to obtain uniqueness property (up to certain requirements), we need the following propositions.

Proposition 3.1.11. *Let $\tau, \tau', \mu, \mu' \in \mathcal{C}$ such that $\alpha = \tau\mu = \tau'\mu', N(\mu) = N(\mu')$ is odd, and $N(\tau)$ and $N(\mu)$ are relatively prime. Then $\mu \equiv \mu' \bmod 2$ implies $\mu = \mu'$ or $\mu = -\mu'$.*

Fix a *total ordering* of $\mathcal{C}$ and make $\mathcal{C}$ an ordered additive group (e.g lexicographic with respect to the coordinates in a fixed $\mathbb{Z}$-base of $\mathcal{C}$). The proposition then gives

Corollary 3.1.12. *Let $\alpha \in \mathcal{C}, N(\alpha) = um, u, m \in \mathbb{N}$ relatively prime, and m odd. Then there are exactly 240 right divisors $\mu \in \mathcal{C}$ of α such that $N(\mu) = m$. Exactly one of these divisors is $\equiv 1 \bmod 2$ and > 0.*

There is also a corollary in the case of norms which are not relatively prime.

Proposition 3.1.13. *Let p be an odd prime number, and $\alpha \in \mathcal{C}$ such that $p \mid N(\alpha)$ and $p \nmid \alpha$. If $\tau, \pi, \tau', \pi' \in \mathcal{C}$, $\alpha = \tau\pi = \tau'\pi'$, and $N(\pi) = N(\pi') = p$, then $\pi = \pi' \bmod 2$ implies $\pi = \pi'$ or $\pi = -\pi'$.*

Proof. By Corollary A.0.15, there exist $\rho, \gamma \in \mathcal{C}$ such that $\alpha = \gamma p + \rho$ and $N(\rho) \leq \frac{1}{2}p^2$. Since

$$N(\alpha) = N(\gamma p) + N(\rho) + tr(\gamma p \bar{\rho}) \text{ and } p \mid N(\alpha)$$

implies p divides $N(\rho)$, thus $N(\rho) = lp$ for some l. Because of $l \leq \frac{1}{2}p$ the numbers l and p are relatively prime and we can apply Proposition 3.1.11 to factorize ρ. But the right divisors π of α and ρ such that $N(\pi) = \bar{\pi}\pi = p$ are the same. □

The argument proving Corollary 3.1.12 now yields this corollary:

Corollary 3.1.14. *Let p, α as in the Proposition 3.1.13. Then there are exactly 240 right divisors $\pi \in \mathcal{C}$ of α such that $N(\pi) = p$. Exactly one of these divisors is $\equiv 1 \bmod 2$ and > 0.*

Therefore, by induction on n, the proposition and the corollary gives the main result of Rehm[10], which has been mentioned in the previous subsection.

Theorem 3.1.4(Rehm) Let $\alpha \in \mathcal{C}$ be primitive. Suppose that $N(\alpha) = p_1 \cdots p_s$ where the p_i's are prime integers, not necessarily distinct. There exist a unique $\epsilon \in \mathcal{C}^\times$ and unique $\pi_i \in \mathscr{P}(p_i)$ for $i = 1, \ldots, s$, such that:

$$\alpha = \underbrace{(\ldots((}_{\text{open brackets}} \epsilon\pi_1)\pi_2)\pi_3)\ldots)\pi_s.$$

Furthermore, consider the products of elements of $\mathcal{C}$ of the following form

$$\underbrace{(\ldots((}_{\text{open brackets}} \epsilon\alpha_1)\alpha_2)\alpha_3)\ldots)\alpha_s.$$

with $\epsilon \in \mathcal{C}^\times, \alpha_i \in \mathcal{C} - \mathcal{C}^\times$. If we restrict our attention to elements in $\mathscr{P}(p) \subset \mathcal{C}$, we will have Lemma 3.1.5 mentioned in previous subsection.

Lemma 3.1.5 Any irreducible product $(\ldots((\epsilon\pi_1)\pi_2)\pi_3)\ldots)\pi_t$ of an invertible element ϵ in $\mathcal{C}^\times$ and elements $\pi_1, \ldots, \pi_t$ of $\mathscr{P}(p)$ is primitive.

Proof. We will prove by contradiction.
Suppose α is an irreducible product of an invertible element and elements of $\mathscr{P}(p)$ of minimal length that is not primitive. Then α can be written as:

$$\alpha = \beta\pi$$

where β is a primitive irreducible product of an invertible element and elements of $\mathscr{P}(p)$ and π is an element of $\mathscr{P}(p)$.

Note: If $\alpha, \gamma \in \mathcal{C}, c(\alpha), c(\gamma)$ denote their content respectively, and $\bar{\pi} \in \mathscr{P}(p)$, then we have:

$$c(\alpha)|c(\alpha\bar{\pi})$$

because the coefficients of $\alpha\bar{\pi}$ are integer linear combinations of the coefficients of α in a $\mathbb{Z}$ basis.

Since

$$\begin{aligned} \alpha\bar{\pi} &= (\beta\pi)\bar{\pi} \\ &= \beta(\pi\bar{\pi}) \text{ by Corollary A.0.12} \\ &= p\beta \end{aligned}$$

This together with the note implies that $c(\alpha) = p$ and that p divides α. Therefore, we may write α as :

$$\alpha = \gamma p = \gamma(\bar{\pi}\pi) = (\gamma\bar{\pi})\pi \text{ (Corollary A.0.12)}$$

for some $\gamma \in \mathcal{C}$.
In the beginning of this proof, we write $\alpha = \beta\pi$, thus, $\beta = \gamma\bar{\pi}$. Since β is primitive, then γ is necessarily primitive. By Theorem 3.1.4 (Rehm), we can write γ uniquely as an irreducible product of a unit ϵ and elements $\pi_1, \dots, \pi_s$ of $\mathscr{P}(p)$:

$$\gamma = (\dots((\epsilon\pi_1)\pi_2)\cdots)\pi_s.$$

This implies that β is of the form:

$$\beta = ((\dots((\epsilon\pi_1)\pi_2)\cdots)\pi_s)\bar{\pi}.$$

This is again an irreducible product, for if $\pi_s = \pi$, then β will be divisible by p, which contradicts to our assumption that β is primitive. Again by applying Theorem 3.1.4, we know that this is the only way we can write β as an irreducible product, and therefore the product α is necessarily of the form:

$$\alpha = \beta\pi = (((\dots((\epsilon\pi_1)\pi_2)\cdots)\pi_s)\bar{\pi})\pi.$$

The occurence of $\bar{\pi}, \pi$ consecutively, implies that the product is no longer irreducible, which contradicts to the irreducibility of α. □

Now, we can prove Proposition 3.1.6 that we mentioned in the previous subsection.

Proposition 3.1.6 Any element $\alpha \in \mathbb{O}(\mathbb{Z})$ of norm $N(\alpha) = p^t$ and with $\alpha \equiv 1(\mathrm{mod} 2\mathfrak{C})$, can be uniquely written as:

$$\alpha = \pm p^s((\dots(\pi_1\pi_2)\cdots\pi_{t-2s-1})\pi_{t-2s},$$

where $((\dots(\pi_1\pi_2)\cdots\pi_{t-2s-1})\pi_{t-2s}$ is an irreducible product with elements $\pi_i \in \mathscr{P}(p)$.

Proof. Given $\alpha \in \mathbb{O}(\mathbb{Z})$ and $N(\alpha) = p^t$. If there is a prime number q dividing α, then q should divide $N(\alpha)$, thus, $q = p$. Therefore, we can write α as:

$$\alpha = p^s\alpha',$$

where s is the largest nonnegative integer such that $p^s|\alpha$ and $p \nmid \alpha'$. Now, we have $\alpha' = p^{-s}\alpha \in \mathbb{O}(\mathbb{Z}) \subset \mathfrak{C}$ which is primitive. We can apply Theorem 3.1.4 to obtain:

$$\alpha' = \underbrace{(\dots((}_{\text{open brackets}}\ \epsilon\pi_1)\pi_2)\pi_3)\dots)\pi_r,$$

where $\epsilon \in \mathfrak{C}^\times$ is unique and $\pi_i \in \mathscr{P}(p)$ for $i = 1, \dots, r$. Taking to the account the norm of α, we must have $r = t - 2s$. We are done with the proof if we are able to show that $\epsilon = \pm 1$.

- First, we will show that the invertible element ϵ is in $\mathbb{O}(\mathbb{Z})$. We will prove by contradiction. Assume that ϵ is not in $\mathbb{O}(\mathbb{Z})$. In other words, $\epsilon \in \mathcal{C}^\times - \mathbb{O}(\mathbb{Z})$

Claim: If $a \in \mathcal{C}^\times - \mathbb{O}(\mathbb{Z})$ and $b \in 1 + 2\mathcal{C}$, then $ab \in \mathcal{C}^\times - \mathbb{O}(\mathbb{Z})$.

