UNIVERZITET U BEOGRADU

MATEMATIČKI FAKULTET

Hamza Daoub

Konačni Prsteni i Usmereni Grafovi: Razvoj Teorije i Algoritama

DOKTORSKA DISERTACIJA

BEOGRAD, 2013

UNIVERSITY OF BELGRADE

FACULTY OF MATHEMATICS

Hamza Daoub

Finite Rings and Digraphs: Further Development of Theory and Algorithms

DOCTORAL Thesis

BELGRADE, 2013

BELGRADE UNIVERSITY

Abstract

Faculty of Mathematics
Department of Mathematics

Doctor of Philosophy

Finite Rings and Digraphs: Further development of Theory and Algorithms

by HAMZA ELHADI DAOUB

In this thesis, we are going to highligth two different relations between graphs and finite commutative rings. The first one is the well known as Unitary Cayley Graph, where the study of this assocciation and some results are presented from [1]. The second one is a completely different; it connects digraphs with quadratic polynomials with coeffitents in $\mathbb{Z}_n$ under the mapping $(a, b) \longmapsto (a + b, ab)$, for some $n < \infty$. A Computer calculations are involved to support the study. The algorithm which is used for these calculations is built on original Mathematica and Matlab Softwares. Furthermore, Some principles are needed in this thesis for the seek of support and completeness…

Scientific field (naučna oblast): Mathematics (matematika)
Narrow scientific field (uža naučna oblast): Algebra (Algebra)
UDC: 512.7:519.178(043.3)

Podaci o mentoru i članovima komisije:

MENTOR:
Redovni profesor dr. Aleksandar Lipkovski
Matematički fakultet,
Univerzitet u Beogradu

ČLANOVI KOMISIJE :
Redovni profesor dr. Žarko Mijajlović
Matematički fakultet,
Univerzitet u Beogradu

ČLANOVI KOMISIJE :
Vanredni profesor dr. Zoran Petrović
Matematički fakultet,
Univerzitet u Beogradu

ČLANOVI KOMISIJE :
Docent dr. Miroslav Marić
Matematički fakultet,
Univerzitet u Beogradu

ČLANOVI KOMISIJE :
Redovni profesor dr. Miodrag Rašković
Matematički institut SANU,
Univerzitet u Beogradu

Datum odbrane:

Acknowledgements

I would like to thank Allah first, then express my gratitude to my supervisor Aleksandar Lipkovski for all the help he has given me over the last three years, including, but far from limited to, his help in of many of the results contained within. I would like to acknowledge those who shaped my earlier mathematical education: The staff of professor at department of methematics.

Finally I would like to thank my family for the support they have provided throughout not just the last years but my entire life. Most importantly though, I must acknowledge My wife, without whose endless encouragement, patience and love I could not have completed this thesis.

To each of the above, I extend my deepest appreciation.. . .

Contents

List of Figures

List of Tables

This thesis is dedicated to My family…

Chapter 1

Preliminaries

In this chapter, some essential concepts in Commutative rings and graph theory are proposed to the support the introduced associations between graphs and rings; which are presented in the second and third chapters.

1.1 Introduction to Rings

In this section, a short account of Commutative rings with unity is presented. The aim of this presentation is the proper abstract setting for unique factorization theorems for polynomials.

1.1.1 Definitions and Examples of Ring Structure

A ***Comutative ring with unity*** is a ring R that satisfies two more axioms under multiplication;

- The commutative property; that is, $a.b = b.a$ for any $a, b \in R$
- The existence of the unit in R; that is, $a \times 1 = 1 \times a = a$ for all $a \in R$.

Example 1.1.1. *Let $R = \{(a, b) : a, b \in \mathbb{R}\}$. For (a, b) and (c, d) in R; we define an addition and multiplication on R as follows:*

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b).(c, d) = (ac, bd).$$

The ring obtained this way is called the direct product of $\mathbb{R}$.

We will use only ring to avoid the repetition of the phrase "*comutitive ring with unity*". Let R be a ring. An element a of R is a ***unit*** if there is $b \in R$ such that $ab = 1$. The set of units $U(R)$ forms a group and it is called the ***group of units of*** R. A nonzero element, which has no multiplicative inverse will be called a ***proper element***. Thus the elements of R is divided into three classes: zero, units and proper elements.

Remark. The word *subring* has the obvious meaning: a subset of a ring which is a ring under the inherited sum and product.

In what follows we shall often use the chinese reminder theorem (see [2]):

Theorem 1.1.1. *(Chinese remainder theorem). Suppose that $b_1, b_2, ..., b_k$ are k positive integers that are relatively prime in pairs. If $a_1, ..., a_k$ are any integers, then the simultaneous congruences*

$$x \equiv a_i \mod b_i, i = 1, ..., k,$$

have a common solution that is unique modulo $b_1 b_2 ... b_k$.

1.1.2 Ideals

An ***ideal*** in a ring R is a subset I of R such that

1. $0 \in I$;
2. if $a, b \in I$, then $a + b \in I$;
3. if $a \in I$ and $r \in R$, then $ra \in I$.

An ideal $I \neq R$ is called a proper ideal.

Example 1.1.2. *The set I of 2×2 real matrices of the form $\begin{bmatrix} r & 0 \\ 0 & 0 \end{bmatrix}$ with the standard operations form an ideal with multiplicative identity $1_I = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. Note that $I \subseteq R$, the ring of all 2×2 real matrices, but $1_I \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.*

Recall that a subring which is closed under left(right)-multiplication by any element of the ring is called left(right) ideal. ***A princple ideal ring*** is a ring in which every ideal has the form $< a >$. A ***maximal ideal*** is an ideal which is maximal amongst all proper ideals. A ***prime ideal*** is a proper ideal satisfies that; if $a, \in R$ such that $ab \in P$, then $a \in P$ or $b \in P$.

If R is a commutative ring and I is an ideal in R, then the equivalence class of $a \in R$, namely,

$$[a] = \{b \in R : b \equiv a \mod I\}$$

is called the congruence class of $a \mod I$. The set of all the congruence classes mod I is denoted by R/I. This set is called the ***quotient ring*** of R modulo I.

Example 1.1.3. *The set of multiples of an integer n forms an ideal, which is usually denoted by $n\mathbb{Z}$. The ring $\mathbb{Z}_n$ is the quotient ring of $\mathbb{Z}$ modulo the ideal $n\mathbb{Z}$, that is, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.*

A ring R is called ***Artinian***, if, whenever $I_1 \supseteq I_2 \supseteq ... \supseteq I_n \supseteq ...$ is a descending chain of left ideals of R, then there exists an integer k such that $I_j = I_k$ for all $j \geq k$. In other words, there is no infinite properly descending chain of left ideals of R.

We call a ring R ***local*** if R has exactly one maximal ideal I. In this case, we call R/I the residue field of R. A ring with only finitely many maximal ideals is called ***semi-local***.

Example 1.1.4. *The ring of integers $\mathbb{Z}$ is not Artinian since $\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset ...$ is an infinite properly descending chain of ideals. While the ring $\mathbb{Z}_n$ is an Artinian for $n < \infty$.*

One may get immediate from the Lattice Isomorphism Theorem that every quotient R/I of an Artinian ring R by an ideal I is again an Artinian ring.

Let I be an ideal of the commutative ring R and define

$$rad\ I = \{r \in R : r^n \in I\ for\ some\ n \in \mathbb{Z}^+\}$$

called the radical of I.

Let I be an ideal of the commutative ring R and define

$Jac\ I$ to be the intersection of all maximal ideals of R that contain I

where the convention is that $Jac\ R = R$. (If I is the zero ideal, $Jac\ 0$ is called the Jacobson radical of the ring R, so $Jac\ I$ is the preimage in R of the Jacobson radical of R/I.)

In an arbitrary ring an element r such that $r^n = 0$ for some integer $n > 1$ is called ***nilpotent***. An ideal $I \leq R$ is called ***nilradical*** $\Re_R$ if $x \in I$ implies $x^n = 0$ for some positive integer n. We observe that in the ring $\mathbb{Z}_{p^n}$ every nonunit is nilpoten.

Lemma 1.1.1.

1. *(Nakayama's Lemma) If M is any finitely generated $R-$module and $\mathfrak{J}M = M$, then $M = 0$.*
2. *The Jacobson radical contains the nilradical of $R:\ rad0 \subset JacR$.*

Lemma 1.1.2. *The following are equivalent:*

1. *R is an Artinian ring.*
2. *Every nonempty set of ideals of R contains a minimal element under inclusion.*

The next result gives the main structure theorem for Artinian rings(e.g [3]).

Theorem 1.1.2. *Let R be an Artinian ring.*

1. *There are only finitely many maximal ideals in R.*
2. *The quotient $R/(JacR)$ is a direct product of a finite number of fields. More precisely, if $M_i, ..., M_n$ are the finitely many maximal ideals in R then*

$$R/(jacR) \cong k_i \times ... \times k_n,$$

where k_i is the field R/M for $1 \leq i \leq n$.

3. *Every prime ideal of R is maximal.*
4. *The ring R is isomorphic to the direct product of a finite number of Artinian local rings.*

Proof. To prove (1), let S be the set of all ideals of R that are the intersection of a finite number of maximal ideals. By lemma 1.1.2, S has a minimal element, say $M_i \cap M_2 \cap ...M_n$. Then for any maximal ideal M we have

$$M \cap M_1 \cap M_2 \cap ...M_n = M_1 \cap M_2 \cap ... \cap M_n,$$

so $M_1 \cap M_2 \cap ... \cap M_n \subseteq M$. According to the fact which says "If R is commutative, I_1 and I_2 be ideals of R and assume P is a prime ideal of R that contains $I_1 I_2$ (for example, if P contains $I_1 \cap I_2$). Then either I_1 or I_2 is contained in P.", $M_i \subset M$ for some i. Thus $M = M_i$ and so $M_1, ..., M_n$ are all the maximal ideals of R.

The proof of (2) is immediate from the Chinese Remainder Theorem applied to $M_1, ..., M_n$, since these maximal ideals are clearly pairwise comaximal and their intersection is $Jac\ R$.

For (3), we first prove $\mathfrak{J} = Jac\ R$ is nilpotent. By descending chain condition. there is some $m > 0$ such that $\mathfrak{J}^m = \mathfrak{J}^{m+1}$ for all positive i. By way of contradiction assume $\mathfrak{J}^m \neq 0$. Let S be the set of proper ideals I such that $I\mathfrak{J}^m \neq 0$, so $\mathfrak{J} \in S$. Let I_0 be a minimal element of S. There is some $x \in I_0$ such that $x\mathfrak{J}^m \neq 0$, so by minimality we must have $I_0 = (x)$. But now $((x)\mathfrak{J})\mathfrak{J}^m = x\mathfrak{J}^{m+1} = x\mathfrak{J}^m$, so it follows by minimality of (x) that $(x) = (x)\mathfrak{J}$. By Nakayama's Lemma, then $(x) = 0$, a contradiction. This proves $Jac\ R$ is nilpotent.

Since $Jac\ R$ is nilpotent, in particular $Jac\ R \subset rad\ 0$, so these two ideals are equal by Lemma1.1.1.

Every prime ideal P in R contains the nilradical of R, hence contains $Jac\ R$ by what has already been proved. The image of P is a prime ideal in the quotient ring $R/(Jac\ R) = k_1 \times ... \times k_n$. But in a direct product of rings $R_1 \times R_2$ (where each R_i has a 1) every ideal is of the form $I_1 \times I_2$, where I_j is an ideal of R_j for $j = 1, 2$. It follows that a prime ideal in $k_1 \times ... \times k_n$ consists of the elements that are 0 in one of the components. In particular, such a prime ideal is also a maximal ideal in $k_1 \times ... \times k_n$ and it follows that P was a maximal ideal in R, which finishes the proof of (3).

Let $M_1, ..., M_n$ be all the distinct maximal ideals of R and let $(Jac\ R)^m = 0$ as in (3). Then

$$\prod_{i=1}^{n} M_i^m \subseteq \left(\prod_{i=1}^{n} M_i\right)^m \subseteq (Jac\ R)^m = 0$$

By the Chinese Remainder Theorem it follows that

$$R = (R/M_1^m) \times (R/M_1^m) \times ... \times (R/M_n^m)$$

and each (R/M_i^m) is an Artinian ring with unique maximal ideal M_i/M_i^m, proving (4). □

A nonzero ring R is an integral domain if, for all $r, s \in R$ with $r \neq 0$, $s \neq 0$, the product $rs \neq 0$. A principal ideal domain (PID) is a domain in which every ideal is principal. A field F is an integral domain such that for every $a \in F$ there is $b \in F$ such that $a.b = 1 \in F$.

Let R be a ring. If $r, s \in R$, then r ***divides*** s if there exists $t \in R$ such that $rt = s$. Two elements r, s are ***associates*** if there is $u \in U(R)$ such that $ru = s$. An element $r \neq 0$ is a ***zero divisor*** if there is $s \neq 0$ in R such that $rs = 0$. Let $r \neq 0$ be in R; r is ***reducible*** if there exist $a, b \in U(R)$ such that $r = ab$; r is ***irreducible*** if r is not reducible. We can now state our most important definition. A ring R, with unity, is a ***unique factorization ring*** (UFR) if for each nonzero nonunit $r \in R$,

1. there exist irreducible elements, $r_1, ..., r_n$, such that $r = r_1...r_n$, and
2. whenever $r = r_1...r_n = s_1...s_m$ where $r_1, ..., r_n, s_1, ..., s_m$, are irreducible, then $n = m$ and each $r_i, 1 \leq i \leq n$, is an associate of some $s_j, 1 \leq j \leq m$, and each s_k is an associate of some r_i.

Let us look to some examples of rings which are not an integral domain; these are $\mathbb{Z}_m$ where m is a nonprime integer greater than 1.

Consider $m = 4$, the first example for which $\mathbb{Z}_m$ is not an integral domain. Let r denote the element $r+ < m >$ of $\mathbb{Z}_m$. Then $U(\mathbb{Z}_4) = \{1, 3\}$ while the nonunits are 0 and 2. Clearly, 2 is irreducible in $\mathbb{Z}_4$; hence $\mathbb{Z}_4$ is a UFR.

Next let $m = 6$; then $U(\mathbb{Z}_6) = \{1, 5\}$ and $R-U(R) = \{O, 2, 3, 4\}$. However, notice that 4 =2.2, 3 = 3.3, and 2= 2.4. Therefore, $\mathbb{Z}_6$ contains no irreducible elements, and hence fails to be a UFR.

The definition of the unique factorization property in domains is quite similar to rings. The only difference is the stucture of the domains where they are without zero divizors.

Proposition 1.1.1. *Consider R be a PID, $a \in R$ and $d = gcd(a, m)$. Then, a and d are associates in R/I where $I =< m >$.*

Proof. We have that a and d are associates if and only if there exists $x \in R$ such that x and m are relatively prime and $a = xd$, that is, $a - xd \in < m >$. So, if there exists $t \in R$ such that $\frac{a}{d} - t\frac{m}{d}$ and m are relatively prime, we set $x = \frac{a}{d} - t\frac{m}{d}$ and the result follows. □

Now, we turn to the study of factorization in R/I. We would like to write every nonzero nonunit element of R/I as a product of weak irreducible elements.