Proof: Since a is not in $\mathbb{O}(\mathbb{Z})$, then a must have at least one coordinate in the basis $1, i, j, k, t, it, jt, kt$ which is in the form $\frac{m}{2}$, where m is and odd integer. Since $b \in 1 + 2\mathcal{C}$, then we can write $b = 1 + 2c$, where $c \in \mathcal{C}$. Now, write

$$ab = a(1 + 2c) = a + 2ac.$$

However, $2ac$ is in $\mathbb{O}(\mathbb{Z})$, so ab has some coordinate of the form $\frac{m}{2} + n$, where n is some integer. This shows that ab is not in $\mathbb{O}(\mathbb{Z})$.

If $\epsilon \in \mathcal{C}^\times - \mathbb{O}(\mathbb{Z})$ and we apply the claim recursively, we obtain that

$$\epsilon\pi_1, (\epsilon\pi_1)\pi_2, \ldots, ((\ldots(\epsilon\pi_1)\pi_2)\pi_3)\ldots\pi_{t-2s-1}\big)\pi_{t-2s}$$

are all in $\mathcal{C}^\times - \mathbb{O}(\mathbb{Z})$, so are α' and α, which is a contradiction because we know that $\alpha', \alpha \in 1 + 2\mathcal{C} \subset \mathbb{O}(\mathbb{Z})$.
Therefore, ϵ must be in $\mathbb{O}(\mathbb{Z})$, which means ϵ is among the 16 units of $\mathbb{O}(\mathbb{Z})^\times$.

- We have,

$$\alpha' = ((\ldots(\epsilon\pi_1)\pi_2)\pi_3)\ldots\pi_{t-2s-1}\big)\pi_{t-2s},$$

so, applying Corollary A.0.12.

$$\begin{aligned}
\alpha' &= ((\ldots(\epsilon\pi_1)\pi_2)\pi_3)\ldots\pi_{t-2s-1}\big)\pi_{t-2s} \\
\alpha'\overline{\pi}_{t-2s} &= p((\ldots(\epsilon\pi_1)\pi_2)\pi_3)\ldots\pi_{t-2s-2}\big)\pi_{t-2s-1} \\
&\vdots \\
((\ldots(\alpha'\overline{\pi}_{t-2s})\overline{\pi}_{t-2s-1})\ldots)\overline{\pi}_1 &= p^{t-2s}\epsilon
\end{aligned}$$

So, we have,

$$\epsilon = p^{2s-t}((\ldots(\alpha'\overline{\pi}_{t-2s})\overline{\pi}_{t-2s-1})\ldots\overline{\pi}_2)\overline{\pi}_1.$$

The set 1+2$\mathcal{C}$ is stable by multiplication, therefore $((\ldots(\alpha'\overline{\pi}_{t-2s})\overline{\pi}_{t-2s-1})\ldots\overline{\pi}_2)\overline{\pi}_1$

belongs to $1 + 2\mathcal{C}$ and so does ϵ.

ϵ is an invertible element that is contained in both $\mathbb{O}(\mathbb{Z})$ and also $1 + 2\mathcal{C}$. This can only be satisfied by ± 1. Hence, $\epsilon = \pm 1$. □

3.2 Finite Graph T

We have constructed the infinite (p^3+1)-regular tree. Now, consider the reduction modulo q (as mentioned earlier in this chapter):

$$\tau_q : \mathbb{O}(\mathbb{Z}) \to \mathbb{O}(\mathbb{F}_q)^\times.$$

Let Z be the center of $\mathbb{O}(\mathbb{F}_q)^\times$, i.e.

$$Z = \{\alpha \in \mathbb{O}(\mathbb{F}_q)^\times : \alpha = \bar{\alpha}\}.$$

By definition of the product $*$, the following holds:

$$\tau_q(\alpha * \beta) = \tau_q(\pm p^{-s}\alpha\beta) = \tau_q(\pm p^{-s})\tau_q(\alpha)\tau_q(\beta).$$

This shows that $\tau_q(\alpha * \beta)$ and $\tau_q(\alpha)\tau_q(\beta)$ differ only by element in the center. Hence, taking quotient of the codomain by the center, we obtain the following well-defined map:

$$\Pi_q : \Lambda \to \mathbb{O}(\mathbb{F}_q)^\times / Z.$$

Since $\mathbb{O}(\mathbb{F}_q)^\times$ is a Moufang Loop, $\mathbb{O}(\mathbb{F}_q)^\times/Z$ is also a Moufang Loop. Therefore,

Lemma 3.2.1. *The map Π_q is a homomorphism of Moufang Loops.*

We denote the kernel of Π_q by $\Lambda(q)$, the set

$$S_{p,q} = \Pi_q(\mathscr{P}(p)).$$

and the finite graph T:

$$T := \mathcal{G}(\mathrm{Im}(\Pi_q), S_{p,q}).$$

where $\mathrm{Im}(\Pi_q)$ is the image of Π_q.

Now, we will study further the map Π_q, by determining its image and kernel.

- Image of Π_q.

  Define the following:

  - M_1 : subloops of $\mathbb{O}(\mathbb{F}_q)^\times$ consisting of invertible elements of norm 1;
  - M_p : subloops of $\mathbb{O}(\mathbb{F}_q)^\times$ consisting of invertible elements of norm a power of p;
  - $Z_1 := \{-1, 1\}$;
  - $Z_p := \{\pm p^s, s = 0, 1, \ldots, q-2\}$.

  Since $Z_1 \subset Z_p \subset \mathbb{F}_q^\times$, we can embed the corresponding quotient loops in $\mathbb{O}(\mathbb{F}_q)^\times/Z$ as follows:

$$\begin{array}{ccccc} M_1/Z_1 & \hookrightarrow & M_p/Z_p & \hookrightarrow & \mathbb{O}(\mathbb{F}_q)^\times/Z \\ aZ_1 & \mapsto & aZ_p & & \\ & & bZ_p & \mapsto & bZ \end{array}$$

  Through these embeddings, they can be identified as suloops of $\mathbb{O}(\mathbb{F}_q)^\times/Z$. By result of Paige[9], M_1/Z_1 is a simple Moufang loop and an index 2 normal subloop of $\mathbb{O}(\mathbb{F}_q)^\times/Z$. It follows that

$$M_p/Z_p = M_1/Z_1 \text{ or } \mathbb{O}(\mathbb{F}_q)^\times/Z.$$

  Furthermore,

  Lemma 3.2.2. *Im* $\Pi_q = M_p/Z_p$.

  Proof. ($\subset$) Every element of Λ has norm a power of p, so we have Im $\Pi_q \subset M_p/Z_p$.

  ($\supset$) To proceed, we have to prove the following claim:

  Claim: For any element $\alpha = a_0 + a_1 i + \ldots + a_7 kt \in \mathbb{O}(\mathbb{Z})$ such that $N(\alpha) \equiv p^r (\bmod q)$ for some integer r, there exists an element $\beta = b_0 + b_1 i + \ldots + b_7 kt \in 1 + 2\mathcal{C}$ such that

(i) $a_i \equiv b_i (\text{mod} q)$

(ii) $N(\beta) = p^l$ for some integer l.

Proof of Claim:

To prove the Claim, we use a result of Malyshev [?] on the number of solutions of integral definite-positive quadratic forms, as used in [5].

Note: A result of Malyshev on the number of solutions of integral definite-positive quadratic forms can be described as follows: Let $f(x_1, \ldots, x_n)$ be a quadratic form in $n \geq 4$ variables with integral coefficients and discriminant d. Let m be an integer prime to $2d$. Then there exists some constant depending on $f, K(f)$ such that for any $N \geq K(f)$, N generic for f (i.e $f \equiv N(\text{mod} r)$ has at least one solution for every r), gcd $(m, 2d) = 1$ and for which there exist integers a_i such that

$$\gcd(a_1, \ldots, a_n, m) = 1, f(a_1, \ldots, a_n) \equiv N(\text{mod} m),$$

then there are integers $b_1, \ldots, b_n$ such that

(i) $b_i \equiv a_i (\text{mod} m)$

(ii) $f(b_1, \ldots, b_n) = N$.

We will divide the proof in two cases.

- For case $p \equiv 1(\text{mod} 4)$.

  Define

  $$f(x_0, \ldots, x_7) := x_0^2 + 4(x_1^2 + \ldots + x_7^2).$$

  This is an integral positive definite quadratic form with discriminant $d = 2^7$. Applying the result of Malyshev with integer $m = q$, where q is a prime number greater than p. Clearly, $\gcd(2dp^l, q) = 1$ for any l. Since α is taken with $N(\alpha) \equiv p^r (\text{mod} q)$, then by taking $a'_0 = a_0$ and $a'_i \equiv 2^{-1} a_i (\text{mod} q)$ for

$i = 1, \ldots, 7$, we see that $(a'_0, \ldots, a'_7)$ satisfies

$$f(a'_0, \ldots, a'_7) \equiv p^r (\mathrm{mod} q).$$

We can also find $(a'_0, \ldots, a'_7)$ such that $\gcd(a'_0, \ldots, a'_7, q) = 1$. By Malyshev result, there exist a constant $K(f)$ depending on f. Now, choose l such that $p^l \geq K(f)$ and $p^l \equiv p^r (\mathrm{mod}\ q)$. This p^l is generic for f. Therefore, there exist integers $(b'_0, \ldots, b'_7)$ satisfying

$$b_0'^2 + 4b_1'^2 + \cdots + 4b_7'^2 = p^l.$$

This implies the existence of octonion β of norm equal to p^l, which is congruent to p^r modulo q by setting $b_0 = b'_0, b_i = 2b'_i$ for $i = 1, \ldots, 7$. Since $b_0 \equiv 1(\mathrm{mod}2)$ then it implies that β belongs to $1 + 2\mathfrak{C}$.