Proposition 1.1.2. *Let $a \neq 0$ be a nonunit element of R/I. Then, a can be written as $a = b.p_1^{n_1}.p_2^{n_2}...p_r^{n_r}$, where b is an unit of R/I, $0 \leq n_i \leq k_i$, $i = 1, 2, ..., r$ and $m = p_1^{k_1}.p_2^{k_2}...p_r^{k_r}$ is the irreducible factorization of m in R. Also, this factorization is unique.*

Proof. From the Proposition 1.1.1 above, we have that a and d are associates, where $d = gcd(a, m)$. Since d is a divisor of m, then $d = p_1^{n_1}.p_2^{n_2}...p_r^{n_r}$, where $0 \leq n_i \leq k_i$, $i = 1, 2, ..., r$. Therefore, $a = b.d = b.p_1^{n_1}.p_2^{n_2}...p_r^{n_r}$, where b is an unit of R/I. Such factorization is unique because suppose that $a = c.p_1^{n_1^{'}}.p_2^{n_2^{'}}...p_r^{n_r^{'}}$ and $0 \leq n_i \leq k_i$, $i = 1, 2, ..., r$, where c is an unit of R/I.
Set $r = p_1^{n_1^{'}}.p_2^{n_2^{'}}...p_r^{n_r^{'}}$. So, we have that both, r and d are divisors of m and also, d and r are associates. Thus, we conclude that d and r are also associates, and this implies that $n_i^{'} = n_i, i = 1, 2, ..., r$, since R is an unique factorization domain. □

Proposition 1.1.3. *If $m = p_1^{k_1}.p_2^{k_2}...p_r^{k_r}$ is the irreducible factorization of m in R, then p_i is irreducible in R/I if and only if $k_i \geq 2$.*

Lemma 1.1.3. *$\mathbb{Z}_m$ is a UFR if and only if m is a power of a prime.*

Proof. Suppose m is not a power of a prime. Let p be a prime dividing m. Then p is not a nilpotent element of $\mathbb{Z}_m$, for if so, then $p^k = 0$ for some $k > 1$, and therefore, m divides p^k which is impossible. Hence $\mathbb{Z}_m$ is not a UFR.
On the other hand, Suppose that $m = p^k, k > 1$. By the factorization of the Proposition 1.1.2, we have that every nonzero element $a \in \mathbb{Z}_m$ can be written as $a = xp^e$, where x is an unit element and $e \leq k$. Since $p^r = 0$ for all $r \geq k$, we see that $0 \leq e < k$. So, again by Proposition 1.1.2, this factorization is unique. Finally, Proposition 1.1.3 tells us that p is an irreducible element of R/I since $k \geq 2$. Thus, the proof follows. □

Theorem 1.1.3. *Every Principal Ideal Domain is a Unique Factorization Domain.*

Proof. See [3](Theorem 14. p. 287) □

Note that not every unique factorization domain is PID. For instance $\mathbb{Z}[x]$ is unique factorization domain but not PID.

1.1.3 Ring Homomorphism

A ring homomorphism from R to $R^{'}$ is a mapping $\varphi : R \longrightarrow R^{'}$ such that

$$\varphi(a + b) = \varphi(a) + \varphi(b),$$

$$\varphi(ab) = \varphi(a)\varphi(b)$$

for all a and b in R. The kernel of φ is defined to be

$$ker\varphi = \{a \in R : \varphi(a) = 0\}.$$

Example 1.1.5. *Let n be a given integer, $n > 0$. Then the mapping $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ given by*

$$f(a) = [a]$$

where $[a]$, the equivalence class to which a belongs ($a \in \mathbb{Z}$), is a homomorphism since we know that

$$[a + b] = [a] + [b],$$

$$[ab] = [a][b].$$

Example 1.1.6. *The projection mapping*

$$p_j : \prod R_i \longrightarrow R_j$$

is a ring homomorphism for each j.

A ring homomorphism always takes 0 to 0. However, it might not take unity to unity. For instance, take the mapping:

$$\varphi : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_6$$

given by $\varphi(0) = 0$ and $\varphi(1) = 3$. This is a homomorphism of additive groups since the order of 3 in $\mathbb{Z}_6$ is 2. It is also multiplicative since $3^2 = 3$ in $\mathbb{Z}_6$. Thus 3 is idempotent in $\mathbb{Z}_6$ (a solution of the equation $x^2 = x$).

Lemma 1.1.4. *Let n and m be integers greater than one, and m divides n. The map $\varphi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$ is a ring homomorphism.*

Proof. Since m divides n. then, there is an integer k with $n = km$. Let $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ be the standard projection; i.e., $\pi(a) = [a]_m$.

Define $\varphi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$ by

$$\varphi([a]_n) = \pi(a).$$

We must show that φ is well-defined. If $[a]_n = [b]_n$, then there is an integer l with $a - b = ln = lkm$.

Thus,

$$\pi(a) = [a]_m = [b + lkm]_m = [b]_m = \pi(b). \quad \square$$

The following theorem is the so-called the Chinese Reminder Theorem.

Theorem 1.1.4. *If n, m are relatively prime then we have a ring isomorphism:*

$$\varphi : \mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$$

Proof. The ring homomorphism φ is given by

$$\phi(a) = (a \mod n, a \mod m)$$

This is a ring homomorphism because n and m divide nm:

$$(a +_{nm} b) = (a +_n b, a +_m b) = (a, a) + (b, b) = \varphi(a) + \varphi(b)$$

$$\varphi(ab) = (ab, ab) = (a, a)(b, b) = \varphi(a)\varphi(b)$$

Lets look at just the first step:

$$a +_{nm} b \equiv a +_n b \mod n$$

This is because both numbers are congruent to $a + b$ modulo n.
It is easy to see that φ is a bijection, and that by using the Euclidean algorithm. □

Corollary 1.1.1. *For $n > 1$ an integer, write $n = \prod_{i=1}^{k} p_i^{e_i}$, where the p_i are distinct primes. Then there is a ring isomorphism $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times ... \times \mathbb{Z}_{p_k^{e_k}}$*

Proof. Show that ring isomorphisms $F \cong G \times H$ *and* $H \cong J \times K$ imply a ring isomorphism $F \cong G \times J \times K$. Then use induction. □

Theorem 1.1.5. *Consider that $n \cong 1(mod\ m)$. The function $f : \mathbb{Z}_m \to \mathbb{Z}_{mn}$ given by $f([x]_m) = [nx]_{mn}$ is an injective homomorphism .*

Proof. Let $[a]_m, [b]_m \in \mathbb{Z}_m$. Then

$$f([a]_m + [b]_m) = f([a + b]_m) = [n(a + b)]_{mn} = [na]_{mn} + [nb]_{mn} = f([a]_m) + f([b]_m).$$

Furthermore, we note that

$$f([a]_m)f([b]_m) = [na]_{mn}[nb]_{mn} = [n^2ab]_{mn}.$$

We are given that $n \cong 1\ (mod\ m)$, hence $n = mq + 1$ for some $q \in \mathbb{Z}$. By multiplying both sidesof this equation by n we get $n^2 = mnq + n$, so $n^2 \cong n\ (mod\ mn)$. Therefore, we get

$$f([a]_m)f([b]_m) = [n^2ab]_{mn} = [nab]_{mn} = f([ab]_m) = f([a]_m[b]_m).$$

Hence f is a homomorphism. To show f is injective, we can compute the kernel of f. Let $x \in ker(f)$. Then $[0]_{mn} = f([x]_m) = [nx]_{mn}$ so $mn|nx \Rightarrow m|nx$. But $n \cong 1(mod\ m)$ tells us that $(m, n) = 1$. So we have $m|nx \Rightarrow m|x$. Therefore $[x]_m = [0]_m$ and so $ker(f) = \{[0]_m\}$. Hence f is injective. □

1.1.4 Polynomial Rings

Let R be a ring. A polynomial with coeffcients in the ring R is an expression $f(x)$ of the form

$$a_0 + a_1x + a_2x^2 + ... + a_mx^m,$$

where a_i is an element of R for $i = 0, 1, 2, ..., m$. If $a_i = 0$ then the term a_ix^i may be omitted when writing down the expression dening the polynomial. Now $R[x]$ denotes the set of all such polynomials over R.

Example 1.1.7. *The set of all quadratic polinomials $a_0x^2+a_1x+a_2$ with cofficients $a, b \in \mathbb{Z}_n$ forms a polynomial ring.*

Proposition 1.1.4. *If R is an integral domain, then $R[x]$ is also an integral domain.*

Proof. If $f, g \in R[x]$ and $fg = 0$,then $f_0 g_0 = 0$ in R. Therefore, since R is an integral domain, either $f_0 = 0$ or $g_0 = 0$ or both. Suppose that $f_0 = 0$. Then

$$(fg)_1 = f_1 g_0 + f_0 g_1 = 0$$

either $f_1 = 0$ or $g_0 = 0$. continuing in this way, we forced to get $f = 0$ or $g = 0$. That shows us that the $R[x]$ has no zero divisors. □

Proposition 1.1.5. *Let F be a field. Then $F[x]$ is a PID.*

Proof. Let $A \subseteq F[x]$ be any ideal. To show that A is principal, we may assume that $A \neq (0)$. Then A contains some nonzero elements, and we can choose $f \in A$ with $deg(f)$ as small as possible.
Since $f \in A$ and A is an ideal. we have $(f) \subseteq A$ and we claim that in fact $(f) = A$. To see this, let $g \in A$ and write $g = fq + r$ by division algorithm, where either $r = 0$ or $deg(r) < deg(f)$. Now $r = g - fq$ is an element of A, and so by our choice of f, it cannot be that $deg(r) < deg(f)$. The only alternative. Therefore, is that $r = 0$ and hence $g = fq \in (f)$, as required. Therefore $F[x]$ is a PIR.
Since the field F is surely a domain, $F[x]$ is a domain by Proposition 1.1.4, and we are done. □

It is obviously noticed from Theorem 1.1.3 and Proposition 1.1.5 that if F is a field, then $F[x]$ is a unique factorization domain.

A polynomial f over F of positive degree which can be factored as $f = gh$ where g and h are polynomials over F of positive degree is called *reducible* over F; A polynomial of positive degree which can not be thus factored is called ***irreducible*** over F.

Since $\mathbb{Z}_p$ is a field, a polynomial of the form $x^2 - ax + b \in \mathbb{Z}_p[x]$ is reducible if and only if there exist $c, d \in \mathbb{Z}_p$ so that, $x^2 - ax + b = (x - c)(x - d)$. There are $\binom{p}{2}$ such polynomials for which $c \neq d$ and p for which $c = d$. Therefore, there are exactly

$$\binom{p}{2} + p = \frac{p(p-1)}{2} + p = \frac{p(p+1)}{2}$$

reducible monic quadratic polynomials in $\mathbb{Z}_p[x]$. Since there are p^2 polynomials of the form $x^2 - ax + b$ and each one is either reducible or irreducible, we conclude there are

$$p^2 - \frac{p(p+1)}{2} = \frac{p(p-1)}{2}$$

irreducible monic degree 2 polynomials in $\mathbb{Z}_p[x]$.

The following theorem characterizes the roots of the polynomial $ax^2 + bx + c \equiv 0 \mod p$.

Theorem 1.1.6. *The quadratic polynomial $ax^2 + bx + c \mod p$ has at most two solutions, and those solutions are given by*

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

In particular, if $b^2 - 4ac$ is a quadratic nonresidue mod p then $x^2 - ax + b = 0$ has no solutions mod p.

Proof. The elementary development of the quadratic formula is dependent solely on the field properties and so can be carried out purely symbolically in $\mathbb{Z}_p$. Suppose

$$ax^2 + bx + c = 0.$$

Then,

$$x^2 + \frac{b}{a}x = \frac{-c}{a}.$$

Completing the square on the left side in the usual manner gives

$$x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} = \frac{b^2}{4a^2} - \frac{c}{a}$$

where $\frac{b^2}{4a^2}$ is defined since $4 \neq 0$ and $a^2 \neq 0$ in $\mathbb{Z}_p$ (since p is odd). Then

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{2a} \Longrightarrow x + \frac{b}{2a} = \pm\frac{\sqrt{b^2 - 4ac}}{2a}$$

where the square root has the meaning described above. Finally,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \quad \square$$

Proposition 1.1.6. *Let $n_1, ..., n_k$ be a mutually coprime set of positive numbers. Let $n = n_1...n_k$. If $f(x) \equiv 0 \mod n_i$ has N_i solutions $\mod n_i$, then $f(x) \equiv 0 \mod n$ has $N_1...N_k$ solutions $\mod n$.*

Proof. If $f(x) \equiv 0 \mod n$, then $f(x) \equiv 0 \mod n_i$ for each i, since $n_i \mid n$. In particular, each solution $x \mod n$ induces a $k-tuple$ of solutions $x \mod n_i$ to the

k congruences $f(x) \equiv 0 \mod n_i$. Conversely, given a $k-tuple$ of solutions $a_1, ..., a_k$ to $f(x) \equiv 0 \mod n_i$, we can find a unique $a \mod n$ such that $a \equiv a_i \mod n_i$, by the Chinese Reminder Theorem. (We are simultaneously solving the system $x \equiv a_i \mod n_i$.) In particular, $f(a) \equiv 0 \mod n_i$. Therefore, $a \mod n$ is a solution to $f(x) \equiv 0 \mod n$. This means that each $k - tuple$ of solutions to $f(x) \equiv 0 \mod n_i$ induces a solution to $f(x) \equiv 0 \mod n$. One easily sees that these two associations are inverse to each other, so there is a $1 - 1$ correspondence between solutions to $f(x) \equiv 0 \mod n$ and simultaneous solutions to $f(x) \equiv 0 \mod n_i$. Since each $f(x) \equiv 0 \mod n_i$ has N_i solutions, altogether there are $N_1 ... N_k$ possible different $k-tuples$ of solutions to these congruences, and therefore $N_1 ... N_k$ different solutions $\mod n$ to $f(x) \equiv 0 \mod n$. □

A polynomial $f \in k[x_1, x_2, ..., x_n]$ is ***symmetric*** if

$$f(x_{\tau(1)}, x_{\tau(2)}, ..., x_{\tau(n)}) = f(x_1, x_2, ..., x_n)$$

for every possible permutation $x_{\tau(1)}, x_{\tau(2)}, ..., x_{\tau(n)}$ of the variables $x_1, x_2, ..., x_n$.

Given variables $x_1, x_2, ..., x_n$, we define $\sigma_1, \sigma_2, ..., \sigma_n \in k[x_1, x_2, ..., x_n]$ by

$$\begin{aligned} \sigma_1 &= x_1 + x_2 + ... + x_n \\ &... \\ \sigma_r &= \sum_{\tau(1)<\tau(2)<...<\tau(r)} x_{\tau(1)} x_{\tau(2)} ... x_{\tau(r)}. \\ &... \\ \sigma_n &= x_1 x_2 ... x_n \end{aligned}$$

And σ_i is a symmetric polynomial for all $i = 1, ..., n$.

A classical theorem on symmetric polynomials attributed to Newton, states that

$$(R[x_1, x_2, ..., x_n])_{symmetric} \cong R[\sigma_1, \sigma_2, ..., \sigma_n]$$

. A short account on the proof can be found in [4].

1.2 Introduction to Directed Graphs

In a graph, edges are unordered pairs of vertices and thus have no direction. In a directed graph, edges are ordered pairs of vertices and thus have a direction (or orientation) from the first vertex to the second vertex in the ordered pair. Most of the ideas introduced for graphs can be carried over to directed graphs, modified only to take into account the directions of the edges.

1.2.1 Definitions and Basic Stracture

A ***directed graph or digraph*** D is a triple consisting of a vertex set $V(D)$, an edge set $E(D)$, and a function assigning each edge an ordered pair of vertices. The first vertex of the ordered pair is the tail of the edge, and the second is the head; together, they are the endpoints. We say that an edge is an edge from its tail to its head. The terms "***head***" and "***tail***" come from the arrows used to draw digraphs.

The ***empty graph*** on n vertices, denoted by E_n, is the graph of order n where E is the empty set.

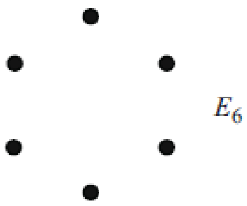

FIGURE 1.1: An Empty Graph

Let D be any digraph. A ***walk*** of length k in D is a sequence of vertices $v_0, v_1, ..., v_{k-1}$ of D such that for each $i = 1, 2, ..., k-1$, the edge e_i has tail v_{i-1} and head v_i. If the edges in a walk are distinct, then the walk is called ***a trail***. A walk is **closed** if $v_0 = v_{k-1}$. A ***path*** in D is a walk in which all the vertices are distinct.

Proposition 1.2.1. *Let D be a digraph and let u, v be a pair of distinct vertices in D. If D has an $\{u,v\}$-walk W, then D contains an $\{u,v\}$-path P such that $A(P) \subseteq A(W)$. If D has a closed $\{u,u\}$-walk W, then D contains a cycle C through u such that $A(C) \subseteq A(W)$.*

Proof. Consider a walk P from u to v of minimum length among all (u,v)-walks whose arcs belong to $A(W)$. We show that P is a path. Let $P = u_1u_2...u_k$, where $u = u_1$ and $v = u_k$. If $u_i = u_j$ for some $1 \leq i < j \leq k$, then the walk $P[u_1, u_i]P[u_{j+1}, u_k]$ is shorter than P; a contradiction. Thus, all vertices of P are distinct, so P is a path with $A(P) \subseteq A(W)$. Let $W = w_1w_2...w_k$ be a walk from $u = w_1$ to itself ($u = w_k$). Since D has no loop, $w_{k1} \neq w_k$. Let $v_1v_2...v_t$ be a shortest walk from $v_1 = w_1$ to $v_t = w_{k1}$. We have proved above that $v_1v_2...v_t$ is a path. Thus, $v_1v_2...v_tv_1$ is a cycle through $v_1 = u$. □

An arc $v_{i1}v_i \in E(D)$ is called a forward edge of the walk, and an edge v_iv_{i1} is called a backward edge of the walk. The net length of a walk is the difference between the number of forward edges and the number of backward edges, in the walk. Note that the net length may be negative.