· For case $p \equiv 3(\mathrm{mod}4)$.
If l is even, then we can use the same proof as in $p \equiv 1(\bmod 4)$ since in this case $p^l \equiv 1(\mathrm{mod}4)$.
If l is odd, p^l is not generic for f, indeed $f(x_0, \ldots, x_7) \equiv p^l(\mathrm{mod}4)$ has no solution, since it can be reduced to $x_0^2 \equiv 3(\mathrm{mod}4)$ which has no solution. Therefore, we need to consider another quadratic form. Define

$$f(x_0, \ldots, x_7) := 4(x_0^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2) + x_5^2 + x_6^2 + x_7^2.$$

p^l is generic for this f. Moreover, a solution in $\mathbb{Z}^8$ of the equation $f(x_0, \ldots, x_7) = p^l$ gives an element

$$\beta = 2x_0 + 2x_1 i + 2x_2 j + 2x_3 k + 2x_4 t + x_5 it + x_6 jt + x_7 kt$$

of norm p^l. We are done with the proof of the claim if we can show that this β belongs to $1+2\mathcal{C}$.

$$\begin{aligned} f(x_0,\dots,x_7) &= p^l \\ 4(x_0^2+x_1^2+x_2^2+x_3^2+x_4^2)+x_5^2+x_6^2+x_7^2 &= p^l \end{aligned}$$

Reducing modulo 4, we obtain:

$$x_5^2+x_6^2+x_7^2 \equiv 3(\text{mod}4),$$

which implies

$$x_5 \equiv x_6 \equiv x_7 \equiv 1(\text{mod}2).$$

The element

$$\frac{\beta-1}{2} = \frac{2x_0-1}{2}+x_1i+x_2j+x_3k+x_4t+\frac{x_5}{2}it+\frac{x_6}{2}jt+\frac{x_7}{2}kt$$

satisfies the characterization of element of $\mathcal{C}$ which mentioned in Lemma A.0.13. Hence, β is indeed an element in $1+2\mathcal{C}$.

This complete the proof for the claim.

From the claim, in both cases, we obtain an element β in $1+2\mathcal{C}$ of norm p^l. By Proposition 3.1.6, we can write β as follow:

$$\beta = \epsilon p^s \gamma,$$

for some nonnegative integer $s, \epsilon \in \{-1,1\}$ and γ is an irreducible product of elements of $\mathscr{P}(p)$ (i.e. $\gamma \in \Lambda$).

From the construction of β, we have $\tau_q(\alpha) = \tau_q(\beta)$. This implies that $\tau_q(\beta) \in \tau_q(\alpha)Z_p$. From the fact that $\beta = \epsilon p^s\gamma$, we know that $\tau_q(\beta) = \tau_q(\gamma)$. We conclude that

$$\tau_q(\gamma) \in \tau_q(\alpha)Z_p.$$

Since $\gamma \in \Lambda$, then this implies $\tau_q(\alpha)Z_p \in \text{ Im } \Pi_q$.

□

Since M_1/Z_1 is of index 2 in $\mathbb{O}(\mathbb{F}_q)^\times/Z$, the image loop $\Pi_q(\Lambda) = M_p/Z_p$ is either equal to M_1/Z_1 or $\mathbb{O}(\mathbb{F}_q)^\times/Z$. As a direct consequence:

Corollary 3.2.3. – *If* $\left(\frac{p}{q}\right) = 1$*, then Im* $\Pi_q = M_1/Z_1$*.*

– *If* $\left(\frac{p}{q}\right) = -1$*, then Im* $\Pi_q = \mathbb{O}(\mathbb{F}_q)^\times/Z$*.*

Proof. Consider the following loop homomorphism,

$$\begin{array}{rcl} \mathbb{O}(\mathbb{F}_q)^\times & \to & \mathbb{Z}/2\mathbb{Z} \\ \alpha & \mapsto & \left(\dfrac{N(\alpha)}{q}\right) \end{array}$$

By regarding the definition of Z, it factorizes into this homomorphism:

$$\varepsilon : \mathbb{O}(\mathbb{F}_q)^\times/Z \to \mathbb{Z}/2\mathbb{Z}.$$

For $\alpha Z \in \mathbb{O}(\mathbb{F}_q)^\times/Z$ where $N(\alpha) = 1, \alpha Z$ will be mapped to 1 by ε. So, the Kernel of ε contains M_1/Z_1. Now, consider an element $\pi \in \mathscr{P}(p)$. Since $N(\pi) = p$, then the image of $\Pi_q(\pi)$ under the map ε is either 1 or -1 in $\mathbb{Z}/2\mathbb{Z}$, according to the sign of $\left(\frac{p}{q}\right)$.

- If $\left(\frac{p}{q}\right) = -1$, then all $\pi \in \mathscr{P}(p)$ is mapped to -1, thus, the set $\Pi_q(\mathscr{P}(p))$ is not contained in the Ker(ε). In other words,

  $$\Pi_q(\mathscr{P}(p)) \subset \mathbb{O}(\mathbb{F}_q)^\times/Z - M_1/Z_1.$$

  From Lemma 3.2.2, we know that Im$\Pi_q = M_p/Z_p$. Since $\Pi_q(\mathscr{P}(p)) \subset$ Im (Π_q), and M_1/Z_1 is a proper subset of M_p/Z_p, then the Im(Π_q) should strictly contain M_1/Z_1. By Paige's Theorem, this implies that Im$(\Pi_q) = \mathbb{O}(\mathbb{F}_q)^\times/Z$.

- If $\left(\frac{p}{q}\right) = 1$, then

  $$\Pi_q(\mathscr{P}(p)) \subset \text{Ker}(\varepsilon).$$

The multiplicativity of the Legendre symbol shows that $\mathrm{Im}(\Pi_q) \subset \mathrm{Ker}(\varepsilon)$. Since ε is not a trivial map, then $\mathrm{Ker}(\varepsilon) \neq \mathbb{O}(\mathbb{F}_q)^\times/Z$. Hence $\mathrm{Im}(\Pi_q) \subsetneq \mathbb{O}(\mathbb{F}_q)^\times/Z$. Lemma 3.2.2 gives the following:

$$M_1/Z_1 \subset M_p/Z_p = \mathrm{Im}(\Pi_q) \subsetneq \mathbb{O}(\mathbb{F}_q)^\times/Z.$$

By Paige's Theorem, we conclude that $\mathrm{Im}(\Pi_q) = M_1/Z_1$.

□

- Kernel of Π_q

  By definition,

$$\mathrm{Ker}\ \Pi_q = \{\alpha \in \Lambda : \tau_q(\alpha) \in Z\}.$$

Let $\alpha = a_0 + a_1 i + \cdots + a_7 kt$, then α is in the kernel if $q \mid a_i$ for $i = 1, \ldots, 7$, and $N(\alpha) \in \mathbb{F}_q^\times$. The condition for the norm is clearly satisfied by elements in Λ since element in Λ has norm a power of p which is invertible in $\mathbb{F}_q$. If we denote the kernel by $\Lambda(q)$, this gives:

$$Ker(\Pi_q) = \Lambda(q) = \{\alpha \in \Lambda : q \mid a_1, \ldots, q \mid a_7\}.$$

This implies the following isomorphism holds

$$\Lambda/\Lambda(q) \simeq M_p/Z_p$$

Having the more precise form of the Image of Π_q, we will divide our general finite graph T in 2 cases, depending the Legendre symbol $\left(\frac{p}{q}\right)$.

Definition 3.2.4.

- If $\left(\frac{p}{q}\right) = -1$, let $X^{p,q}$ be the Cayley Graph $\mathcal{G}(\mathbb{O}(\mathbb{F}_q)^\times/Z, S_{p,q})$.
- If $\left(\frac{p}{q}\right) = 1$, let $Y^{p,q}$ be the Cayley Graph $\mathcal{G}(M_1/Z_1, S_{p,q})$.

We have $|\mathbb{O}(\mathbb{F}_q)^\times/Z| = q^7 - q^3$ by Lemma 3.1.1. It follows that

$$|X^{p,q}| = q^7 - q^3 \text{ and } |Y^{p,q}| = \frac{1}{2}(q^7 - q^3).$$

Now, we study further about the graph $X^{p,q}$ and $Y^{p,q}$.

Proposition 3.2.5. *The graph $X^{p,q}$ and $Y^{p,q}$ have the following properties:*

(i) The graphs $X^{p,q}$ and $Y^{p,q}$ are connected.

(ii) The graphs $X^{p,q}$ and $Y^{p,q}$ are (p^3+1)-regular.

(iii) The graphs $X^{p,q}$ are bipartite and the graphs $Y^{p,q}$ are not.

Proof. (i) The set $\mathscr{P}(p)$ generates Λ as a loop. The proof of Corollary 3.2.3 has shown that $S_{p,q}$ generates M_1/Z_1, the set of vertices of Y if $\left(\frac{p}{q}\right) = 1$, and it generates $\mathbb{O}(\mathbb{F}_q)^\times/Z$ (the set of vertices of $X^{p,q}$ when $\left(\frac{p}{q}\right) = -1$. Therefore, both $X^{p,q}$ and $Y^{p,q}$ are connected.

(ii) We will prove it in several steps.

- $|S_{p,q}| = p^3+1$.
  Recall that in the previous section, we have proved that $|\mathscr{P}(p)| = p^3+1$. Since $S_{p,q} = \Pi_q(\mathscr{P}(p))$, then it is sufficient to show that two distinct elements of $\mathscr{P}(p)$ are brought by Π_q to distinct elements of $\mathbb{O}(\mathbb{F}_q)^\times/Z$. Let $\pi, \pi' \in \mathscr{P}(p)$ be two distinct elements. To prove by contradiction, suppose that

$$\Pi_q(\pi) = \Pi_q(\pi').$$

It means that $\tau_q(\pi)Z = \tau_q(\pi')Z$ in $\mathbb{O}(\mathbb{F}_q)^\times/Z$. This is equivalent to $\Pi_q(\pi * \bar{\pi}') \in$ Ker $(\Pi_q) = \Lambda(q)$. By definition of kernel, if $\alpha = a - 0 + a_1 i + a_2 j + \ldots + a_7 kt \in$ Ker (Π_q) then q will divides all a_i except a_0. So, by taking norm, we obtain

$$p^2 = a_0^2 + q^2x^2$$

for some $x \in \mathbb{Z}$. If $x \neq 0$, then we get $p^2 \geq q^2$. But this is impossible since we take q to be greater than p.
If $x = 0$, then $\pi * \bar{\pi}' \in Z$, that is $\pi = \pi'$, which contradicts to the fact that they are distinct.

From both cases we obtain a contradiction. We conclude that if $\pi \neq \pi'$ then $\Pi_q(\pi) \neq \Pi_q(\pi')$. Therefore

$$|\mathscr{P}(p)| = p^3 + 1 \Rightarrow |S_{p,q}| = p^3 + 1.$$

- $S_{p,q} = S_{p,q}^{-1}$.
  We already know that if $\pi \in \mathscr{P}(p)$ then its inverse for $*$ is $\bar{\pi}$ and is in $\mathscr{P}(p)$, thus, $\mathscr{P}(p)^{-1} = \mathscr{P}(p)$ for $*$. Since Π_q is an homomorphism on loops and $S_{p,q} = \Pi_q(\mathscr{P}(p))$, it implies that $S_{p,q}^{-1} = S_{p,q}$.
- $1Z \notin S_{p,q}$.
  This is true, otherwise, there would be a $\pi \in \mathscr{P}(p)$ that would also be in $\Lambda(q)$. By the definition of $\Lambda(q)$, we see that this is impossible.

(iii) – The graphs $X^{p,q}$ are bipartite.
We define $X^{p,q}$ for the case $\left(\frac{p}{q}\right) = -1$, with the set of vertices is $\mathbb{O}(\mathbb{F}_q)^\times/Z$. Consider the partition of the set of vertices $A \cup B = \mathbb{O}(\mathbb{F}_q)^\times/Z$ as follows:

$$A := M_1/Z_1 \text{ and } B := \mathbb{O}(\mathbb{F}_q)^\times/Z - M_1/Z_1.$$

Let $v \in A$ be a vertex with $v = \Pi_q(\alpha)$ and let $w = \Pi_q(\beta)$ be a neighbour of v. By construction of Cayley graphs, there exists $\pi \in \mathscr{P}(p)$, such that

$$\Pi_q(\alpha * \pi) = \Pi_q(\alpha)\Pi_q(\pi) = \Pi_q(\beta).$$

This leads to

$$\left(\frac{N(\beta)}{q}\right) = \left(\frac{N(\alpha)p}{q}\right) = \left(\frac{N(\alpha)}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{p}{q}\right) = -1,$$

since $v \in A$ implies $\left(\frac{N(\alpha)}{q}\right) = 1$. This means that $w \in B$. Similarly, any neighbor x of $w \in B$ is in A, so the graph $X^{p,q}$ is bipartite.

- The graphs $Y^{p,q}$ are not bipartite.

We define $Y^{p,q}$ for the case $\left(\frac{p}{q}\right) = 1$, with the set of vertices is M_1/Z_1. AS seen above, a bipartition $A \cup B$ of the set of vertices M_1/Z_1 would imply a non trivial loop homomorphism:

$$M_1/Z_1 \to \mathbb{Z}/2\mathbb{Z}.$$

The kernel of this homomorphism would consist of a non trivial normal subloop of M_1/Z_1, but this is impossible since by Paige's Theorem, M_1/Z_1 is simple.

□

From the fact that bipartite graphs have only even cycles, there is a good lower bound on the size of cycles of even length. Hence, when considering the girth, since $Y^{p,q}$ is not bipartite, we will take the *bipartite double cover* of $Y^{p,q}$ when $\left(\frac{p}{q}\right) = 1$.

Definition 3.2.6. *Double cover of a graph* G with vertex set V and edge set E is the graph with vertex $V' = V \times \{0, 1\}$ and there exists an edge between (x, b) and (x, b') if and only if $\{x, x'\} \in E$ and $b' \neq b$.

Remark 3.2.7. The double cover is a bipartite graph and is connected if and only if G is not bipartite.

3.3 Bound on the Girth

In the quaternion case, the Cayley graph is constructed from a group, so the resulting graph is vertex-transitive. Therefore, for bounding the girth, it is sufficient to consider the lower bound of a cycle starting from vertex with label **1** (identity). This is not the case for construction based on octonions. We do not know whether our construction is vertex transitive or not. However, it is also sufficient to study the cycles starting at the vertex label **1** due to the following two lemmas:

Lemma 3.3.1. *Given $\alpha \in \Lambda$, there is a one-one correspondence between:*

(a) the closed paths without bactracking of length t' starting at the vertex $\Pi_q(\alpha)$, and

(b) the irreducible products in Λ of length t' belonging to the kernel $\Lambda(q)$ of Π_q.

Proof. (a) ⇒ (b) A closed path of length t' without backtracking starting at $\Pi_q(\alpha)$ corresponds to an irreducible product in Λ, of length t', with letters denoted by $\beta_1, \dots, \beta_{t'} \in \mathscr{P}(p)$, such that:

- There is no backtracking, i.e.

$$\forall 2 \leq i \leq t'-1, \Pi_q((\dots(\alpha * \beta_1) * \dots) * \beta_{i+1}) \neq \Pi_q((\dots(\alpha * \beta_1) * \dots) * \beta_{i-1}).$$

- It is a closed path, i.e

$$\text{if } \gamma := (\dots(\alpha * \beta_1) * \dots) * \beta_{t'}, \text{ then } \Pi_q(\alpha) = \Pi_q(\beta).$$

Now, we need to show that the irreducible product $\beta := (\dots(\beta_1\beta_2)\dots)\beta_{t'}$ is in $\Lambda(q)$. Consider

$$\begin{aligned}
\gamma\bar{\beta}_{t'} &= ((\dots(\alpha\beta_1)\dots\beta_{t'-1})\beta_{t'})\bar{\beta}_{t'} \\
&= (\dots(\alpha\beta_1)\dots\beta_{t'-1})(\beta_{t'}\bar{\beta}_{t'}) \text{ by Corollary A.0.12} \\
&= p(\dots(\alpha\beta_1)\dots\beta_{t'-1}) \\
\gamma\bar{\beta}_{t'}\bar{\beta}_{t'-1} &= p((\dots(\alpha\beta_1)\dots\beta_{t'-2})\beta_{t'-1})\bar{\beta}_{t'-1} \\
&= p(\dots(\alpha\beta_1)\dots\beta_{t'-2})(\beta_{t'-1}\bar{\beta}_{t'-1}) \text{ by Corollary A.0.12} \\
&= p^2(\dots(\alpha\beta_1)\dots\beta_{t'-2}) \\
&\vdots \\
\gamma\bar{\beta} &= p^{t'}\alpha
\end{aligned}$$

We have

$$\gamma\bar{\beta} = p^{t'}\alpha \Leftrightarrow \gamma * \bar{\beta} = \alpha \Leftrightarrow \Pi_q(\gamma) * \Pi_q(\bar{\beta}) = \Pi_q(\alpha).$$

By assumption of being a closed path, $\Pi_q(\gamma) = \Pi_q(\alpha)$, we obtain $\Pi_q(\bar{\beta}) = 1Z$, since $\mathbb{O}(\mathbb{F}_q)^\times/Z$ is a loop. This is equivalent to say that $\bar{\beta} \in \ker \Pi_q = \Lambda(q)$, and hence β as well.