Note that a ***cycle*** is a closed walk, where $v_0 = v_{k-1}$ and the vertices $v_0, v_1, ..., v_{k-1}$ are distinct from each other. The ***distance*** between two vertices of a graph is the number of edges of the shortest path between them.

Let us illustrate these definitions with an example. In the graph of Figure 1.2, a, c, f, c, b, d is a walk of length 5. The sequence b, a, c, b, d represents a trail of length 4, and the sequence d, g, b, a, c, f, e represents a path of length 6. Also, while e, d, b, a, c, f, e is a cycle. In general, it is possible for a walk, trail, or path to have length 0.

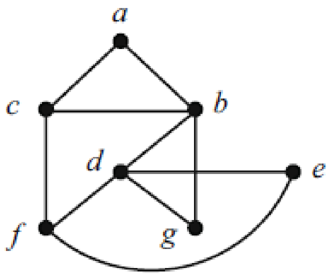

FIGURE 1.2: Basic Definitions

In a digraph D, a vertex has two degrees. The outdegree ***outdeg(v)*** of a vertex v is the number of edges of which v is the tail of a vertex; the indegree ***indeg(v)*** of v is the number of edges of which v is the head of a vertex. The degree $deg(v)$ of a vertex v of D is defined by $deg(v) = outdeg(v) + indeg(v)$. The maximum degree is $\Delta(G)$, the minimum degree is $\delta(G)$. Clearly, the sum of the indegrees of the vertices of a digraph equals the sum of the outdegrees. It is often referred to as the First Theorem of Graph Theory.

Proposition 1.2.2. *In a graph G, the sum of the degrees of the vertices is equal to twice the number of edges. Consequently, the number of vertices with odd degree is even.*

Proof. Let $S = \sum_{v \in V} deg(v)$. Notice that in counting S, we count each edge exactly twice. Thus, $S = 2|E|$ (the sum of the degrees is twice the number of edges). Since S is even, it must be that the number of vertices with odd degree is even. □

The terminology used in discussing digraphs is quite similar to that used for graphs. The cardinality of the vertex set of a digraph D is called the order of D and is denoted by $n(D)$, or simply n. The size $m(D)$ (or m) of D is the cardinality of its arc set.

Theorem 1.2.1. *[5] If G is a digraph of order n and size m with $V(G) = \{v_1, v_2, ..., v_n\}$, then*

$$\sum_{i=1}^{n} outdeg(v_i) = \sum_{i=1}^{n} indeg(v_i)$$

Proof. When the outdegrees of the vertices are summed, each arc is counted once, since every arc is incident $from$ exactly one vertex. Similarly, when the indegrees are summed, an arc is counted just once since every arc is incident *to* a single vertex. □

A graph is ***regular*** provided each vertex has the same degree. If k is the common degree, then the graph is regular of degree k. A connected regular graph of degree 2 is a ***circuit***.

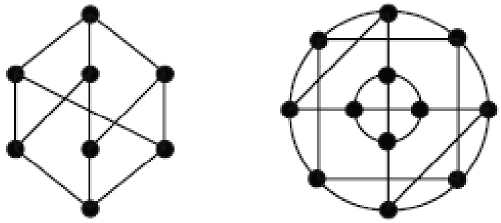

Figure 1.3: Examples of Regular Graphs

A ***subgraph*** of a graph G is a graph such that $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$ and the assignment of endpoints to edges in is the same as in G. We then write $H \subseteq G$ and say that "G contains H".

Given a graph G, ***the complement of*** G, denoted by $\bar{G}$, is the graph whose vertex set is the same as that of G, and whose edge set consists of all the edges that are not present in G.

The ***components*** of a graph G are its maximal connected subgraphs. A component is ***trivial*** if it has no edges; otherwise it is nontrivial. An isolated vertex is a vertex of degree 0. Therefore, Deleting a vertex or an edge can increase the number of components. Although deleting an edge can only increase the number of components by 1, deleting a vertex can increase it by many. When we obtain a subgraph by deleting a vertex, it must be a graph, so deleting the vertex also deletes all edges incident to it.

The union of graphs $G_1, ..., G_k$, written $G_1 \cup G_2 \cup ... \cup G_k$, is the graph with vertex set $\bigcup_{k}^{i=1} V(G_i)$ and edge set $\bigcup_{k}^{i=1} E(G_i)$. The intersection of graphs $G_1, ..., G_k$, written $G_1 \cap G_2 \cap ... \cap G_k$, is the graph with vertex set $\bigcap_{k}^{i=1} V(G_i)$ and edge set $\bigcap_{k}^{i=1} E(G_i)$.

Let $G = (V, E)$ be a graph with vertex set V and edge set E; similarly let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$. The conjunction $G = G_1 \wedge G_2$ is defined by $V = V_1 \times V_2$ and $\{u, v\} = \{(u_1, u_2), (v_1, v_2)\} \in E$ if and only if $\{u_1, v_1\} \in E_1$ and $\{u_2, v_2\} \in E_2$.

Two vertices u and v of a digraph D are ***adjacent*** if there is an arc of the form uv or vu. We call a vertex u ***incident*** to an edge e if $u \in E$.

The ***underlying graph*** of a digraph H is the graph G obtained by treating the edges of H as unordered pairs; the vertex set and edge set remain the same, and the endpoints of an edge are the same in G as in H, but in G they become an unordered pair.

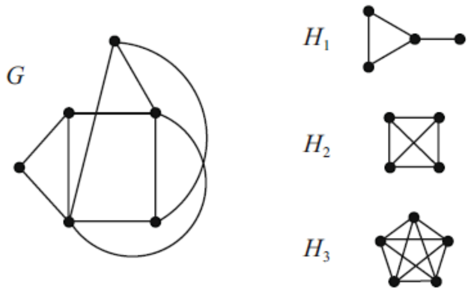

Figure 1.4: H_1 and H_2 are Subgraphs of G.

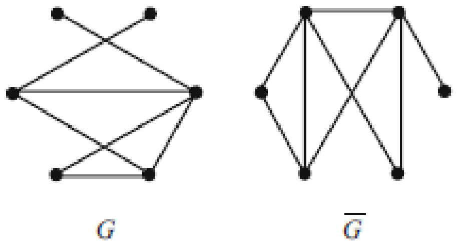

Figure 1.5: A Graph and Its Complement

A ***clique*** in a graph is a set of pairwise adjacent vertices. An ***independent set*** is a set of pairwise non-adjacent vertices. A graph G is ***multipartite*** if its vertex set is a union of disjoint independent sets, which are known as partite classes. Observe that a set of vertices is independent in G if it contains no pair of adjacent vertices. In terms of the associated partition, we have the following condition. A given digraph D satisfies $G \to \overrightarrow{C_k}$ if and only if the vertices of G can be partitioned into k independent sets $S_0, S_1, ..., S_{k-1}$ so that each edge of D goes from S_i to S_{i+1} for some $i = 0, 1, ..., k-1$ (with addition modulo k).

A graph G is ***bipartite*** if $V(G)$ is the union of two disjoint (possibly empty) independent sets called partite sets of G.

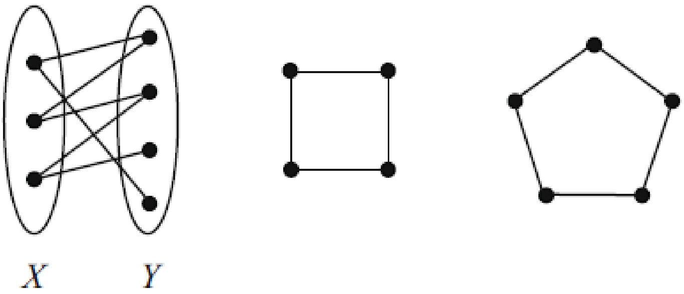

Figure 1.6: Two Bipartite Graphs and One Non-bipartite Graph.

A ***complete graph*** is a simple graph whose vertices are pairwise adjacent; the (unlabeled) complete graph with n vertices is denoted K_n.

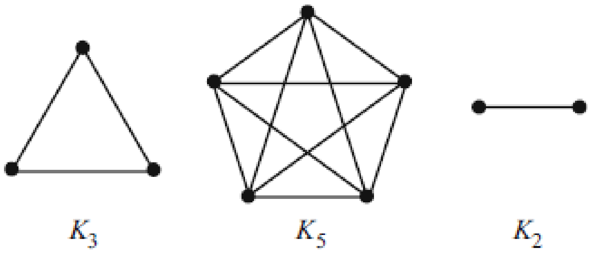

Figure 1.7: Examples of Complete Graphs

Let m and n be positive integers. The ***complete bipartite graph*** $K_{m,n}$ is the bipartite graph with vertex set $V = U \cup W$, where U contains m vertices and W

contains n vertices and each pair $\{u, w\}$ where $u \in U$ and $w \in W$ is an edge of $K_{m,n}$. Thus $K_{m,n}$ has exactly mn edges.

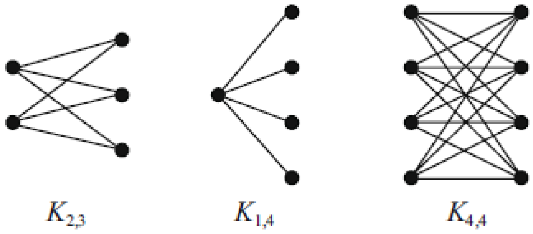

Figure 1.8: A Few Complete Bipartite Graphs.

A ***vertex-coloring*** of a graph is an assignment of a color to each vertex so that vertices that are joined by an edge are colored differently. One way to color a graph is to assign a different color to each vertex.
Note that a bipartite graph is complete bipartite if every vertex is adjacent to every vertex outside its partite class.

1.2.2 Graph Homomorphisms

Let G be a graph with vertex set V, and let H be a graph with vertex set W. A ***homomorphism*** from G to H is a mapping $\varphi : V \to W$ such that uv is an edge of G implies $\{\varphi(u), \varphi(v)\}$ is an edge of H. We write $G \to H$ to indicate that a homomorphism from G to H exists. A homomorphism of G to H is also called an $H-$colouring of G, or that G is $H - colourable$.[6]

We can apply the above definition of homomorphism to the corresponding symmetric digraphs of G and H. The homomorphisms of graphs preserve adjacency, while homomorphisms of digraphs also preserve the directions of the arcs. Therefore, a homomorphism of digraphs $G \longrightarrow H$ is also a homomorphism of the underlying graphs, but not conversely.

Note that for graphs $\varphi(u)\varphi(v) \in E(H)$ implies that $\varphi(u) \neq \varphi(v)$, since each edge of H consists of two distinct elements.

A homomorphism $\varphi : G \longrightarrow H$ is called injective, if $u \neq v \in V(G)$ implies $\varphi(u) \neq \varphi(v) \in V(H)$, i.e., if φ is one to one. An injective homomorphism is also called an monomorphism.

A homornorphism $\varphi : G \longrightarrow H$ is called surjective, if $v \in V(H)$ implies that there is a vertex $u \in V(G)$ such that $\varphi(u) = v$, i.e., if φ is onto vertices. A surjective homomorphism is also called an epimorphism.

A homomorphism which is both injective and surjective, is called a isomorphism.

The following theorem is the so-called Dual path theorem. It represents the homomorphism to oriented paths.

Theorem 1.2.2. *Suppose D is a Digraph and P an oriented path. Then $G \nrightarrow P$ if and only if there is an oriented path W such that $W \to G$ and $W \nrightarrow P$.*

If $G \to P$ and W is an oriented path such that $W \to G$, then of course $W \to P$ by composition. Thus the sufficiency of the condition is obvious. The necessity is shown in [7].

Since the homomorphic image of a directed path may be a walk, so one can observe the following:

Proposition 1.2.3. *A mapping $f : V(P_k) \to V(G)$ is a homomorphism of P_k to G if and only if the sequence $f(0), f(1), ..., f(k)$ is a walk in G.*

In particular, homomorphisms of G to H map paths in G to walks in H, and hence do not increase distances. If we denote by $d(u, v)$ the distance (length of a shortest path) from u to v in D, then we have the following fact.

Proposition 1.2.4. *[8] If $f : G \to H$ is a homomorphism, then $d(f(u), f(v)) \leq d(u, v)$, for any two vertices u, v of G.*

Proof. If $u = v_0, v_1, ..., v_k = v$ is a path in G, then $f(u) = f(v_0), f(v_1), ..., f(v_k) = f(v)$ is a walk of the same length k in H. Since every walk from $f(u)$ to $f(v)$ contains a path from $f(u)$ to $f(v)$, we must have $d(f(u), f(v)) \leq k$. □

In the spirit of the theorem 1.2.2, we may expect that for an oriented cycle $\overrightarrow{C}$ we have, $G \to \overrightarrow{C}$ if and only if there is an oriented cycle homomorphic to G that is not homomorphic to $\overrightarrow{C}$. An equivalent restatement of this would say that $G \to \overrightarrow{C}$ if and only if each oriented cycle homomorphic to G is also homomorphic to $\overrightarrow{C}$ [9]. Note that this condition on cycles is stronger than the dorresponding condition on paths.

Proposition 1.2.5. *A mapping $f : V(\overrightarrow{C}_k) \to V(G)$ is a homomorphism of $\overrightarrow{C}_k$ to G if and only if $f(1), f(2), ..., f(k)$ is a closed walk in G.*

Corollary 1.2.1. *$\overrightarrow{C}_{2k+1} \longrightarrow \overrightarrow{C}_{2l+1}$ if and only if $l \leq k$.*

Proof. An odd cycle has no closed odd walk shorter than its length, and has a closed walk of any odd length greater than or equal to its length. □

Figure 1.9 illustrates a homomorphism $f : C_9 \longrightarrow C_5$; the images $f(v), v \in V(C_9)$ are shown in C_5.

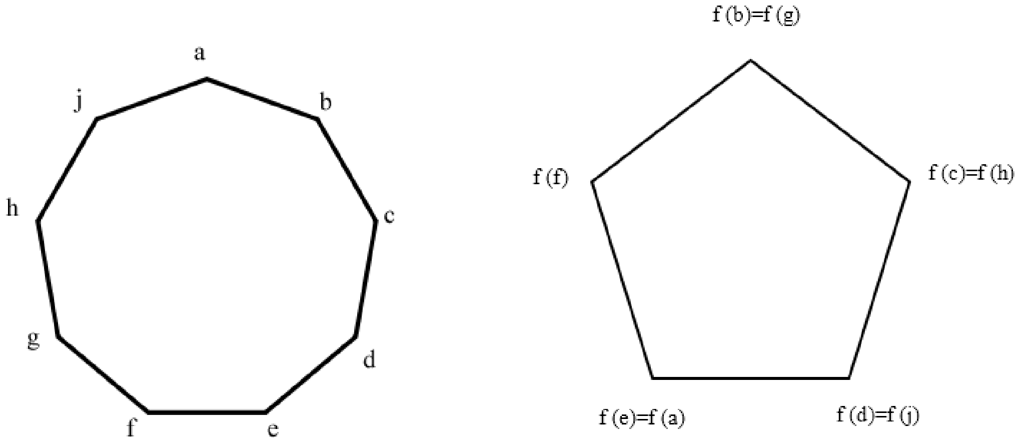

Figure 1.9: Homomorphism of Odd Cycles

Since a cycle is a homomorphic image of a cycle, we can reformulate the last result as follows.

Corollary 1.2.2. *Let $\overrightarrow{C}_k$ be a digraph cycle of length k. A digraph D satisfies $D \to \overrightarrow{C_k}$ if and only if the length of every directed cycle in D is divisible by k.*

Chapter 2

Unitary Cayley Graph

Recalling, there has been a lot of different connections between rings and graphs, such as zero-diisor graps, ...etc. Here we will present one such connection. Some results on the Unitary Cayley graph of a finite ring are presented (e.g [1], [10]). The present study determins precisely the diameter, girth, vertex (edge) connectivity, vertex and edge chromatic number.