(b) $\Rightarrow$ (a) Consider an irreducible product γ in $\Lambda(q)$ of t' elements $\gamma_1, \dots, \gamma_{t'} \in \mathscr{P}(p)$. Define

$$\delta := ((\dots(\alpha\gamma_1)\dots\gamma_{t'-1})\gamma_{t'}.$$

As seen above, $\delta * \bar{\gamma} = \alpha$. It follows that $\Pi_q(\delta * \bar{\gamma}) = \Pi_q(\delta)\Pi_q(\bar{\gamma})$. Since γ is an irreducible product in $\Lambda(q)$, then we have $\Pi_q(\gamma) = 1.Z$. Therefore, we also have $\Pi_q(\bar{\gamma}) = 1.Z$. So, $\Pi_q(\alpha) = \Pi_q(\alpha * \bar{\gamma})$. This corresponds to a path of length t' starting at $\Pi_q(\alpha)$ without backtracking. □

Lemma 3.3.2. *Given $t > 0$, there exists an irreducible product in $\Lambda(q)$ of length $2t$ if and only if $2p^t > q^2$.*

Proof. Let β be an irreducible product in $\Lambda(q)$ of length $2t$, so norm of β, $N(\beta) = p^{2t}$. Moreover, as an element in $\Lambda(q)$, it can be written as:

$$\beta = b_0 + q(b_1 i + b_2 j + \dots + b_7 kt).$$

Combining those two informations, we obtain the following equation:

$$b_0^2 + q^2(b_1^2 + \dots + b_7^2) = p^{2t}.$$

Since we assume that $t > 0$, at least one of the $b_i (i > 0)$ should be nonzero, otherwise, $\beta = b_0$ which means an irreducible product of length 0. Here, we obtain two informations, i.e. $p^{2t} \equiv b_0^2 (\mathrm{mod} q^2)$ and also $b_0^2 < p^{2t}$. By Lemma 2.3.3 in Chapter 2,

$$p^{2t} \equiv b_0^2 (\mathrm{mod} q^2) \Rightarrow p^t \equiv \pm b_0 (\mathrm{mod} q^2),$$

that together with $b_0^2 < p^{2t}$ gives

$$|b_0| < p^t \text{ and } p^t = \pm b_0 + mq^2,$$

for a positive integer m. This implies

$$\begin{aligned} p^{2t} &= (p^t - mq^2)^2 + q^2(b_1^2 + \ldots + b_7^2) \\ &= p^2t - 2mq^2p^t + m^2q^4 + q^2(b_1^2 + \ldots + b_7^2) \\ \Leftrightarrow 2mp^t - m^2q^2 &= b_1^2 + \ldots + b_7^2. \end{aligned}$$

Since at least one $b_i (i > 0)$ is nonzero, then the equality implies $2p^t - mq^2 > 0$ which gives $2p^t > q^2$ since m is a positive integer.

Conversely, if $2p^t > q^2$, then there exists a positive integer m such that

$$2p^t > mq^2 \Rightarrow 2mp^t - m^2q^2 > 0.$$

Since any positive integer is a sum of 5 squares, then we can write $2mp^t - m^2q^2$ as a sum of 7 squares where 2 of them are choosen arbitrarily. Hence, we write

$$2mp^t - m^2q^2 = a_1^2 + \ldots + a_7^2.$$

Take $a_0 = p^t - mq^2$ and let a_1, a_2 be the arbitrary elements. They are chosen in such a way that their parity is different from the parity of a_0. Notice that

$$\begin{aligned} a_0 &\equiv a_0^2 (\text{mod} 2) \\ &\equiv p^{2t} - q^2(a_1^2 + \ldots + a_7^2)(\text{mod} 2) \\ &\equiv 1 + a_1 + \ldots + a_7 (\text{mod} 2) \end{aligned}$$

Since the parity of a_1, a_2 differ from the parity of a_0, then

- if a_0 is even, there are 3, 5 or 7 of the a_i's $(i > 0)$ are odd;
- if a_0 is odd, there are 0, 2, or 4 of the a_i's $(i > 0)$ are odd.

From this, we deduce that there is a suitable permutation of $(a_1, \ldots, a_7)$, such that:

$$(a_4, a_5, a_6, a_7) \equiv (1 - a_0, a_1, a_2, a_3)(\text{mod} 2) \text{ and } a_0 + a_1 + a_2 + a_3 \equiv 1(\text{mod} 2).$$

This implies by using Lemma A.0.13 for the integral octonions $\mathcal{C}$, that $a_0 + q(a_1 i +$

$\ldots + a_7kt)$ lies in $1 + 2\mathfrak{C}$ and therefore also in $\Lambda(q)$. □

Using both lemmas together, we obtain:

Proposition 3.3.3. *The length of the smallest cycles of even length in $X^{p,q}$ or in $Y^{p,q}$ is equal to*

$$2\lceil 2\log_p q - \log_p 2\rceil.$$

Proof. The smallest cycles of even length, call it of length $2t$, exists if and only if there exists an irreducible product of length $2t$ which belongs to $\Lambda(q)$ by Lemma 3.3.1. Applying Lemma 3.3.2, we know that such a product exists if and only if $2p^t > q^2$. The smallest t which satisfies this inequality is clearly equal to $\lceil 2\log_p q - \log_p 2\rceil$. □

Now, we have had sufficient knowledge to prove the main theorem:

Theorem 3.3.4. *For all pairs (p, q) of odd primes such that $p < q$, denoting $k = p^3 + 1$, we have:*

(i) the girth of $X^{p,q}$, denoted as $g(X^{p,q})$, satisfies:

$$g(X^{p,q}) \geq \frac{12}{7}\log_{k-1}|X^{p,q}| - 2\log_p 2.$$

The constant $\frac{12}{7}$ is the largest possible.

(ii) For the non-bipartite graphs $Y^{p,q}$ (defined when $\left(\frac{p}{q}\right) = 1$), the following inequality holds:

$$g(Y^{p,q}) \geq \frac{6}{7}\log k - 1|X^{p,q}| - \log_p 2 = \frac{6}{7}\log_{k-1}|Y^{p,q}| - \frac{5}{7}\log_p 2.$$

Proof. The first part of (i) is a consequence of the fact that $X^{p,q}$ is bipartite, therefore any cycle it contains is of even length. We can apply Proposition 3.3.3 to get the lower bound of the length of such cycle is equal to $2\lceil 2\log_p q - \log_p 2\rceil$. Hence

$$g(X^{p,q}) = 2\lceil 2\log_p q - \log_p 2\rceil = 2\lceil \frac{6}{7}\log_{p^3} q^7 - \log_p 2\rceil \geq \frac{12}{7}\log_{k-1}(q^7 - q^3) - 2\log_p 2,$$

and the first part of (i) follows. The optimality of the constant $\frac{12}{7}$ follows from the fact that

$$g(X^{p,q}) = 2\lceil 2\log_p q - \log_p 2\rceil = (1+o(1))\frac{12}{7}\log_{p^3}(q^7 - q^3) = (1+o(1))\frac{12}{7}\log_{k-1}|X^{p,q}|$$

as q tends to infinity.

To prove (ii), notice that the double cover graph of $Y^{p,q}$ is equal to $X^{p,q}$ by definition and that the length of the smallest cycle of the double cover is at most twice the length of a cycle in $Y^{p,q}$, therefore

$$g(X^{p,q}) \leq 2g(Y^{p,q}),$$

and hence (ii) follows. □

Chapter 4

Conclusions

In this thesis, we have given two explicit constructions of graph with large girth based on quaternions and octonions algebra, which achieve the constant $c = \frac{4}{3}$ and $c = \frac{12}{7}$ respectively. We also created a computer program using Magma computer algebra to construct the graph based on quaternions and determine its girth. In one of the handbook of Magma computer algebra, there is a way to define the octonions algebra using Magma. There might be a possibility to develop a computer program using Magma to construct the graph based on octonions.

In addition, for the quaternion case, Morgenstern [8], finally obtained infinite family of graphs achieving the constant $c = \frac{4}{3}$ for all degrees of the form $k = q+1$ where q is any prime power. The construction is based on quaternions over function fields. It may be interesting to carry over this construction to octonions. There would be indeed a hope to build the graphs of girths $\frac{12}{7} \log_{k-1} n$ for various degrees k, not only of the form $k = p^3 + 1$, with p is a prime number.

Furthermore, the construction of the graph based on octonions by X. Dahan and J.-P. Tillich [] is a Cayley graph on loops. However, they stress that the graphs presented here may be Cayley graphs on groups. The question is: "Which group?". A simpler open problem given by them is the vertex-transitivity of these graphs.

Finally, the main open problem is, of course, whether there is a construction of graphs with large girth that can increase the lower bound. Or, in other words, "is there any possibility to construct graphs with large girth that achieve a constant c greater than $\frac{12}{7}$?"

Appendix A

Quaternions and Octonions Algebra

In this chapter, we will recall about the quaternions algebra and some useful properties of it. We will also give an introduction to octonions algebra, its properties and define the integral octonions.

Quaternions

Definition A.0.5. The *Hamiltonian quaternion algebra* over R, denoted by $\mathbb{H}(R)$, is the associative unital algebra given by the following presentation:

(i) $\mathbb{H}(R)$ is the free R-module over the symbols $1, i, j, k$; that is, $\mathbb{H}(R) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in R\}$;

(ii) 1 is the multiplicative unit;

(iii) $i^2 = j^2 = k^2 = -1$;

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

This definition is natural, in the sense that any unital ring homomorphism $R_1 \to R_2$ extends to a unital ring homomorphism $\mathbb{H}(R_1) \to \mathbb{H}(R_2)$ by mapping 1 to 1, i to i, j to j and k to k.

If $q = a_0 + a_1 i + a_2 j + a_3 k$ is a quaternion, its *conjugate* quaternion is $\bar{q} = a_0 - a_1 i - a_2 j - a_3 k$. The *norm* of q is $N(q) = q\bar{q} = \bar{q}q = a_0^2 + a_1^2 + a_2^2 + a_3^2$. Note that the quaternionic norm, like the Gaussian norm, is multiplicative; that is, given $q_1, q_2 \in \mathbb{H}(R)$,

$$N(q_1 q_2) = N(q_1)N(q_2).$$

Lemma A.0.6. *Let $q \in \mathbb{H}(\mathbb{Z})$, then the following properties are equivalent*

i. *q is invertible in $\mathbb{H}(\mathbb{Z})$;*

ii. $N(q) = 1$

iii. $q \in \{\pm 1, \pm i, \pm j, \pm k\}$

Quaternion that satisfies one of those properties is called *unit.*

Definition A.0.7. A quaternion $\alpha \in \mathbb{H}(\mathbb{Z})$ is *prime* if α is not a unit in $\mathbb{H}(\mathbb{Z})$ and if, whenever $\alpha = \beta\gamma$ in $\mathbb{H}(\mathbb{Z})$, then either β or γ is a unit.

Besides by definition, we can also determine a prime quaternion by the following lemma given in [5]

Lemma A.0.8. *$\alpha \in \mathbb{H}(\mathbb{Z})$ is prime in $\mathbb{H}(\mathbb{Z})$ if and only if $\mathbb{N}(\alpha)$ is prime in $\mathbb{Z}$.*

Now, we have the following factorization

Proposition A.0.9. *Every quaternion $\alpha \in \mathbb{H}(\mathbb{Z})$ is a product of prime quaternions.*

Proof. We proceed by induction over $N(\alpha)$, the case $N(\alpha) = 1$ (i.e. α is invertible) being trivial. Therefore, we may assume that $N(\alpha) > 1$. If α is a prime, there is nothing to prove. Otherwise, α can be written as a product of 2 quaternions, that is : $\alpha = \beta\gamma$, where none of them is a unit, which means $N(\beta), N(\gamma) > 1$. And since the norm is multiplicative, we must have $N(\beta) < N(\alpha), N(\gamma) < N(\alpha)$. Therefore, by induction hypothesis, β, γ are products of prime quaternions, and so is α. □

Octonions

Definition A.0.10. The *octonion algebra* over a ring R, denoted by $\mathbb{O}(R)$ is the 8-dimensional R-module with canonical basis denoted by $1, i, j, k, t, it, jt, kt$ (referred as the *unit bases*), where $1, i, j, k$ is the usual quaternion basis that satisfies

$$i^2 = j^2 = k^2 = -1, ij = k, \tag{A.1}$$

and unit basis $x \neq 1$ satisfies $x^2 = -1$.

We will write $\mathbb{O}(R)$ as $\mathbb{O}$ only when the meaning of R is clear from the context. Here we will choose $R = \mathbb{Z}, \mathbb{Q}, \mathbb{F}_p$.
The *conjugate* of an octonion $\alpha = a_0 + a_1 i + \ldots + a_7 kt$ is defined as:

$$\bar{\alpha} = 2a_0 - \alpha,$$

i.e.

$$\bar{\alpha} = a_0 - a_1 i - \ldots - a_7 kt.$$

It is a (ring) antiautomorphism of $\mathbb{O}$, that is a bijection $\mathbb{O}$ that satisfies for any

$\alpha, \beta \in \mathbb{O}$:

$$\begin{aligned} \bar{1} &= 1 \\ \overline{\alpha+\beta} &= \bar{\alpha}+\bar{\beta} \\ \overline{\alpha\beta} &= \bar{\beta}\bar{\alpha} \end{aligned}$$

If we let the quaternion algebra $\mathbb{H}$ be the R-module with basis $1, i, j, k$, then the octonions can be viewed as $\mathbb{O} = \mathbb{H} + \mathbb{H}t$. The multiplication of octonions is completely determined by the multiplication of quaternions and the rule

$$(\alpha_1 + \alpha_2 t)(\beta_1 + \beta_2 t) = \alpha_1\beta_1 - \bar{\beta}_2\alpha_2 + (\beta_2\alpha_1 + \alpha_2\bar{\beta}_1)t$$

for $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{H}$.
We can check by calculation that octonion algebras are not associative, but are *alternative* algebras:

$$\text{(alternative algebra identities) } (\alpha\alpha)\beta = \alpha(\alpha\beta) \text{ and } \beta(\alpha\alpha) = (\beta\alpha)\alpha.$$

These two conditions are equivalent to the fact that the trilinear map called *associator*

$$[a, b, c] = a(bc) - (ab)c$$

is alternating. It follows that octonion algebras satisfy the *Artin theorem*:

Theorem A.0.11. (Artin) *In an alternative algebra, any two elements generate an associative subalgebra.*

Proof. (See Schafer [11]) □

This theorem gives a corollary that will be used frequently, as follow:

Corollary A.0.12. *Let α, β be elements of $\mathbb{O}(\mathbb{Q})$. Then*

$$(\alpha\beta)\bar{\beta} = \alpha(\beta\bar{\beta}), \alpha(\bar{\alpha}\beta) = (\alpha\bar{\alpha})\beta.$$

In addition, in an alternative algebra, the following rules hold for all α, β, γ :

$$\begin{aligned} (\alpha\beta\alpha)\gamma &= \alpha((\beta\alpha)\gamma) \\ (\alpha\beta)(\gamma\alpha) &= \alpha(\beta\gamma)\alpha \\ ((\beta\alpha)\gamma)\alpha &= \beta(\alpha\gamma\alpha) \end{aligned}$$

These rules are known as *Moufang Rules/Moufang Identities.*

As for quaternions, octonions are also endowed with a *norm* N. If $\alpha = a_0 + a_1 i + \ldots + a_7 kt$ is an octonion, the *norm* of α is defined by

$$N(\alpha) = \alpha\bar{\alpha} = a_0^2 + a_1^2 + \ldots + a_7^2.$$

This norm also has the multiplicativity property, i.e: $N(\alpha\beta) = N(\alpha)N(\beta)$ for any octonions α and β. This follows directly from Theorem A.0.11 and the anti-automorphism property, that

$$N(\alpha\beta) = (\alpha\beta)\overline{\alpha\beta} = (\alpha\beta)(\bar{\beta}\bar{\alpha}) = \alpha(\beta\bar{\beta})\bar{\alpha} = N(\beta)\alpha\bar{\alpha} = N(\alpha)N(\beta).$$

$\alpha \in \mathbb{O}(R)$ is invertible if there exists $\beta \in \mathbb{O}$ such that

$$\begin{aligned} & \alpha\beta = 1 \\ \Leftrightarrow\ & \bar{\alpha}\alpha\beta = \bar{\alpha} \\ \Leftrightarrow\ & N(\alpha)\beta = \bar{\alpha} \\ \Leftrightarrow\ & \beta = N(\alpha)^{-1}\bar{\alpha} \end{aligned}$$

Thus, the inverse of α is $\alpha^{-1} = N(\alpha)^{-1}\bar{\alpha}$. If we denote the set of invertible octonions as $\mathbb{O}(R)^{\times}$, then

$$\mathbb{O}(R)^{\times} = \{\alpha \in \mathbb{O}(R) : N(\alpha) \in R^{\times}\}.$$

An octonion α is called *integral* if $\mathrm{tr}(\alpha) \in \mathbb{Z}$ and $N(\alpha) \in \mathbb{Z}$.

The Set of Integral Elements $\mathcal{C}$

From Definition A.0.10, there are 7 unit bases of octonions. A *triad* is defined as a set of 3 elements among the seven unit bases $\{1, i, j, k, t, it, jt, kt\}$. There are 35 possible triads and among those triads, only 7 are associative, namely:

$$i, j, k, \quad i, t, it, \quad j, t, jt, \quad k, t, kt, \quad k, jt, it, \quad j, it, kt, \quad i, kt, jt.$$

Each of these associative triads, together with the additional basis unit 1, generate a quaternion subalgebra. Moreover, each of the triads related to one $\mathbb{Z}$-module which among them, they are isomorphic.

Let us consider the $\mathbb{Z}$-module that associates to the triad i, j, k. Define

$$h = \frac{1}{2}(i + j + k + t).$$

Now the three octonions i, j, h generate (by multiplication) $k = ij$ and ih, jh, kh. Define $\mathcal{C}$ as a $\mathbb{Z}$-module generated by the eight octonions

$$i, j, k, h, ih, jh, kh.$$

CLAIM 1: $\mathcal{C}$ is closed under multiplication.