2.1 Introduction

Cayley graphs stem from a type of diagram now called a Cayley colour diagram, which was introduced by A. Cayley in 1878 as a graphic representation of abstract groups. Its definition is suggested by Cayley's theorem (named after Arthur Cayley) and uses a specified, usually finite, set of generators for the group. Cayley colour diagrams were generalized to Schreier coset diagrams by O. Schreier in 1927. Cayley graphs provide graphic representations for abstract groups. They are a bridge between groups and surfaces, and they give rise to examples for various extremal graph problems, and good models for interconnection networks.

Definition 2.1.1. *For a positive integer $n > 1$ the unitary Cayley graph $G_n = Cay(\mathbb{Z}_n, U_n)$ is defined by the additive group of the ring $\mathbb{Z}_n$ of integers modulo n and the multiplicative group U_n of its units. If we represent the elements of $\mathbb{Z}_n$ by the integers $0, 1, ..., n$, then,*

$$U_n = \{a \in \mathbb{Z}_n : gcd(a, n) = 1\}$$

So G_n has vertex set $V(G_n) = \mathbb{Z}_n = \{0, 1, ..., n\}$ and edge set

$$E(G_n) = \{\{a, b\} : a, b \in \mathbb{Z}_n, gcd(a - b, n) = 1\}$$

The graph G_n is regular of degree $|U_n| = \phi(n)$, where $\phi(n)$ denotes the Euler function. If $n = p$ is a prime number, then $G_n = K_p$ is the complete graph on p vertices.

Example 2.1.1. *Suppose the finite groups $G_n = \mathbb{Z}_9$, $G_m = \mathbb{Z}_3 \times \mathbb{Z}_3$. Unitary Cayley graph of these rings are regular graphs of oreder 6 and 4 respectivily.*

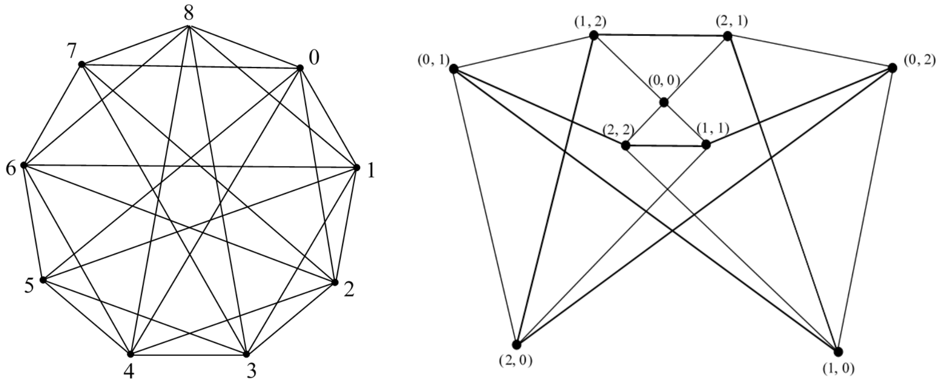

FIGURE 2.1: Cayley Graph of $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$

A generalization of unitary Cayley graphs presents itself readily: given a finite ring R (commutative with unity), one may define $G_R = Cay(R, R^*)$ to be the ring whose vertex set is R, with an edge between x and y if $x - y \in R^*$.

Since R is a finite ring, it is Artinian, and hence $R \cong R_1 \times ... \times R_t$, where each R_i is a finite local ring with maximal ideal m_i. Since $(u_1, ..., u_t)$ is a unit of R if and only if each u_i is a unit in R_i^*, we see immediately that G_R is the conjunction of the graphs $G_{R_1}, G_{R_2}, \ . \ . \ . \ , G_{R_t}$. Moreover, if $x, y \in R_i$, $\{x, y\}$ is an edge of G_{R_i} if and only if $x - y \notin m_i$.

We denote by k_i the (finite) residue field R_i/m_i, $\pi_i : R_i \to k_i$ the quotient map, and $f_i = |k_i|$. We also assume (after appropriate permutation of factors) that $f_1 \leq f_2 \leq ... \leq f_t$.

The following lemma is well known and it is inserted here for the seek of completeness.

Lemma 2.1.1. *If S be a finite local ring with maximal ideal m. Then there exists a prime p such that $|R|$, $|m|$ and $|R/m|$ are all powers of p.*

Two vertices $x = (x_1, ..., x_t)$, $y = (y_1, ..., y_t)$ are adjacent if and only if $x_i - y_i \in R_i^*$ for all $i = 1, ..., t$. Equivalently, x is adjacent to y if and only if for each $i = 1, ..., t$,

$x_i - y_i \notin m_i$, that is, $\pi_i(x_i) \neq \pi_i(y_i)$.

2.2 Vertex Degree

For a finite graph G, with vertices $\{v_1, ..., v_r\}$, a representation of G modulo n is a set $\{a_1, ..., a_r\}$ of distinct, nonnegative integers, $0 \leq a_i < n$ satisfying $gcd(a_i - a_j, n) = 1$ if and only if v_i is adjacent to v_j. The representation number, $Rep(G)$, is the smallest n such that G has a representation modulo n. It was shown by Erdös and Evans (e.g [11]) that any finite graph can be represented modulo some positive integer, and so the representation number of a finite graph is well defined.

Assume that $n = p_{i_1}^{k_1}...p_{i_m}^{k_m}$, where $p_{i_1}, ..., p_{i_m}$ are distinct primes. If in the representation of G_n a vertex v corresponds to an integer a, then we will assign coordinates to v as follows. The coordinates of v with respect to the ordered set of primes $p_{i_1}, ..., p_{i_m}$ are $(v_1, ..., v_m)$, where $v_j \equiv a \bmod p_{i_j}$ for $j = 1, ..., m$, and $v_j \in \{1, ..., p_{i_j} - 1\}$ for $j = 1, ..., m$. If u has coordinates $(u_1, ..., u_m)$ and v has coordinates $(v_1, ..., v_m)$ then u is adjacent to v if and only if $u_j \neq v_j$ for $j = 1, ..., m$. In this coordinate representation two vertices of G_n share the same coordinates if and only if they share the same neighbourhood. Thus we know the structure of G_n (e.g[12]).

Proposition 2.2.1. *Let $n = p_1^{e_1}...p_t^{e_t}$ for distinct primes $p_1, ..., p_t$, where $p_1 < p_2... < p_t$. The degree of a vertex $v \in V(G_n)$ is given by deg$(v) = \phi(n)$.*

Proof. For any $v \in V(G_n)$, using the notation as it is showen above, we assign each vertex v to a set $X(v_1, ..., v_t)$, where $0 \leq v_i \leq p_i - 1$ and $v_i \equiv v \pmod{p_i}$. A vertex v in G_n is adjacent to a vertex $w \in X(w_1, ..., w_t)$ if only if $v_i \neq w_i$ for all i with $1 \leq i \leq t$. For if $v_i = w_i$ for some i, then $v \equiv w \pmod{p_i}$, which implies that $v - w \equiv 0 \pmod{p_i}$. Hence, p_i divides $v - w$, and $v - w$ is not a unit of n. This implies v and w are non-adjacent.
Conversely, if $v_i \neq w_i$ for all i, then $v - w \not\equiv 0 \pmod{p_i}$ for all i. Hence, none of the prime divisors of n divide $v - w$. This implies that $v - w$ is a unit of $\mathbb{Z}_n$, and hence v and w are adjacent.
By construction, each set $X(v_1, ..., v_t)$ has cardinality $\prod_{i=1}^{t} p_i^{e_i - 1}$. Finding the degree of v thus reduces to finding the number of sets whose vertices are adjacent to v, then multiplying by the number of elements per set.
In the collection of sets $X(v_1, ..., v_t)$, each v_i ranges from 0 to p_i, and thus takes

on one of p_i possible values. Suppose the vertices of $X(w_1, ..., w_t)$ are adjacent to those of $X(v_1, ..., v_t)$, the set containing v. Then each w_i must satisfy the conditions $w_i \neq v_i$, $0 \leq w_i \leq p_i - 1$. Each w_i thus takes on one of $p_i - 1$ possible values. The total number of sets $X(w_1, ..., w_t)$ whose vertices are adjacent to those of any $X(v_1, ..., v_t)$ is given by $\prod_{i=1}^{s}(p_i - 1)$. Hence, the degree of v is given by

$$\begin{aligned} deg(v) &= \left(\prod_{i=1}^{t} p_i^{e_i-1}\right)\left(\prod_{i=1}^{t}(p_i-1)\right) \\ &= \prod_{i=1}^{t} p_i^{e_i-1}(p_i-1) \\ &= \prod_{i=1}^{t}\phi(p_i^{e_i}) \\ &= \phi(n) \quad \square \end{aligned}$$

Corollary 2.2.1. *G_n is $\phi(n)$-regular for all n.*

Proof. This follows immediately from Proposition 2.2.1, which gives $\phi(n)$ as the degree of an arbitrary vertex of G_n. □

Proposition 2.2.2. *Let R be any ring. Then*

1. *G_R is a regular graph of degree $|R^*|$.*
2. *Let S be a local ring with maximal ideal m. Then G_S is a complete multipartite graph whose partite sets are the cosets of m in S. In particular, G_S is a complete graph if and only if S is a field.*
3. *If R is any Artinian ring and $R \cong R_1 \times ... \times R_t$ as a product of local rings, then $G_R = \wedge_{i=1}^{t} G_{R_i}$. Hence, G_R is a conjunction of complete multipartite graphs.*

Proof. : The proof of (1) follows from the fact that the neighborhood of any vertex a is $\{a + u : u \in R^*\}$. To prove (2), simply note that $x, y \in S$ are adjacent if and only if $x - y \notin m$ and that S is a field if and only if $m = 0$. The third statement follows from the fact that $R^* = R_1^* \times ... \times R_t^*$. □

Example 2.2.1. *From the figure 2.1, we observe that any vertex $v \in V(\mathbb{Z}_9)$ has degree $\phi(9) = 6$; that is exactly the number of edges which are adjacent to v. Also, the degree of any vertex in $G(\mathbb{Z}_3 \times \mathbb{Z}_3)$ is $|U_3 \times U_3| = 2.2 = 4$.*

Remarks.

1. Since Cayley graphs are k-regular graphs, then we have that

$$k|V| = \sum_{v \in V(G)} deg(v) = 2 \mid E \mid .$$

2. Not every regular graph is a Cayley graph. For instance, the following graph is 3-regular but not unitary Cayley graph.

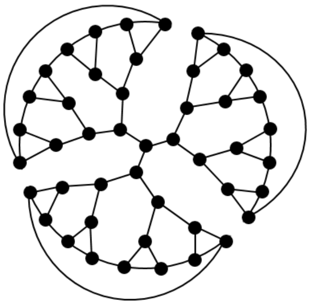

Figure 2.2: 3-Regular Graph with 46 Vertices

$N(v)$ will be used for the neighborhood of a vertex v (that is, the set of vertices adjacent to v) and $N(u,v)$ for the number of common neighbors of the vertices u and v.

Proposition 2.2.3. *Suppose $a = (a_1, ..., a_t)$ and $b = (b_1, ..., b_t)$ are vertices of G_R. Let $I = \{i : 1 \leq i \leq t, \pi_i(a_i) = \pi_i(b_i)\}$ and $J = \{1, ..., t\} - I$. Then*

$$N(a,b) = |R| \prod_{i \in I} (1 - \frac{1}{f_i}) \prod_{j \in J} (1 - \frac{2}{f_j}).$$

Proof. See [1]. □

2.3 Vertex Coloring

The ***Clique Number***, denoted $\omega(G_n)$ is the size of largest complete subgraph that can be found in a graph. The ***chromatic number*** of a graph, denoted by $\chi(G_n)$ is the smallest number of colors needed to color the vertices of so that no two adjacent vertices share the same color.

Next, the chromatic number and the clique number of G_n are going to determined. From now on we always assume that n is an integer, $n \geq 2$.

Theorem 2.3.1. *[10] Let $n = p_1^{e_1} p_2^{e_2} ... p_t^{e_t}$, where $p_1 < p_2 < ... < p_t$ and $e_i \geq 1$ for all $i = 1, ..., t$. Then $\omega(G_n) = \chi(G_n) = p_1$.*

Proof. Let m represent the vertices and k_m is the coloring. For each m, $0 \leq m \leq n-1$, there is a unique k_m, such that $m \equiv k_m(\mod p_1)$. The vertex m is assigned the color k_m. If two vertices m and $m^{'}$ receive the same color then $k_m \equiv k^{'}_m(\mod p_1)$, so $m \equiv m^{'}(\mod p_1)$. This allows m to not be adjacent to

$m^{'}$. Thus, this coloring is proven and therefore, $\chi(G_n) \leq p_1$. It is known in graph theory that $\omega(G_n) \geq \chi(G_n)$. Hence the proof follows. □

We observe that in G_n there exist a $p_1 - clique$. The clique in G_n is $\{0, 1, ..., p_1 - 1\}$ which implies $p_1 \leq \omega(G_n)$.

Example 2.3.1. *Figure 2.3 shows that* $\omega(G_{12}) = \chi(G_{12}) = p_1 = 2$. *For the chromatic number, the vertices that are colored yellow are* $0 \mod 2$ *and the vertices that are colored pink are* $1 \mod 2$. *The clique number is represented by the vertices* $\{0, 1\}$.

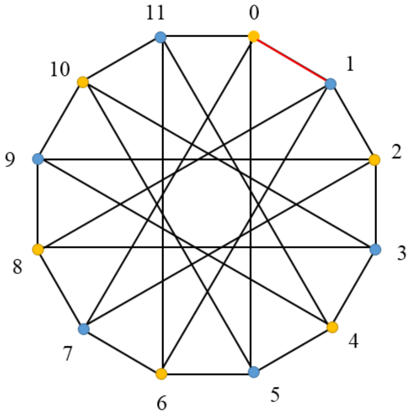

FIGURE 2.3: Cayley graph of $\mathbb{Z}_{12}$

Proposition 2.3.1. *Let* R *be a finite ring. Then* $\omega(G_R) = \chi(G_R) = f_1$.

Proof. See [1]. □

2.4 Diameter and Girth

The distance $d(x, y)$ of vertices x and y of a graph G is the length (number of edges) of a shortest $x, y - path$. The diameter is the maximal distance any two vertices of G may have. The girth of a graph is the length of a shortest cycle contained in the graph.

The following theorem, represents the diameter of the ring of integers for $n \geq 2$. See [10].

Proposition 2.4.1. *The diameter of* G_n *is 1 if* n *is prime, 2 if* n *is an odd composite number, and 3 if* n *is an even composite number.*

Proof. Case 1: Suppose n is prime. Claim: $G_n = K_n$, and the diameter of G_n is 1. [12]

Let n be prime, and let v and w be vertices of G_n. Then $v - w \in \mathbb{Z}_n$, and $v - w < n$.

Because n is prime, this implies that $v-w$ is relatively prime to n. Hence $v-w$ is a unit of the ring $\mathbb{Z}_n$, and v and w are adjacent. Since v and w are arbitrary, each vertex of G_n is adjacent to every other vertex, and $G_n = K_n$.

Case 2: Next, suppose n is an odd composite number, where $n = p_1^{e_1}p_2^{e_2}...p_t^{e_t}$. As in Proposition 2.2.1, we assign each vertex v of G_n to a class $X(h_1,...,h_t)$, where each h_i ranges from 0 to $p_i - 1$. Let $v, w \in V(G)$ be given, where $v \in X(v_1,...,v_t)$ and $w \in X(w_1,...,w_t)$. If $v_i \neq w_i$ for all $1 \leq i \leq t$, then v and w are adjacent.

Suppose $v_i = w_i$ for at least one value of i. Then v and w are non-adjacent, which implies that the diameter of G_n is at least 2. If n is odd, $p_i \geq 3$ for all i. Hence, each h_i has at least three possible values. Thus, we can construct a class $X(u_1,...,u_n)$ such that $u_i \neq v_i$ and $u_i \neq w_i$ for all $0 \leq i \leq n$. Let $u \in X(u_1,...,u_n)$ be given. Then u is adjacent to both v and w, so v, u, w is a path of length two between v and w. Since v and w are arbitrary nonadjacent vertices of G_n, the diameter of G_n is 2.