Proof. We will list all possible multiplications of the elements of the basis below.

$$i^2 = j^2 = k^2 = h^2 = -1,$$

$$jk = -kj = -ih.h = i, \qquad ki = -ik = -jh.h = j, \qquad ij = -ji = -kh.h = k,$$

$$i.ih = j.jh = k.kh = -h,$$

$$ih.i = -h.ih = h - i \qquad jh.j = -h.jh = h - j, \qquad kh.k = -h.kh = h - k,$$

$$(ih)^2 = hi = -1 - ih, \qquad (jh)^2 = hj = -1 - jh, \qquad (kh)^2 = hk = -1 - kh,$$

$$jh.k = -j - ih, \qquad kh.i = -k - jh, \qquad ih.j = -i - kh,$$

$$kh.j = -k + ih, \qquad ih.k = -i + jh, \qquad jh.i = -j + kh$$

$$jh.ih = k - h - ih, \qquad kh.jh = i - h - jh, \qquad ih.kh = j - h - kh,$$

$$kh.ih = -j + h - ih, \qquad ih.jh = -k + h - jh, \qquad jh.kh = -i + h - kh$$

$$k.jh = -j.kh = 1 + j - k + ih,$$

$$i.kh = -k.ih = 1 + k - i + jh,$$

$$j.ih = -i.jh = 1 + i - j + kh.$$

This proves that $\mathcal{C}$ is closed under multiplication. Moreover, $\mathcal{C}$ is an integral domain. (Note that: a module is called an *integral domain* if it is closed under multiplication). □

CLAIM 2: $\mathcal{C}$ contains 240 units.

Proof. Notice that $\mathcal{C}$ contains the elements:

$$\begin{array}{rl}
t = 2h - i - j - k, & it = 2ih + 1 + j - k, \\
jt = 2jh + 1 + k - i, & kt = 2kh + 1 + i - j, \\
\frac{1}{2}(-1 - j + k + it) = ih, & \frac{1}{2}(i + t + jt - kt) = h + jh - kh - i, \\
\frac{1}{2}(-1 - k + i = jt) = jh, & \frac{1}{2}(j + t + kt - it) = h + kh - ih - j, \\
\frac{1}{2}(-1 - i + j + kt) = kh, & \frac{1}{2}(k + t + it - jt) = h + ih - jh - k, \\
\frac{1}{2}(-1 + it + jt + kt) = 1 + ih + jh + kh, & \frac{1}{2}(i + j + k + t) = h, \\
\frac{1}{2}(-1 + i + t + it_{=}h + ih - k, & \frac{1}{2}(-j - k + jt - kt) = jh - kh - i, \\
\frac{1}{2}(-1 + j + t + jt) = h + jh - i, & \frac{1}{2}(-k - i + kt - it) = kh - ih - j, \\
\frac{1}{2}(-1 + k + t + kt) = h + kh - j, & \frac{1}{2}(-i - j + it - jt) = ih - jh - k,
\end{array}$$

all of which are of unit norm. By adding or substracting $1, i, j, k, t, it, jt$ or kt, we find altogether 240 units:

$$\begin{array}{cc}
\pm 1, \pm i, \pm j, \quad \pm k, \pm t, & \pm it, \pm jt, \pm kt \\
\frac{1}{2}(\pm 1 \pm j \pm k \pm it) & \frac{1}{2}(\pm i \pm t \pm jt \pm kt) \\
\frac{1}{2}(\pm 1 \pm k \pm i \pm jt) & \frac{1}{2}(\pm j \pm t \pm kt \pm it) \\
\frac{1}{2}(\pm 1 \pm i \pm j \pm kt) & \frac{1}{2}(\pm k \pm t \pm it \pm jt) \\
\frac{1}{2}(\pm 1 \pm it \pm jt \pm kt) & \frac{1}{2}(\pm i \pm j \pm k \pm t) \\
\frac{1}{2}(\pm 1 \pm i \pm t \pm it) & \frac{1}{2}(\pm j \pm k \pm jt \pm kt) \\
\frac{1}{2}(\pm 1 \pm j \pm t \pm jt) & \frac{1}{2}(\pm \pm k \pm i \pm kt \pm it) \\
\frac{1}{2}(\pm 1 \pm k \pm t \pm kt) & \frac{1}{2}(\pm i \pm j \pm it \pm jt).
\end{array}$$

(See [3]) □

The last seven rows of the table have the following properties: two elements in the same row have no common terms, but any two elements not in the same row have just two common terms, and the four remaining terms of two such elements form another element of the set.

In general, we have the following characterization for $\mathcal{C}$.

Lemma A.0.13. *$\mathcal{C}$ is the set of octonions of the form*

$$\frac{1}{2}(a_0 + a_1 i + a_2 j + a_3 k + a_4 t + a_5 it + a_6 jt + a_7 kt),$$

where the a_i's are integers which satisfy

$$\begin{aligned}(a_0, a_1, a_2, a_3) &\equiv (a_4, a_5, a_6, a_7)(\text{mod} 2) \text{ if } a_0 + a_1 + a_2 + a_3 \equiv 0(\text{mod} 2),\\ (a_0, a_1, a_2, a_3) &\equiv (1 - a_4, 1 - a_5, 1 - a_6, 1 - a_7)(\text{mod} 2) \text{ if } a_0 + a_1 + a_2 + a_3 \equiv 1(\text{mod} 2).\end{aligned}$$

Coxeter([3] 573) showed that the set $\mathcal{C}$ satisfy the Dickson Criterion to be the set of integral elements.

Besides as a set of integral elements, $\mathcal{C}$ itself is a $\mathbb{Z}$-submodule of $\mathbb{O}$ generated by 8 octonions, so it can also be considered as $\mathbb{Z}$-lattice of rank 8. By exhibiting a fundamental domain of small diameter for the lattice $\mathcal{C}$, Coxeter[3] proves the following theorem:

Theorem A.0.14. *For every $\lambda \in \mathbb{O}$, there is a $\gamma \in \mathcal{C}$ such that*

$$N(\lambda - \gamma) \leq \frac{1}{2}$$

Applying this theorem to $\lambda = \alpha\beta^{-1}$ (Rehm), this theorem gives the following corollary:

Corollary A.0.15. *If $\alpha, \beta \in \mathcal{C}$ and $\beta \neq 0$ then there exist $\gamma, \rho \in \mathcal{C}$ such that $\alpha = \gamma\beta + \rho$ and $N(\rho) \leq \frac{1}{2}N(\beta)$.*

Definition A.0.16. Let α be an element of $\mathcal{C}$.

(a) The *content* of α, denoted by $c(\alpha)$ is the largest rational integer dividing α, i.e. $c(\alpha)$ is the greatest common divisor of the coefficients of α in some $\mathbb{Z}$-base of $\mathcal{C}$.

(b) α is called *primitive* if $c(\alpha) = 1$.

(c) α is called a *prime* if $N(\alpha) = p$ is a prime number.

(d) α is *positive*, written as $\alpha > 0$ if and only if the smallest i such that $a_i \neq 0$ is > 0.

Appendix B

Cayley Graph

In this chapter, we will recall the definition and basic properties of Cayley graph on groups. Moreover, we will introduce the Cayley graph define on loops, that is used in the construction of our graph based on octonions.

Cayley Graph on Groups

Let G be a group (finite or infinite), and let S be a nonempty, finite subset of G. We assume that S is symmetric; that is, $S = S^{-1}$.

Definition B.0.17. The *Cayley graph* $\mathcal{G}(G, S)$ is the graph with vertex set $V = G$ and edge set

$$E = \{\{x, y\} : x, y \in ; \exists s \in S : y = xs\}.$$

Two vertices are adjacent if one is obtained from the other by right multiplication by some element of S. The symmetry of S implies the symmetry of the adjacency relation, so the resulting graph is undirected.

Proposition B.0.18. *Let $\mathcal{G}(G, S)$ be a Cayley graph; set $k = |S|$.*

(a) $\mathcal{G}(G, S)$ is a simple, k-regular, vertex-transitive graph.

(b) $\mathcal{G}(G, S)$ *has no loop if and only if* $1 \notin S$.

(c) $\mathcal{G}(G, S)$ *is connected if and only if* S *generates* G.

(d) If there exists a homomorphism χ *from* G *to the multiplicative group* $\{1, -1\}$*, such that* $\chi(S) = \{-1\}$*, then* $\mathcal{G}(G, S)$ *is bipartite. The converse holds provided* $\mathcal{G}(G, S)$ *is connected.*

Proof. (a) The adjacency matrix of $\mathcal{G}(G, s)$ is

$$A_{xy} = \begin{cases} 1 & \text{if there exists} \quad s \in S \quad \text{such that} \quad y = xs, \\ 0 & \text{otherwise.} \end{cases}$$

From this it is clear that $\mathcal{G}(G, S)$ is simple and k-regular. On the other hand, G acts on the left on $\mathcal{G}(G, S)$ by left multiplication: this action is transitive on $V = G$.

(b) This result is clear.

(c) $\mathcal{G}(G, S)$ is connected if and only if every $x \in G$ is connected to $1 \in G$ by a path of edges. But this holds if and only if every $x \in G$ can be expressed as a word on the alphabet S, that is, if and only if S generates G.

(d) If the homomorphism $\chi : G \to \{\pm 1\}$ is given, then

$$V_{\pm} = \{x \in G : \chi(x) = \pm 1\}$$

defines a bipartition of $\mathcal{G}(G, S)$. For the converse, assume that $\mathcal{G}(G, S)$ is connected and bipartite. Denote by V_+ the class of the bipartition through

$1 \in G$ and by V_- the other class. (Note that $S \subset V_-$.) We then define a map $\chi : G \to \{\pm 1\}$ by

$$\chi(x) = \begin{cases} 1 & \text{if } x \in V_+, \\ -1 & \text{if } x \in V_-. \end{cases}$$

To check that χ is a group homomorphism, we first observe that, since S generates G,

$$\chi(x) = (-1)^{l_S(x)},$$

where $l_S(x)$ is the word length of x with respect to S, hence, the distance from x to 1 in $\mathcal{G}(G,S)$. The fact that $G = V_+ \cup V_-$ then makes it clear that χ is a group homomorphism.

□

Cayley Graph on Loops

Definition B.0.19. A *loop* is a set L with a binary operation $*$, such that

(i) for each a and b in L, there exist unique elements x and y in L such that: $a * x = b$ and $y * a = b$;

(ii) there exists a unique element e such that $x * e = x = e * x$ for all x in L.

It follows that every element of a loop has a unique left and right inverse. A loop where the left and right inverses coincide is called *inverse loop.* We denote in this case by x^{-1} the unique element such that $x * x^{-1} = x^{-1} * x = e$.

Definition B.0.20. A *Moufang loop* is a loop satisfying one of the three equivalent following identities:

$$\text{Moufang identities:}\quad \begin{aligned}(\alpha\beta\alpha)\gamma &= \alpha((\beta\alpha)\gamma)\\ (\alpha\beta)(\gamma\alpha) &= \alpha(\beta\gamma)\alpha\\ ((\beta\alpha)\gamma)\alpha &= \beta(\alpha\gamma\alpha)\end{aligned}$$

Definition B.0.21. (directed/undirected Cayley graph on a loop) Let L be a loop and S be a generating set for it. The directed Cayley graph $\overrightarrow{\mathcal{G}}(L, S)$ is a graph with elements of L as vertices and the set $\{(l, ls), l \in L, s \in S\}$ as edges. The undirected Cayley graph $\mathcal{G}(L, S)$ is obtained from $\overrightarrow{\mathcal{G}}(L, S)$ by replacing each directed edge (l, ls) by an undirected edge $\{l, ls\}$. Equivalently, there is an edge between l and l' if and only if there exists $s \in S$ such that either $l' = ls$ or $l = l's$.

In the previous chapter, we know that for the Cayley graph on a group, the undirected Cayley graph is a $|S|$-regular graph without self-loops if and only if $S = S^{-1}$ and $1 \notin S$. There is a generalization of this property for Cayley graphs on loops.

Proposition B.0.22. *$\mathcal{G}(L, S)$ is a $|S|$-regular graph without loops iff*

(i) For all $l \in L, l \notin lS$,

(ii) $l \in (ls)S$ for any $s \in S$.

Note that if L is a Moufang loop, then this is equivalent to $1 \notin S$ and $S^{-1} = S$, as in group. A problem occur in Cayley graph on loop that it is not necessarily vertex transitive as for Cayley graph on group. This is because the left multiplication by a loop element does not necessarily yield a graph automorphism because of the lack of associativity. However, any regular graph can be realized as Cayley graph on a certain loop [9].

Appendix C

Program with Magma Computer Algebra

```
//Asking for input from user
repeat
print ”Input a prime p = ”;
readi p;
print ”Input a prime q > p”;
readi q;
until IsPrime(p) and IsPrime (q) and q gt p;

// defining Sp
rp:=Floor(SquareRoot(p));
A:=[* *];
Sol:={@ @};
i := 1;
j:=0;
```

```
for a := 0 to rp do
for b:= -Floor(SquareRoot(p-a^2))to Floor(SquareRoot(p-a^2)) do
for c:= -Floor(SquareRoot(p-a^2-b^2)) to Floor(SquareRoot(p-a^2-b^2)) do
for d:= -Floor(SquareRoot(p-a^2-b^2-c^2))to Floor(SquareRoot(p-a^2-c^2)) do
if a^2 +b^2 + c^2 + d^2 eq p then
Append(~A,[a,b,c,d]);
i:=i+1;
end if;
end for;
end for;
end for;
end for;
if IsDivisibleBy((p-1), 4) then
for j:=1 to i-1 do
  if IsOdd(A[j][1]) then
    Include(~Sol, A[j]);
  end if;
end for;
elif IsDivisibleBy ((p-3), 4) then
  for j:=1 to i-1 do
  if IsEven(A[j][1]) then
    if  A[j][1] gt 0 then
    Include(~Sol, A[j]);
  elif A[j][2] gt 0 then
    Include(~Sol, A[j]);
  end if;
  end if;
end for;
end if;

//Finding x,y
I := {};
for m in [0..q-1] do
for n in [0..q-m-1] do
if IsDivisibleBy(m^2+n^2+1, q) then
x:=m;
y:=n;
break;
end if;
end for;
end for;
G:= GeneralLinearGroup(2, q);

//Finding inverse of element in GF(q)
Inv:=function(ni)
if ni eq 1 or ni eq q-1 then
di:= ni;
else
di:= ni^(q-2);
end if;
return di;
end function;
```

```

//Function for reducing matrices
ma:=[* *];
reduction:=function(ma)
if ma[1] ne 0 then
bu:=Inv(ma[1]);
else
bu:=Inv(ma[2]);
end if;
m1:=ma[1]*bu;
m2:=ma[2]*bu;
m3:=ma[3]*bu;
m4:=ma[4]*bu;
return Matrix(FiniteField(q), 2, 2, [m1,m2,m3,m4]);
end function;

//Matrix associate
L:=[* *];
assoc:= function(L)
b1:= (L[1]+x*L[2]+y*L[4])mod q;
b2:= (-y*L[2]+L[3]+x*L[4])mod q;
b3:= (-y*L[2]-L[3]+x*L[4])mod q;
b4:= (L[1]-x*L[2]-y*L[4])mod q;
An:=reduction([b1,b2,b3,b4]);
return An;
end function;
```

```

//Set of generators
Gen:={@ @};
for k:=1 to #Sol do
Include(~Gen, assoc(Sol[k]));
end for;
print ”Psi(Sp)=”, Gen;
print ”The constructed Cayley graph is ”, #Gen, ”-regular”;

//Function to construct the graph
u:=#Gen;
Li:=[* *];
tim:=function(Li, r)
D:= Matrix(FiniteField(q), 2, 2, Li)*Gen[r];
D1:= reduction(ElementToSequence(D));
return D1;
end function;

//Function for Checking the Set of Vertices
bon:=[];
check:= function(bon, z)
if not IsEmpty (bon[z] meet bon[z-1]) then
na:=z; ta:=z-1;
else na:=1; ta:=1;
end if;
return [na, ta];
```

```
end function;

//Constructing the Cayley graph
set:=[];
Insert(~set, 1, {Id(G)});
for h:=1 to q do
lala:={@ @};
Y:=lala;
for x in set[h] do
for k:=1 to u do
CK:=tim(ElementToSequence(x), k);
if h eq 1 then
Y:= Y join Include(lala, CK);
elif h ne 1 and CK notin set[h-1] then
Y:= Y join Include(lala, CK);
end if;
Insert(~set,(h+1), Y);
end for;
end for;

//Checking Cycle and Determining the Girth
U:=check(set, h+1);
if U ne [1,1] then
U;
print ”The girth is equal to”, U[1]+U[2]-2;
break;
```

```
end if;
if #set[h+1] lt (p+1)*p^(h-1) then
print ”The girth is equal to”, 2*h;
break;
end if;
if h gt 3 then //erasing previous unused set
set[h-2]:={@ @};
end if;
end for;

//Theoritical Bound
if LegendreSymbol(p,q) eq -1 then
print ”The graph is bipartite.”;
print ”The lower bound of the girth is”, 4*(Log(q)/Log(p)) - (Log(4)/Log(p));
car:= q^3-q;
else
print ”The graph is nonbipartite.”;
print ”The lower bound of the girth is”, 2*(Log(q)/Log(p));
car:= (q^3-q)/2;
end if;
print ”Moore upper Bound” , 2*(Log(car)/Log(p));
```

References

[1] Norman Biggs. *Algebraic graph theory*. Cambridge University Press, London, 1974. Cambridge Tracts in Mathematics, No. 67. 1

[2] John H. Conway and Derek A. Smith. *On quaternions and octonions: their geometry, arithmetic, and symmetry*. A K Peters Ltd., Natick, MA, 2003.

[3] H. S. M. Coxeter. Integral Cayley numbers. *Duke Math. J.*, 13:561–578, 1946. 57

[4] Xavier Dahan and Jean-Pierre Tillich. Ramanujan graphs of very large girth based on octonions. 2010. 1, 3, 21

[5] Giuliana Davidoff, Peter Sarnak, and Alain Valette. *Elementary number theory, group theory, and Ramanujan graphs*, volume 55 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2003. 2, 4, 8, 35, 50

[6] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988. 2, 4

[7] G. A. Margulis. Explicit constructions of graphs without short cycles and low density codes. *Combinatorica*, 2(1):71–78, 1982. 1, 2

[8] Moshe Morgenstern. Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q. *J. Combin. Theory Ser. B*, 62(1):44–62, 1994. 48

[9] Lowell J. Paige. A class of simple Moufang loops. *Proc. Amer. Math. Soc.*, 7:471–482, 1956. 34, 62

[10] Hans Peter Rehm. Prime factorization of integral Cayley octaves. *Ann. Fac. Sci. Toulouse Math. (6)*, 2(2):271–289, 1993. 25, 26, 27, 28, 29

[11] R. D Schafer. *An Introduction to Nonassociative Algebras*. 52