Case 3: Suppose n is even, and $n \geq 2$. We again let $v, w \in V(G)$ be given, where $v \in X(v_1,...,v_t)$ and $w \in X(w_1,...,w_t)$. If $v_i \neq w_i$ for all $1 \leq i \leq t$, then v and w are adjacent. If $v_i = w_i$ for some i, the situation is more complicated. We have $n = p_1^{e_1}p_2^{e_2}...p_t^{e_t}$, with $p_1 = 2$. Thus, for each $X(h_1,...,h_t)$, h_1 has only two possible values. If $v_1 = w_1$ for v and w, we can again construct a class $X(u_1,...,u_n)$ such that $u_i \neq v_i$ and $u_i \neq w_i$ for all $0 \leq i \leq n$. Thus, any vertex in l is adjacent to both v and w, and the minimum length for a path between v and w is 2.

If, $v_1 \neq w_1$, but $v_i = w_i$ for some $i \geq 2$, the above argument fails. Clearly, v and w are non-adjacent. However, we cannot construct a class whose vertices are adjacent to both v and w. The first coordinate of any class will be equal either to v_1 or w_1. Thus, there is no path of length two between v and w. Since there exist pairs of vertices in G_n which are not connected by any path of length 1 or 2, the diameter of G_n is at least 3.

We now show that the diameter of G_n is exactly 3. We construct a class of vertices $X(u_1,...,u_t)$, as follows. If $v_i \neq w_i$, let $u_i = w_i$. If $v_i = w_i$, let u_i be any integer such that $u_i \neq w_i$, $0 < u_i < p_i - 1$. Let $u \in X(u_1,...,u_t)$ be given. Then u is adjacent to v. Also, u and w agree in their first coordinate, so there exists a vertex y adjacent to both u and w. Hence v, u, y, w is a path of length three between v and w. So the minimun length for such a path is three, so the diameter of G_n is at most 3. Combining this result with the lower bound for diameter given above, this implies that the diameter of G_n is exactly 3. $\square$

In the following we use $diam(G)$ and $gr(G)$ (respectively) to denote the diameter and girth of a graph G.

Theorem 2.4.1. *Let $R \cong R_1 \times ... \times R_t$ be an Artinian ring. Then*

$$diamG_R = \begin{cases} 1 & if \quad t = 1 \; and \; R \; is \; a field \\ 2 & if \quad t = 1 \; and \; R \; isn't \; a field \\ 2 & if \quad t \geq 2, f_1 \geq 3 \\ 3 & if \quad t \geq 2, f_1 = 2, f_2 \geq 3 \\ \infty & if \quad t \geq 2, f_1 = f_2 = 2 \end{cases}$$

Proof. See [1]. □

Theorem 2.4.2. *Let $R \cong R_1 \times ... \times R_t$ be an Artinian ring. Then*

$$grG_R = \begin{cases} 3 & if \qquad f_1 \geq 3 \\ 6 & if \qquad R \cong \mathbb{Z}_2^r \times \mathbb{Z}_3 \; for \; some \; r \geq 1 \\ \infty & if \qquad R \cong \mathbb{Z}_2^r \; for \; some \; r \geq 1 \\ 4 & otherwise \end{cases}$$

Proof. See [1]. □

Corollary 2.4.1. *The number of triangles in G_R is $\frac{|R|^3}{6} \prod_{i=1}^{t} (1 - \frac{1}{f_i})(1 - \frac{2}{f_i})$.*

Proof. If $f_1 = 2$, then by Proposition 2.2.3. G_R is triangle-free, so the claim holds in this case. If $f_1 \geq 3$, then given a vertex $a \in R$, by Proposition 2.2.2 there are $|R^*| = |R| \prod_{i=1}^{t} (1 - \frac{1}{f_i})$ choices for an adjacent vertex b. Now, Proposition 2.2.3. implies that there are $|R| \prod_{i=1}^{t} (1 - \frac{1}{f_i})$ choices for a third vertex which is a common neighbor of both a and b. Since any such triangle may be formed in 6 distinct ways, the total number of triangles is

$$\frac{|R|^3}{6} \prod_{i=1}^{t} (1 - \frac{1}{f_i})(1 - \frac{2}{f_i}). \quad \square$$

Example 2.4.1. *Consider the ring $R = \mathbb{Z}_4 \times \mathbb{Z}_9$. Then $f_1 = |\mathbb{Z}_4/\{0, 2\}| = 2$ and $f_2 = |\mathbb{Z}_9/\{0, 3, 6\}| = 3$. In the figure 2.4 we observe that $diamG_R = 3$; that is exactly the minimum number of edges between any two vertices. Furthermore, $grG_R = 4$ such that the shortest length of any cycle is 4. In this ring we note that $Cay(R, R^*)$ is tiangle-free; that is*

$$\frac{36^3}{6}(1 - \frac{1}{2})(1 - \frac{2}{2})(1 - \frac{1}{3})(1 - \frac{2}{3}) = 0$$

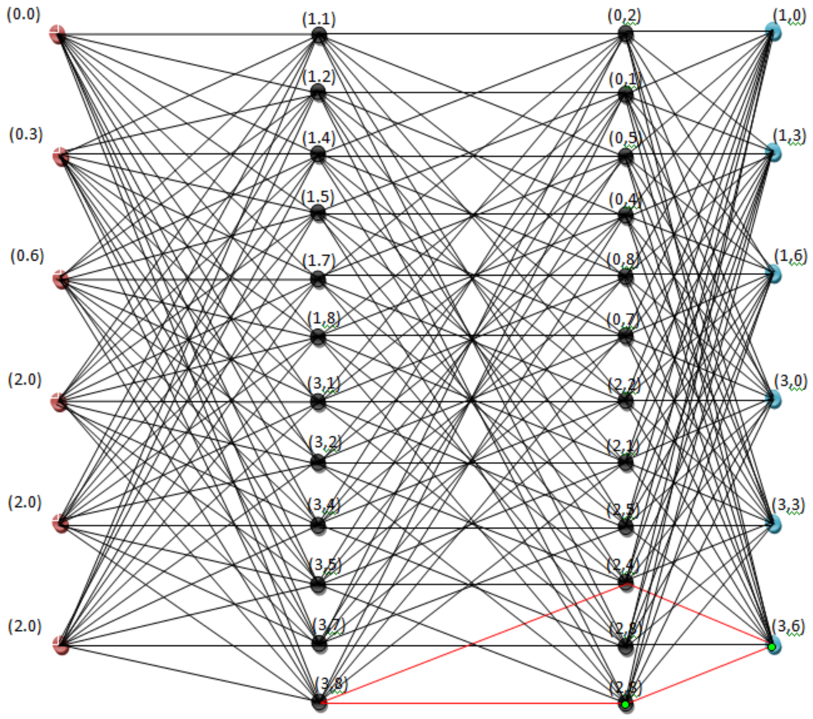

Figure 2.4: Cayley Graph of $\mathbb{Z}_4 \times \mathbb{Z}_9$

2.5 Connectivity

A separating set or ***vertex cut*** of a graph G is a set $S \subseteq V(G)$ such that $G - S$ has more than one component. The vertex connectivity, or simply connectivity $\kappa(G)$, of a graph is defined to be the minimum number of vertices whose removal disconnects the graph, or reduces it to single vertex; for example $\kappa(K_p) = p - 1$, $\kappa(K_{n,n}) = n$.

A graph with more than two vertices has connectivity 1 if and only if it is connected and has a cutvertex. A graph with more than one vertex has connectivity 0 if and only if it is disconnected.

An edge cut of a multigraph G is an edge-set of the form $[S; \bar{S}]$, with $\phi \neq S \neq V(G)$ and $\bar{S} = V(G) - S$.

$$For\ S, T \subseteq V(G),\ [S, T] = \{xy \in E(G) : x \in S, y \in T\}.$$

The edge-connectivity of G is

$$\kappa^{'}(G) = min\{|[S, \bar{S}]| : [S, \bar{S}]\ is\ an\ edge\ cut\}.$$

A graph G is $k-$edge-connected if there is no edge cut of size $k-1$.
Let G be a connected graph. A disconnecting set of edges in G is a subset $D \subseteq E(G)$, such that removing the edges in D from G yields a disconnected graph.

Let u and v be distinct vertices of a graph G. An u, v-disconnecting set of edges in G is a subset H of $E(G)$ such that removing the edges of H from G yield a graph with no paths from u to v.

We will use Menger's theorem for edge connectivity to find edge connectivity of G_n.

Theorem 2.5.1. ***Menger's Theorem*** *Suppose x and y are distinct vertices of a graph G. Then the minimim size of an x, y-disconnecting set of edges equals the maximum number of pairwise edge-disjoint x, y-paths in G.*

Theorem 2.5.2. *The unitary Cayley graph X_n has vertex connectivity $\kappa(n) = \phi(n)$.*

Proof. The proof is presented in [13](Theorem 4. page 3). It is left to the reader, because some unrequired concepts are involved in the proof. □

Proposition 2.5.1. *The edge connectivity $\kappa^{'}(G_n)$ of G_n is equal to $\phi(n)$.*

Proof. For $n < 3$, the proposition is trivial. Let $n \geq 3$ be given. First, we show $\kappa^{'}(G_n) \geq \phi(n)$.
Let v and w be vertices of G_n. Since G_n can be decomposed into $\frac{\phi(n)}{2}$ disjoint Hamiltonian cycles [1]. Hence, there are at least $\phi(n)$ paths from v to w whose edge sets are disjoint. By Menger's theorem, to disconnect v and w, we must remove at least $\phi(n)$ edges. Since v and w are arbitrary vertices of G_n, $\kappa^{'}(G_n) \geq \phi(n)$.
To see that $\kappa^{'}(G_n) = \phi(n)$, note that we can isolate a vertex v of G_n, simply by removing all edges incident at v. Since the degree of any vertex of G_n is $\phi(n)$, we can isolate a vertex by removing $\phi(n)$ edges. Hence, $\kappa(G_n) \leq \phi(n)$. Since we have already shown the other inequality, $\kappa(G_n) = \phi(n)$, and the proof is complete. □

Theorem 2.5.3. *(**Whitney [1932a]**)[14] If G is a simple graph, then*

$$\kappa(G) \leq \kappa^{'}(G) \leq \delta(G).$$

Proof. The edges incident to a vertex v of minimum degree form an edge cut; hence $\kappa^{'}(G) \leq \phi(G)$. It remains to show that $\kappa(G) < \kappa^{'}(G)$.
We have observed that $\kappa(G) \leq n(G) - 1$. Consider a smallest edge cut $[S, \overline{S}]$. If every vertex of S is adjacent to every vertex of $\overline{S}$, then $\mid [S, \overline{S}] \mid = \mid S \mid\mid \overline{S} \mid \geq$

[1] A Hamiltonian cycle is a cycle which contains every vertex of a graph

$n(G) - 1 \geq \kappa(G)$, and the desired inequality holds.
Otherwise, we choose $x \in S$ and $y \in \overline{S}$ with $x \not\leftrightarrow y$. Let T consist of all neighbors of x in $\overline{S}$ and all vertices of $S - \{x\}$ with neighbors in $\overline{S}$. Every x, y path passes through T, so T is a separating set. Also, picking the edges from x to $T \cap \overline{S}$ and one edge from each vertex of $T \cap S$ to $\overline{S}$ (shown bold below) yields $\mid T \mid$ distinct edges of $[S, \overline{S}]$. Thus $\kappa^{'}(G) = \mid [S, \overline{S}] \mid \geq \mid T \mid \geq \kappa(G)$. □

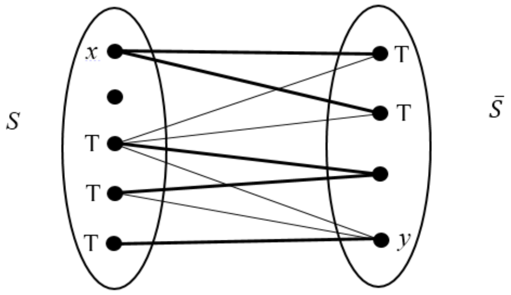

Figure 2.5

Proposition 2.5.2. *Let R be any finite ring, and let $\kappa(G_R)$ and $\kappa^{'}(G_R)$ denote (respectively) the vertex-connectivity and edge-connectivity of its unitary Cayley graph. Then $\kappa(G_R) = \kappa'(G_R) = \phi(R)$.*

Proof. According to Whitney [1932a] $\kappa(G_R) \leq \kappa^{'}(G_R) \leq \mid R^* \mid$ holds. The other direction can be done by showing that that G_R is edge-transitive by observing that for any edge $\{u, v\}$ the automorphism $x \mapsto (v - u)^{-1}(x - u)$ maps u to 0 and v to 1. Hence $\kappa(G_R) = \mid R^* \mid$, it follows that $\kappa(G) = \kappa^{'}(G) = \phi(R)$. □

Chapter 3

Digraphs Associated With Quadratic Polynomials

The quadratic polynomial $x^2 - ax + b$ is reducible over the ring R if it can be factored as $x^2 - ax + b = (x-c)(x-d)$, where $a = c + d$, and $b = cd$. For $n < \infty$, one can construct a mapping $\varphi : R \times R \longrightarrow R \times R$ in the form $(a, b) \longmapsto (a+b, a.b)$. This mapping defines a relation between finite commutative rings R and digraphs [1]. In this chapter the finite commutative ring $\mathbb{Z}_n$ is chosen to work on.

3.1 Introduction

Let $A = \mathbb{Z}_n$ be a finite ring. Define a mapping $\varphi : A^2 \to A^2$ by $(a, b) \longmapsto (a+b, ab)$. Likely, it reflects the ring structure of A. This mapping can be interpreted as a finite directed graph $G = G(A)$ with vertices A^2 and arrows defined by φ. The main idea is to deduce, if possible, ring properties of A from graph properties of G such as, the number of components, the lengths of longest paths and longest cycles, the maximal degree of vertices, etc. The graphs $G(\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z})$ should reflect some number-theoretic properties of integers.

Since $\mathbb{Z}_n$ is finite, it has integer characteristic n. We see that either n is prime, $\mathbb{Z}_n$ is a field and $\mathbb{Z}_n[x]$ is a UFD, or n is not prime, $\mathbb{Z}_n$ has zero-divisors and $\mathbb{Z}_n[x]$ does not have the UF property.

Example 3.1.1. *The following digraphs represents the digraphs of the rings $\mathbb{Z}_1$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. We note that $G(\mathbb{Z}_4)$ and $G(\mathbb{Z}_2 \times \mathbb{Z}_2)$ are not homomorphic, because the digraph $G(\mathbb{Z}_4)$ contains 5 cycles (or 5 closed walks), which is not*

[1] This kind of associations between digraphs and finite rings is proposed by Aleksandar Lipkovski (e.g [15])

satisfied in the digraph $G(\mathbb{Z}_2 \times \mathbb{Z}_2)$.

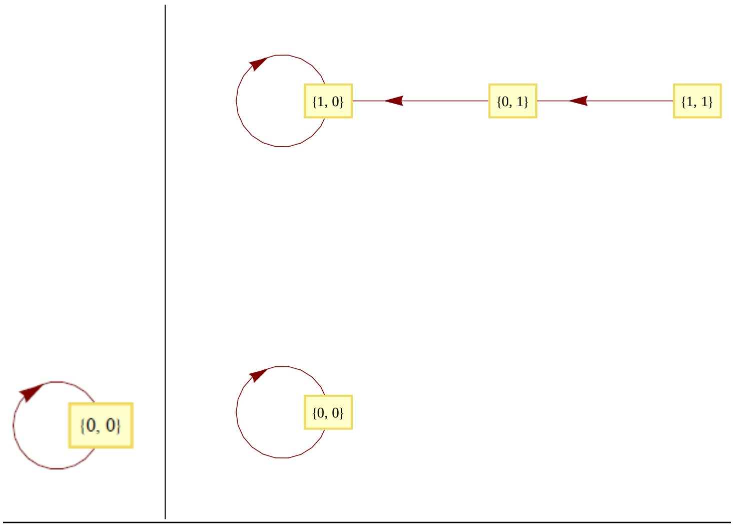

FIGURE 3.1: Digraphs $G_1 = G(\mathbb{Z}_1)$ and $G_2 = G(\mathbb{Z}_2)$

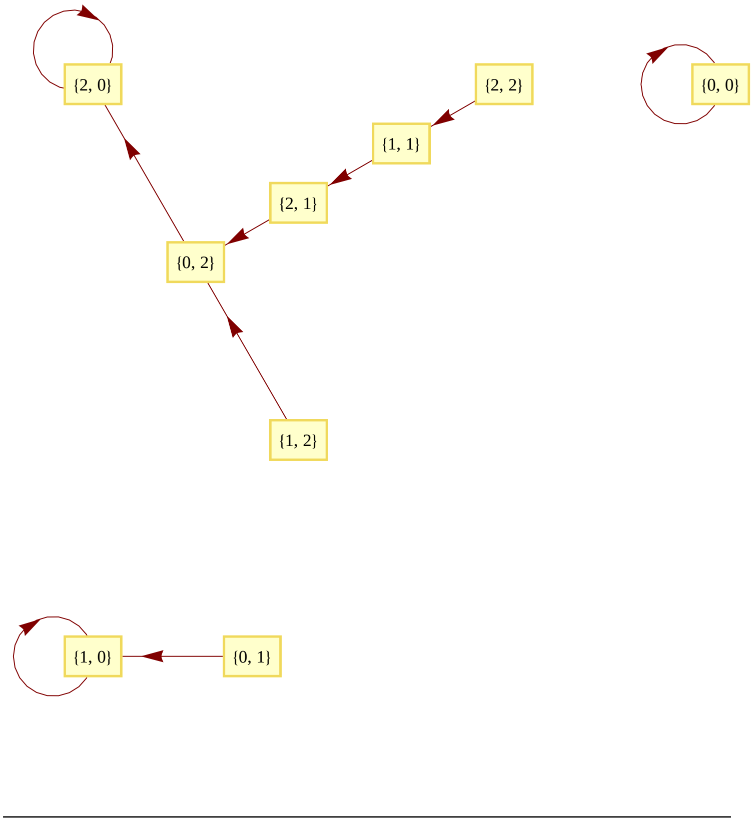

FIGURE 3.2: Digraph $G_3 = G(\mathbb{Z}_3)$

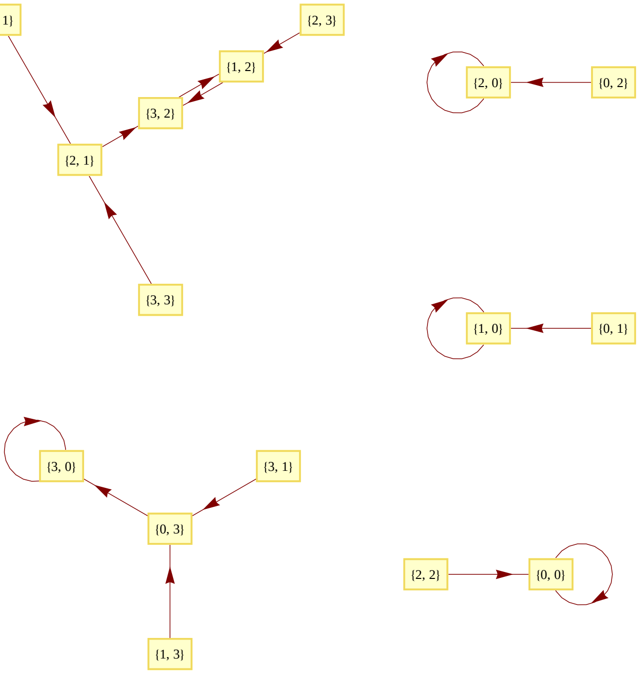

Figure 3.3: Digraph $G_4 = G(\mathbb{Z}_4)$

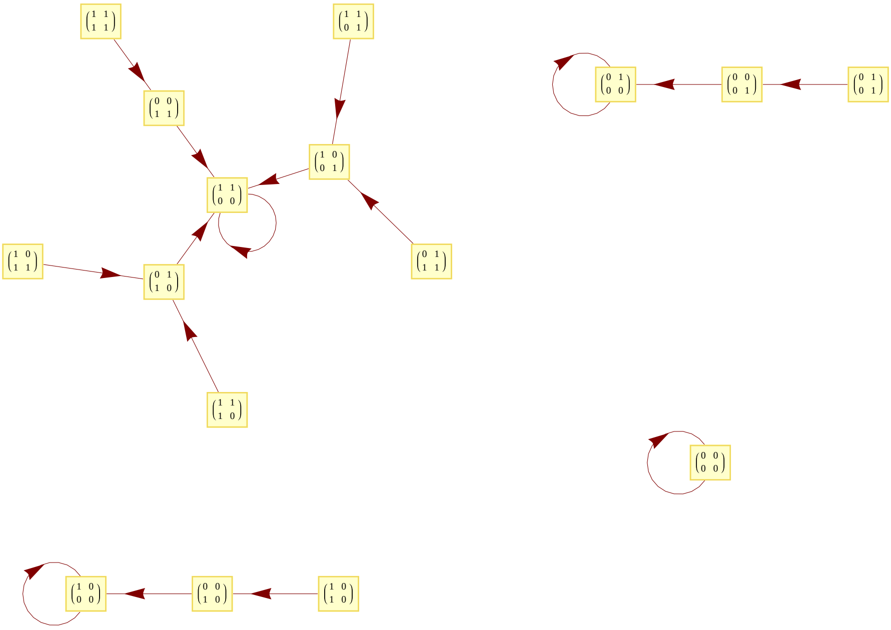
$\begin{pmatrix}1&1\\1&1\end{pmatrix}$
$\begin{pmatrix}1&1\\0&1\end{pmatrix}$
$\begin{pmatrix}0&1\\0&0\end{pmatrix}$
$\begin{pmatrix}0&0\\0&1\end{pmatrix}$
$\begin{pmatrix}0&1\\0&1\end{pmatrix}$
$\begin{pmatrix}0&0\\1&1\end{pmatrix}$
$\begin{pmatrix}1&0\\0&1\end{pmatrix}$
$\begin{pmatrix}1&1\\0&0\end{pmatrix}$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

Figure 3.4: Digraph of $\mathbb{Z}_2 \times \mathbb{Z}_2$

3.2 Degrees and Vertices

As we mentioned previously, the definition of the outgoing (incoming) degree of the vertex (a, b) is the number of arrows beginning (ending) in this vertex. Since G is a graph of a function, then the outgoing degree of each vertex (a, b) equals one. One may ask what the incoming degree of the vertex (a, b) is. The answer is shown in the following Proposition.

Proposition 3.2.1. *The incoming degree of the vertex $(a, b) \in G$ equals the number of distinct roots of the quadratic polynomial $x^2 - ax + b \in \mathbb{Z}_n[x]$.*

Proof. See [15]. □

In the case of G_p for prime p, the incoming degree of a vertex (a, b) can be either 0 (if $x^2 - ax + b$ is irreducible, i.e., $0 \neq 4b - a^2 \in \mathbb{Z}_p$ is a quadratic nonresidue modulo p), or 1 (if $4b - a^2 = 0$), or 2 (if $4b - a^2 \neq 0$ is a quadratic residue modulo p).

In the case of G_n for nonprime n, the incoming degree of a vertex (a, b) can be greater than 2, which depends on the different factorizations of $x^2 - ax + b$.

Theorem 3.2.1. *Let $p_1, p_2, ..., p_k$ be the composition of the number n. Then the highest indegree of any vertex (a, b) in the graph $G(\mathbb{Z}_n)$ is less than or equal to 2^k.*

Proof. Consider $x^2 - ax + b = 0$ be any reducible quadratic polynomial over $\mathbb{Z}_n$. Since the incoming degree of a vertex (a, b) is the number of roots of its polynomial. Then According to Theorem 1.1.6 and Proposition 1.1.6, we observe that

$$indeg(a, b) = 2 \times 2 \times ... \times 2(k - times) = 2^k. \quad \square$$

The starting vertices (a, b) (with incoming degree 0) correspond to irreducible quadratic polynomials $x^2 - ax + b$ in $\mathbb{Z}_n[x]$. It can easily be seen that the number i of irreducible quadratic polynomials is $i \geq n^2 - \binom{n+1}{2} = \frac{n(n-1)}{2}$ ($\mathbb{Z}_n[x]$ has unique factorization exactly when n is prime, and then the equality holds), therefore the number of starting vertices is i. This gives a rough upper estimate for the number of components $c_n \leq i$.

3.3 Components and Closed Paths

Consider closed paths, or cycles, in G. Up to cyclic permutations, the cycles are described by the corresponding arrow sequences.

Definition 3.3.1. *The sequence*

$$(a_1, b_1) \to (a_2, b_2) \to ... \to (a_k, b_k). \tag{3.1}$$

of arrows in G defines a cycle of length k (or a k-cycle) if $(a_k + b_k, a_k b_k) = (a_1, b_1)$ and $(a_i + b_i, a_i b_i) \neq (a_j, b_j)$ for all $j \leq i < k$.

We see from figure 3.3 that there may exist cycles of length 1 as well as longer cycles. The definition also implies that if $k > 1$, then every $b_i \neq 0$.

Proposition 3.3.1. 1. *There are exactly $n = \#A$ cycles of length 1 in G, and they correspond to the vertices $(a, 0)$.*

2. *Each connected component of G contains exactly one cycle, and the number of connected components is $n + \#\{cycles\ of\ length > 1\}$.*
3. *The graph G_1 is a (weakly) connected component of G if and only if A has no nontrivial nilpotent elements.*

Proof. See [15]. □

Observe that in this subject the girth of the digraph G_n is 1, while the diameter is infinity.

Proposition 3.3.2. *For $k = 1$, the sequence" (3.1) is a 1-cycle $\Longleftrightarrow \sigma_1(b) = 0$.*
For $k = 2$, the sequence (3.1) is a 2-cycle $\Longleftrightarrow \sigma_1(b) = \sigma_2(b) = 0$.
For $k = 3$, the sequence (3.1) is a 3-cycle $\Longleftrightarrow \sigma_1(b) = \sigma_2(b) = \sigma_3(b) = 0$.

Proof. See [15]. □

Remarks

1. In the ring $A = \mathbb{Z}_n$, this is equivalent to the condition that n is not squarefree, since $\mathbb{Z}_n$ has no nontrivial nilpotents if and only if n is square-free. This leads to an (inefficient) algorithm for deciding whether a given integer n is square-free: look for 2-cycles in the corresponding graph G_n.
2. The existence of a 3-cycle implies that the ring $\mathbb{Z}_n$ for non-prime n has zero-divisors, since in such case $b_1 b_2 b_3 = 0$ and all $b_i \neq 0$.
3. If the sequence (3.1) is a $k - cycle$, then $\sigma_1(b) = \sigma_2(b) = ... = \sigma_k(b) = 0$. However, as the example $A = \mathbb{Z}_5$ shows, it is already false for $k = 4$: there is a 4-cycle $(2, 2) \longrightarrow (4, 4) \longrightarrow (3, 1) \longrightarrow (4, 3)$ such that $\sigma_1(b) = \sigma_2(b) = \sigma_3(b) = 0$ and $\sigma_4(b) \neq 0$.
4. For any prime number p, if the digraph $G(\mathbb{Z}_p)$ contains $k - cycle$, $k > 1$. Then $\sigma_k(b) \neq 0$, that is because $\mathbb{Z}_p$ is free of zero-divisors.
5. In the $k - cycle$, $k > 1$ we have $b_1 + b_2 + ... + b_k = 0$, $b_1^2 + b_2^2 + ... + b_k^2 = 0$ and $a_1^n.a_2^n...a_k^n = 1$ for any $n \geq 1$.
6. The graph (G_8) in [15] is represented as follows

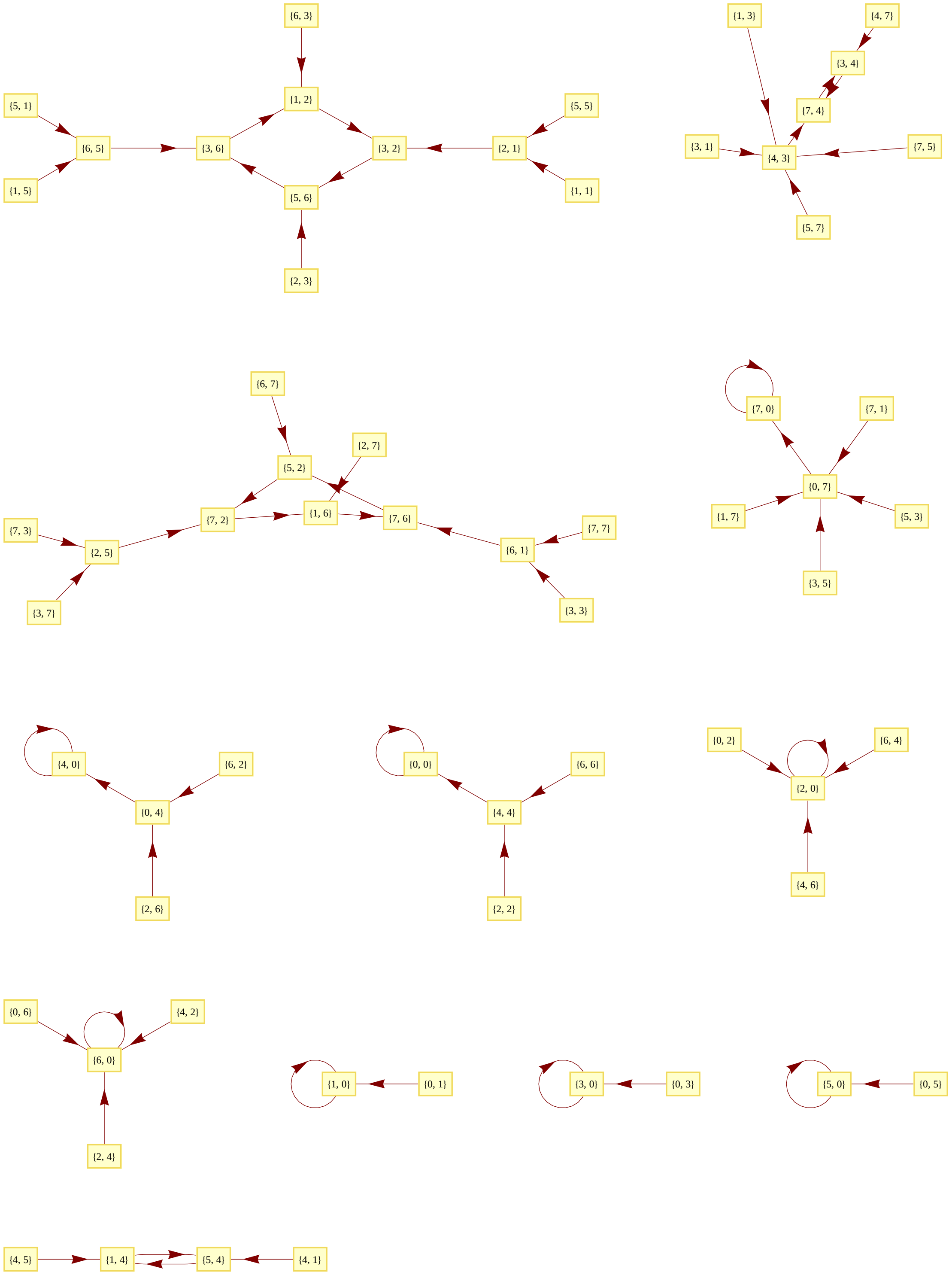

Figure 3.5: Digraph of $\mathbb{Z}_8$

3.4 Further Properties

Let p and q be relatively prime numbers, such that $n = pq$, $p < q$. Define a map

$$\varphi_1 : \mathbb{Z}_n \to \mathbb{Z}_p$$

that maps representatives $0 \leq a < n$ in $\mathbb{Z}_n$ to $(a \mod p)$ in $\mathbb{Z}_p$. Since p divides n, then φ_1 is a homomorphism. Moreover, $ker\varphi_1 = p\mathbb{Z}_n < \mathbb{Z}_n$, and $\mid ker\varphi_1 \mid= p$. Similarly, the same holds for $\varphi_2 : \mathbb{Z}_n \to \mathbb{Z}_q$.

Observe that mappings φ_1 and φ_2 induce mappings of corresponding graphs, which will be denoted again by φ_1 and φ_2.

We will denote the longest cycle in the digraph $G(\mathbb{Z}_n)$ by $\overrightarrow{C_m}$ for short, and all our discussion later will be based on the construction of φ_1 and φ_2. Furthermore, we will refer to $\mathbb{Z}_n$, $\mathbb{Z}_p$ and $\mathbb{Z}_q$ as sets of natural numbers.

Since a closed walk might be a cycle, so according to the structure of φ_1 and φ_2 and the sequence 3.1, we can reformulate the Corrollary 1.2.5 as follows:

Corollary 3.4.1. *A mapping $f : V(\overrightarrow{C}_k) \to V(G)$ is a homomorphism of $\overrightarrow{C}_k$ to G if and only if $f(1), f(2), ..., f(k)$ is a cycle in G.*

That means, a closed walk, which is mapped by $\varphi_1(\varphi_2)$ is a cycle. This consequence will be used in this work from now on.

Proposition 3.4.1. *Let $\overrightarrow{C_m}$ and $\overrightarrow{C_{n_1}}$ be two directed cycles in $G(\mathbb{Z}_n)$ and $G(\mathbb{Z}_p)$ respectively. If $\overrightarrow{C_m} \mapsto \overrightarrow{C_{n_1}}$, then we have n_1 divides m.*

Proof. Suppose that $\overrightarrow{C_m}$ is a s-cycle; that is,

$$(a_1, b_1) \to (a_2, b_2) \to ... \to (a_s, b_s).$$

Since φ_1 is a homomorphism, then

$$(\varphi_1(a_1), \varphi_1(b_1)) \to (\varphi_1(a_2), \varphi_1(b_2)) \to ... \to (\varphi_1(a_s), \varphi_1(b_s))$$

is a cycle in $G(\mathbb{Z}_p)$, and

$$\begin{aligned}(\varphi_1(a_1), \varphi_1(b_1)) &= (\varphi_1(a_s + b_s), \varphi_1(a_s.b_s)) \\ &= (\varphi_1(a_s) + \varphi_1(b_s), \varphi_1(a_s).\varphi_1(b_s)) \qquad (3.2)\end{aligned}$$

Since φ_1 connects q elements in $\mathbb{Z}_n$ into every element $a \in \mathbb{Z}_p$, so that gives us two cases:

1. If $(\varphi_1(a_1), \varphi_1(b_1))$=$(\varphi_1(a_2), \varphi_1(b_2))$. Then by (1), this process will be repeated for all $(\varphi_1(a_i), \varphi_1(b_i))$, $i = 2, ..., s$. Thus $n_1 = 1$ and $m = s.n_1$.

2. If $(\varphi_1(a_1), \varphi_1(b_1)) = (\varphi_1(a_j), \varphi_1(b_j))$, for some $2 < j < s$. Then $(\varphi_1(a_i), \varphi_1(b_i))$, $i < j$ are all different. So according to (3.2) $m = t.n_1$, for $1 \leq t < s$. Hence m is divisible by n_1. □

If we suppose that $n_1|n_2$, $n_1 \neq 1$ (n_1 might equal to n_2), then it is not proved yet that the maps φ_1 and φ_2 send the longest cycle $\overrightarrow{C}_m$ in $G(\mathbb{Z}_n)$ to longest cycles $\overrightarrow{C}_{n_1}$ and $\overrightarrow{C}_{n_2}$ in $G(\mathbb{Z}_p)$ and $G(\mathbb{Z}_q)$ respectively. Because the cycles in $G(\mathbb{Z}_p)$ and $G(\mathbb{Z}_q)$ which is smaller than $\overrightarrow{C}_{n_1}$ and $\overrightarrow{C}_{n_2}$ might have a pre-image which is a cycle with length longer than the pre-image of $\overrightarrow{C}_{n_1}$ and $\overrightarrow{C}_{n_2}$ themselves. For instance, let $\overrightarrow{C}_{n_1} = \overrightarrow{C}_3$ and $\overrightarrow{C}_{n_2} = \overrightarrow{C}_6$ then the pre-image for both of them is $\overrightarrow{C}_6$ while the pre-image of cycles $\overrightarrow{C}_3$ and $\overrightarrow{C}_5$ is a cycle $\overrightarrow{C}_{15}$ which is longer than$\overrightarrow{C}_6$. So this case is not considerable in the following proposition. As a matter of fact the computer calculations show that for n from 1 to 200 this exception case does not exist at all.

Proposition 3.4.2. *The maps φ_1 and φ_2 send the longest directed cycle $\overrightarrow{C}_m$ to the longest directed cycles $\overrightarrow{C}_{n_1}$ and $\overrightarrow{C}_{n_2}$ respectively.*

Proof. Suppose that $\overrightarrow{C}_{n_1}$, $\overrightarrow{C}_{n_2}$ are the longest cycles in $G(\mathbb{Z}_p)$ and $G(\mathbb{Z}_q)$ respectivaly. Then n_1, n_2 will have only two possible cases:

Case (1) If $n_1 = 1$, the cycles $\overrightarrow{C}_{n_1}$ and $\overrightarrow{C}_{n_2}$ have the same pre-image. Let us call it $\overrightarrow{C}_r$, so $n_1|r, n_2|r$ (see Proposition 3.4.1), and by Chinese Reminder Theorem $r = n_2$. Our goal now is to prove that $\overrightarrow{C}_r$ is the longest cycle in $G(\mathbb{Z}_n)$.

Assume that there is an another cycle $\overrightarrow{C}_d \neq \overrightarrow{C}_r$ such that $d > r$, then the length of $\varphi_1(\overrightarrow{C}_d)$ divides the length of $\overrightarrow{C}_d$, also the length of $\varphi_2(\overrightarrow{C}_d)$ divides the length of $\overrightarrow{C}_d$. Then again by using Chinese Reminder Theorem we get $\varphi_1(\overrightarrow{C}_d) > \overrightarrow{C}_{n_1}$ or $\varphi_2(\overrightarrow{C}_d) > \overrightarrow{C}_{n_2}$ (This inequality holds whether $\varphi_1(\overrightarrow{C}_d)$ and $\varphi_2(\overrightarrow{C}_d)$ are relatively primes or they are not relatively primes); This contradicts our assumption, that is $\overrightarrow{C}_{n_1}, \overrightarrow{C}_{n_2}$ are the longest cycles.

Case (2) If (n_1, n_2)=1. As we have done in the case (1), the cycles $\overrightarrow{C}_{n_1}$ and $\overrightarrow{C}_{n_2}$ will have the same pre-image $\overrightarrow{C}_r$ where $n_1|r$, and $n_2|r$. Suppose that there is an another cycle $\overrightarrow{C}_q$ such that $q > r$, then the length of $\varphi_1(\overrightarrow{C}_q)$ divides the length of $\overrightarrow{C}_q$ and the length of $\varphi_2(\overrightarrow{C}_q)$ divides the length of $\overrightarrow{C}_q$ (see Proposition 3.4.1).

- If the length of $\varphi_1(\overrightarrow{C}_q) = n_1$, then the length of $\varphi_2(\overrightarrow{C}_q) > n_2$. Similarly if $\varphi_2(\overrightarrow{C}_q) = n_2$, then the length of $\varphi_1(\overrightarrow{C}_q) > n_1$. Both cases contradict with our assumption.
- If the length of $\varphi_1(\overrightarrow{C}_q) = 1$, in this case the length of $\overrightarrow{C}_q$ equals the length of $\varphi_2(\overrightarrow{C}_q)$, which means $\varphi_2(\overrightarrow{C}_q) > n_2$. This is a contradiction.
- If the length of $\varphi_1(\overrightarrow{C}_q) < n_1$ and it is not 1. Then $\varphi_2(\overrightarrow{C}_q) > n_2$ because $\overrightarrow{C}_q > \overrightarrow{C}_r$, where lengths of the last cycles is the product of $\varphi_1(\overrightarrow{C}_q)$, $\varphi_2(\overrightarrow{C}_q)$ and $\overrightarrow{C}_{n_1}$, $\overrightarrow{C}_{n_2}$ respectively. This case indicates a contradiction.

Hence in both cases we have proved that $\overrightarrow{C}_r = \overrightarrow{C}_m$ which completes the proof. □

Theorem 3.4.1. *Let $p, q \in \mathbb{N}$ be relatively prime numbers, i.e., gcd$(p, q) = 1$. Let $n = p.q$. Then, the length of the longest cycle $\overrightarrow{C_m}$ is the least common multiple of n_1 and n_2, where n_1 and n_2 are the lengths of the longest cycles $\overrightarrow{C_{n_1}}$ and $\overrightarrow{C_{n_2}}$ respectively.*

Proof. We will use the Lemma 1.1.4 in the proof. Consider that $\overrightarrow{C_m}$ is a s-cycle, that is

$$(a_1, b_1) \to (a_2, b_2) \to ... \to (a_s, b_s).$$

Then, $h_1(\overrightarrow{C_m})$ is a cycle in $G(\mathbb{Z}_p)$. Similarly, $h_2(\overrightarrow{C_m})$ is a cycle in $G(\mathbb{Z}_q)$. So according to propositions 3.4.1 and 3.4.2, we have the following cases:

1. If $(a_1, b_1) \in \mathbb{Z}_p \times \mathbb{Z}_p \subset G(\mathbb{Z}_n)$. Then, both h_1 and h_2 send (a_1, b_1) to the same vertex, so that the cycle $\overrightarrow{C_m}$ must terminate at the first multiple of n_1 and n_2, because (a_1, b_1) is a unique original vertex of $(\varphi_1(a_1), \varphi_1(b_1))$ and $(\varphi_2(a_1), \varphi_2(b_1))$.
2. If $(a_1, b_1) \notin \mathbb{Z}_p \times \mathbb{Z}_p$. Then, the map φ_1 sends the element t in $\mathbb{Z}_n$ to element $(t \mod m)$ in $\mathbb{Z}_p$. Similarly, the map φ_2 sends the element t in $\mathbb{Z}_n$ to element $(t \mod k)$ in $\mathbb{Z}_q$. Since m and k are two different modules, by Chinese Remainder Theorem, two different vertices $(\varphi_1(a_1), \varphi_1(b_1))$ and $(\varphi_2(a_1), \varphi_2(b_1))$ uniquely determine the original vertex (a_1, b_1). Thus the length of $\overrightarrow{C_m}$ terminates exactly at the first multiple of the lengths of $\overrightarrow{C_{n_1}}$ and $\overrightarrow{C_{n_2}}$. Hence the proof follows. □

Theorem 3.4.2. *Let $p_1, ..., p_r \in \mathbb{N}$ be pairwise relatively prime numbers, i.e., gcd$(p_i, p_j) = 1$ for $i \neq j$. Let $n = p_1 ... p_r$. Then the longest cycle $\overrightarrow{C_n}$ in $G(\mathbb{Z}_n)$ has a length $m = LCM(n_1, n_2, ..., n_r)$, where $n_1, n_2, ..., n_r$ are the lengths of the longest cycles in $G(\mathbb{Z}_{p_1})$, $G(\mathbb{Z}_{p_2})$, ..., $G(\mathbb{Z}_{p_r})$ respectively.*

Proof. The proof can be done directly by using induction involving Chinese Remainder Theorem. □

The following Proposition is well known as Fermat Little Theorem, and it is represented here for the sake of completeness.

Proposition 3.4.3. *Let p be a prime and $a \in \mathbb{Z}$ be a number that is prime to p (i.e., p does not divide a). Then*

$$a^{p-1} \equiv 1 \; mod \; p.$$

Proposition 3.4.4. *The length of the longest cycle $\overrightarrow{C_{l_{p^m}}}$ can be p^{m-1} or $\alpha.\beta$ for some $\alpha > 1$, where $1 < \beta$ is the length of the cycle, which is less than or equal to $\overrightarrow{C_{n_1}}$.*

Proof. Let p be a prime number, and $m > 1$ be any integer. The function $\varphi : \mathbb{Z}_{p^m} \to \mathbb{Z}_p$ which is defined by $\varphi(a) = a \mod p$ is a homomorphism, and $ker\varphi = p\mathbb{Z}_{p^m} < \mathbb{Z}_{p^m}$, where $\mid ker\varphi \mid = p^{m-1}$.
Suppose that

$$(a_1, b_1) \to (a_2, b_2) \to ... \to (a_s, b_s)$$

is the longest cycle $\overrightarrow{C_{l_{p^m}}}$ in $G(\mathbb{Z}_{p^m})$. Therefore, we have
If $b_1 \in ker\varphi$, then $\varphi(\overrightarrow{C_{l_{p^m}}})$ will be $(a, 0)$, $a = \varphi(a_1) \in \mathbb{Z}_p$. Since then, $l_{p^m} = p^{m-1}$. To prove that, We will consider the case $m = 2$, then use the mathematical induction. Suppose $b_1 \in ker\varphi$, so b_1 can be written in the form tp, where $1 \leq t < p$. Applying the mapping φ on $\overrightarrow{C_{l_{p^2}}}$ yeilds;

$$(a_1, tp) \to (a_1 + tp, a_1tp) \to ... \to (a_1 + (1 + a_1 + a_1^2 + ... + a_1^{p-2}), a_1^{p-1}tp)$$

From Fermat Little Theorem we have the following:
$a_1^{p-1}p \equiv p \; mod \; p^2$
$(a_1^{p-1} - 1)p \equiv 0 \; mod \; p^2$
Since then,

$$(a_1 + (1 + a_1 + a_1^2 + ... + a_1^{p-2}), a_1^{p-1}tp) = (a_1, tp)$$

Which means that this path is closed at (a_1, tp). Therefore, the length of this cycle is p.
If $b_1 \notin ker\varphi$, then a_1 won't be in $ker\varphi$ neither. Thus we have a cycle $\varphi(\overrightarrow{C_{p^m}})$ with length more that 1. According to theorem 3.4.1, we observe that the length of the cycle $\varphi(\overrightarrow{C_{n_1}})$ divides l_{p^m}. Hence $l_{p^m} = \alpha\beta$ for some $\alpha > 1$. □

Note that, at the moment there is no way to determine the value of α in the second case. For instance, when $n = 5$, 5-cycle is the longest cycle in $G(\mathbb{Z}_{25})$. At the same time, 4-cycle is the longest cycle in $G(\mathbb{Z}_5)$. When $n = 11$, 30-cycle is the longest cycle in $G(\mathbb{Z}_{121})$. At the same time, 6-cycle is the longest cycle in $G(\mathbb{Z}_{11})$.

Theorem 3.4.3. *Let $n \in \mathbb{N}$ and $n = p_1^{n_1} p_2^{n_2} ... p_r^{n_r}$ be the decomposition of n into primes, such that $p_i \neq p_j$ for $i \neq j$, Then, the longest cycle $\overrightarrow{C_n}$ of $G(\mathbb{Z}_n)$ has a length $m = LCM(l_{p_1^{n_1}}, l_{p_2^{n_2}}, ..., l_{p_r^{n_r}})$, where $l_{p_1^{n_1}}, l_{p_2^{n_2}}, ..., l_{p_r^{n_r}}$ are the lengths of the longest cycles in $G(\mathbb{Z}_{p^{n_1}})$, $G(\mathbb{Z}_{p^{n_2}})$, ..., $G(\mathbb{Z}_{p^{n_r}})$ respectively.*

Proof. The proof holds by following the preceding argument, Theorem 3.4.2 and Chinese Remainder Theorem. □

Theorem 3.4.4. *Suppose that $n \cong 1 (mod\ m)$. There is a cycle of length $r, r \geq 1$ in the graph $G(\mathbb{Z}_{mn})$(not neccessary the longest one) if and only if the longest cycle in $G(\mathbb{Z}_m)$ is of length r.*

Proof. assume that $\overrightarrow{C_r}$ is the longest cycle in the graph $G(\mathbb{Z}_m)$, that is

$$(a_1, b_1) \rightarrow (a_2, b_2) \rightarrow ... \rightarrow (a_r, b_r)$$

Since f is a homomorphism. Then $f(\overrightarrow{C_r})$ is a cycle in the graph $G(\mathbb{Z}_{mn})$. Since every element in Imf is of the form $[na]_{mn}, a \in \mathbb{Z}_m$, therefore, we notice that

$$(f(a_1), f(b_1)) = (na_1, nb_1) = (n(a_r + b_r), n(a_r.b_r))$$

Since f is injective. Then $f(\overrightarrow{C_r})$ is a cycle of length r.
($\Rightarrow$) This direction can be proved easily by taking a map $g : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m$, where $g(a) = [a]_m$. □

For more generalization, we show graphs of the direct product of rings of integers modulo n.

Theorem 3.4.5. *Let p and q be any two prime numbers. Then the longest cycle in the graph $G(\mathbb{Z}_p \times \mathbb{Z}_q)$ is a cycle of length $n = LCM(n_1, n_2)$, where n_1 is the length of the longest cycle in $G(\mathbb{Z}_p)$ and n_2 is the length of the longest cycle in $G(\mathbb{Z}_q)$.*

Proof. The projection map $\varphi_1 : \mathbb{Z}_p \times \mathbb{Z}_q \rightarrow \mathbb{Z}_p$, where $\varphi_1((a, b)) = [a]_p$ is a homomorphism.
Also the map $\varphi_2 : \mathbb{Z}_p \times \mathbb{Z}_q \rightarrow \mathbb{Z}_q$, where $\varphi_2((a, b)) = [b]_q$ is a homomorphism.
Suppose that $(a_1, b_1) \rightarrow (a_2, b_2) \rightarrow ... \rightarrow (a_r, b_r)$ is the longest cycle in the graph $G(\mathbb{Z}_p \times \mathbb{Z}_q)$, where $a_i, b_i \in Z_p \times \mathbb{Z}_q$.

Since φ_1 is a homomorphism then,

$$\begin{aligned} \varphi_1((a_1, b_1)) &= (\varphi_1(a_1), \varphi_1(b_1)) \\ &= (\varphi_1(a_r + b_r), \varphi_1(a_r.b_r)) \\ &= (\varphi_1(a_r) + \varphi_1(b_r), \varphi_1(a_r).\varphi_1(b_r)) \end{aligned} \tag{3.3}$$

From the definition of φ_1, we observe that $\varphi_1(a_i)$ is the first coordinate of a_i, we will refere to it by a_{i1}, similarly, $\varphi_1(b_i)$ is the first coordinate of b_i, we will refere to it by b_{i1}.
$\varphi_2(a_i)$ is the second coordinate of a_i, we will refer to it by a_{i2}, similarly, $\varphi_2(b_i)$ is the second coordinate of b_i, we will refer to it by b_{i2}.
Thus, from (3.3) we get

$$(a_{11}, b_{11}) = (a_{r1} + b_{r1}, a_{r1}.b_{r1}). \tag{3.4}$$

It is clear that $\varphi_1(\overrightarrow{C_r})$ is a cycle in $G(\mathbb{Z}_p)$, also it satisfies (3.4). That shows us $\varphi_1(\overrightarrow{C_r})$ divides $\overrightarrow{C_r}$.
If we repeat the same procedure on φ_2, we get

$$\begin{aligned} \varphi_2((a_1, b_1)) &= (\varphi_2(a_1), \varphi_2(b_1)) \\ &= (\varphi_2(a_r + b_r), \varphi_2(a_r.b_r)) \\ &= (\varphi_2(a_1) + \varphi_2(b_r), \varphi_2(a_r).\varphi_2(b_r)) \end{aligned} \tag{3.5}$$

Therefore,

$$(a_{12}, b_{12}) = (a_{r2} + b_{r2}, a_{r2}.b_{r2}). \tag{3.6}$$

It is clear that $\varphi_2(\overrightarrow{C_r})$ is a cycle in $G(\mathbb{Z}_q)$, also it satisfies (3.6). That shows us $\varphi_2(\overrightarrow{C_r})$ divides $\overrightarrow{C_r}$, which means $\overrightarrow{C_r}$ is a multiple of $\varphi_1(\overrightarrow{C_r})$ and $\varphi_2(\overrightarrow{C_r})$.
Observe that n_1 and n_2 are the lengths of the longest cycles in the graphs $G(\mathbb{Z}_p)$ and $G(\mathbb{Z}_q)$ respectivily. Furthermore, the maps φ_1 and φ_2 are onto and the multiple of these two cycles is longer than any other two cycles.
Therefore, according to Theorem 3.4.1, we find that the length of $\overrightarrow{C_r}$ is the Least Common Multiple of $\varphi_1(\overrightarrow{C_r})$ and $\varphi_2(\overrightarrow{C_r})$. □

Theorem 3.4.6. *Let p be a prime number, and $\overrightarrow{C_{n_1}}$ is the longest cycle in the graph $G(\mathbb{Z}_p)$. The longest cycle in the graph $G(\mathbb{Z}_p \times \mathbb{Z}_p)$ is a cycle of length*

1. *$k = LCM(n_1, \beta)$, if there is a cycle of length β such that $1 < \beta < n_1$ and $(n_1, \beta) = 1$.*

2. *$k = n_1$ if there is no such a cycle $\overrightarrow{C_\beta}$, $1 < \beta < n_1$. Or the only cycles which are shorter than $\overrightarrow{C_{n_1}}$ are cycles of length divides n_1.*

Proof. Define the maps $\varphi_1 : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$, by $\varphi_1((a, b)) = [a]_p$, and $\varphi_2 : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$, by $\varphi_2((a, b)) = [b]_p$.

The maps φ_1 and φ_2 are homomorphisms and onto. Consider that $\overrightarrow{C_r}$ is the longest cycle in $G(\mathbb{Z}_p \times \mathbb{Z}_p)$; that is, $(a_1, b_1) \to (a_2, b_2) \to ... \to (a_r, b_r)$, where $a_i, b_i \in Z_p \times Z_p$.

Since φ_1 is a homomorphism then,

$$\begin{aligned} \varphi_1((a_1, b_1)) &= (\varphi_1(a_1), \varphi_1(b_1)) \\ &= (\varphi_1(a_r + b_r), \varphi_1(a_r.b_r)) \\ &= (\varphi_1(a_r) + \varphi_1(b_r), \varphi_1(a_r).\varphi_1(b_r)) \end{aligned} \tag{3.7}$$

We will use the same notations as we mentioned in the last theorem. a_{i1} refers to the first coordinate in the element a_i. Similarly, b_{i1} refers to the first coordinate of $b_i.a_{i2}$ refers to the second coordinate in the element a_i, similarly, b_{i2} refers to the first coordinate of b_i.

Thus, from (3.7) we get

$$(a_{11}, b_{11}) = (a_{r1} + b_{r1}, a_{r1}.b_{r1}). \tag{3.8}$$

It is clear that $\varphi_1(\overrightarrow{C_r})$ is a cycle in $G(\mathbb{Z}_p)$, also it satisfies (3.8). That shows us $\varphi_1(\overrightarrow{C_r})$ divides $\overrightarrow{C_r}$.

If we repeat the same proccess on φ_2, we get

$$\begin{aligned} \varphi_2((a_1, b_1)) &= (\varphi_2(a_1), \varphi_2(b_1)) \\ &= (\varphi_2(a_r + b_r), \varphi_2(a_r.b_r)) \\ &= (\varphi_2(a_1) + \varphi_2(b_r), \varphi_2(a_r).\varphi_2(b_r)) \end{aligned} \tag{3.9}$$

Therefore,

$$(a_{12}, b_{12}) = (a_{r2} + b_{r2}, a_{r2}.b_{r2}). \tag{3.10}$$

It is clear that $\varphi_2(\overrightarrow{C_r})$ is a cycle in $G(\mathbb{Z}_q)$, it satisfies (3.10). That shows us $\varphi_2(\overrightarrow{C_r})$ divides $\overrightarrow{C_r}$.

Considering that φ_1 and φ_2 are onto, and $\overrightarrow{C_r}$ is multiple of $\varphi_1(\overrightarrow{C_r})$ and $\varphi_2(\overrightarrow{C_r})$. Then, by Chinese Reminder Theorem we have the following:

1. If $G(\mathbb{Z}_p)$ contains at least a cycle $\overrightarrow{C_\beta}$, such that $1 < \beta < n_1$, and $(n_1, \beta) = 1$. Then $m = LCM(n_1, \beta)$.
2. If $G(\mathbb{Z}_p)$ contains no cycles or contains cycle $\overrightarrow{C_\beta}$ such that $1 < \beta < n_1$, or $\beta | n_1$ Then $m = LCM(n_1, \beta) = n_1$.

The largest multiple that we can get is the longest cycle in $G(\mathbb{Z}_p)$, which means that the length of $\overrightarrow{C_r}$ is exactly the length of the longest cycle in $G(\mathbb{Z}_p)$. □

Theorem 3.4.7. *Let $p_1^{n_1}, p_2^{n_2}, ..., p_r^{n_r}$ be coprimes, such that $p_i \neq p_j$ for $i \neq j$, Then, the longest cycle $\overrightarrow{C_n}$ in $G(\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times ...\mathbb{Z}_{p_r^{n_r}})$ has a length $m = LCM(l_{p_1^{n_1}}, l_{p_2^{n_2}}, ..., l_{p_r^{n_r}})$, where $l_{p_1^{n_1}}, l_{p_2^{n_2}}, ..., l_{p_r^{n_r}}$ are the lengths of the longest cycles in $G(\mathbb{Z}_{p^{n_1}})$, $G(\mathbb{Z}_{p^{n_2}})$, ..., $G(\mathbb{Z}_{p^{n_r}})$ respectively.*

Proof. This theorem can be proved in other way. Define a mapping $\varphi : \mathbb{Z}_{p_1^{n_1} p_2^{n_2} ... p_r^{n_r}} \rightarrow \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times ...\mathbb{Z}_{p_r^{n_r}}$ by $\varphi([a]_{p_1^{n_1} p_2^{n_2} ... p_r^{n_r}}) = ([a]_{p_1^{n_1}}, [a]_{p_2^{n_2}}, ..., [a]_{p_r^{n_r}})$. This mapping is well defined. Furthermore, it is an isomorphism. We know that the longest cycle in $G(\mathbb{Z}_{p_1^{n_1} p_2^{n_2} ... p_r^{n_r}})$ is the least commmon multiple of the length of the longest cycles in the digraphs $G(\mathbb{Z}_{p^{n_1}})$, $G(\mathbb{Z}_{p^{n_2}})$, ..., and $G(\mathbb{Z}_{p^{n_r}})$ (e.g [16]). Since φ is bijection, Then the longest cycle in $G(\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times ...\mathbb{Z}_{p_r^{n_r}})$ has a length equal to the length of the longest cycle in $G(\mathbb{Z}_{p_1^{n_1} p_2^{n_2} ... p_r^{n_r}})$. □

Chapter 4

Matlab and Mathematica Algorithms

In this chapter we are going to present the algorithms, which have been built on computer softwares Mathematica and Mathlab, to calculate the requested associated digraphs in chapter 3. Some notations are presented and quoted from [17].

4.1 Fundamental Number-Theoretic Algorithms

An algorithm is an effective method expressed as a finite list of well defined instructions for calculating a function. Starting from an initial state and initial input, the instructions describe a computation that, when executed, proceeds through a finite number of well-defined successive states, eventually producing "output and terminating at a final ending state. For us, an algorithm will be a method which, given certain types of inputs, gives an answer after a finite amount of time.

Several things must be considered when one describes an algorithm. The first is to prove that it is correct, i.e. that it gives the desired result when it stops. Then, since we are interested in practical implementations, we must give an estimate of the algorithm's running time, if possible both in the worst case, and on average.

The size of the inputs for an algorithm will usually be measured by the number of bits that they require. For example, the size of a positive integer N is $[lgN] + 1$. We will say that an algorithm is linear, quadratic or polynomial time if it requires time $O(lnN)$, $O(ln^2N)$, $O(P(lnN))$ respectively, where P is a polynomial. If the time required is $O(Na)$, we say that the algorithm is exponential time. Finally, many algorithms have some intermediate running time, for example

$$e^{C\sqrt{lnNlnlnN}},$$

which is the approximate expected running time of many factoring algorithms and of recent algorithms for computing class groups. In this case we say that the algorithm is sub-exponential.

One of the most common operations used in number theory is modular multiplication, i.e. the computation of ab modulo some number N, where a and b are non-negative integers less than N. This can, of course, be trivially done using the formula $div(mul(a, b), N)$, the result being the value of remainder. When many such operations are needed using the same modulus N, there is a more clever way of doing this, due to P. Montgomery which can save 10 to 20 percent of the running time, and this is not a negligible saving since it is an absolutely basic operation.

Many of the algorithms that we give are valid over any base ring or field R where we know how to compute. We must emphasize however that the behavior of these algorithms will be quite different depending on the base ring. Let us look at the most important example.

The simplest rings are the rings $R = \mathbb{Z}/N\mathbb{Z}$, especially when N is small. Operations in R are simply operations "modulo N" and the elements of R can always be represented by an integer less than N, hence of bounded size. Using the standard algorithms mentioned in the preceding section, and a suitable version of Euclid's extended algorithm to perform division, all operations need only $O(ln^2N)$ bit operations (in fact $O(1)$ since N is considered as fixed!). An important special case of these rings R is when $N = p$ is a prime, and then $R = \mathbb{F}_p$ the finite field with p elements. More generally, it is easy to see that operations on any finite field $\mathbb{F}_q$ with $q = p^k$ can be done quickly.

4.2 Introduction to Mathematica

Mathematica is a program created by physicist Stephen Wolfram. He's the iconoclastic London-born genius who won a PhD from California Institute of Technology in just one year, at age 20. Mathematica 1.0 was officially launched on Thursday, June 23, 1988.

Mathematica is renowned as the world's ultimate application for computations. But it's much more, it's the only development platform fully integrating computation into complete workflows for modelling the simulation, visualization, development, documentation and appointments.

Using unique hybrid symbolic numeric computation, Mathematica delivers results of method reliability imprecision, it solves problems other tools cannot. With Mathematica people can get results faster, thanks to thousands of highly optimized algorithms. Mathematica also can connects to all existing applications and databases, allowing us to build a new or existing work and infrastructures effortless deliver our content in applications cross-platform using innovate technologies, like computable document format. Twenty-five years of building on bold design principles make Mathematica the world's ultimate computation platform.

Mathematica is redefining the field of graph visualization, significantly raising the quality and efficiency of automatic graph layout, and allowing immediate graph visualization to become a mainstream part of the everyday computational workflow.

Built into Mathematica is a large collection of original and state-of-the-art graph layout algorithms developed through a collaboration between algorithm developers and graphic designers at Wolfram Research. Given particular data, Mathematica automatically selects the best algorithms to use, and by being able to draw on Mathematica vast web of geometric, numeric, graph theoretic, visualization and rendering capabilities, it is able to achieve a very high level of efficiency, routinely handling graphs with even millions of nodes.

4.2.1 Algorithm Construction

In the beginning, we turn back to the construction of the associated digraphs with quadratic polynomials in $\mathbb{Z}_n[x]$. The maping $\varphi : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \times \mathbb{Z}_n$, which is defined by $\varphi((a, b)) = (a + b, ab)$, presents digraph with edges and vertices $(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n$. The cycles are defined as in 3.1. Every component starts with irreducible vertex and ends with a cycle.

Remark. The vertex (a, b) is represented in Mathematica in this form {a, b}. The algorithm is mainly divided into several parts; to achieve it, we need first to create the ring $\mathbb{Z}_n$. That is,

```
L1 = Table[i, i, 0, n - 1]
```

where n is input value. The addition and multiplication on this ring is defined in this way:

```
Mod[a[[1]] + a[[2]], n], Mod[a[[1]] * a[[2]], n]
```

Now, we can see the main parts of the algorithm

- Create the set of vertices $\mathbb{Z}_n \times \mathbb{Z}_n$

  ```
  A = CartesianProduct[L1, L1]
  ```

- Define the mapping φ by

  ```
  f[a] := Mod[a[[1]] + a[[2]], n], Mod[a[[1]]*a[[2]], n]
  ```

- The first part of the excution, that we create the paths, where the mapping φ maps the first vertex in A then its image consecutively untill the image of one vertex is already included in the path. Afterwords, new component is being started. The vertices, which are mapped by φ, are immediatly removed from A. Indeed, some of these paths are subcomponents in $G(\mathbb{Z}_n)$.

  ```
  i = 1;
  While[l > 0,
  b_i = A[[1]];
  Z = DeleteCases[A, A[[1]]];
  A = Z;
  l = Length[A];
  If[l == 0, Break[]];
  If[Cases[A, f[b_i[[1]]]]==f[b_i[[1]]],
  v=1;
  While[Cases[A, f[b_i[[v]]]]==f[b_i[[v]]],
  AppendTo[b_i, f[b_i[[v]]]] ;
  Z = DeleteCases[A, f[b_i[[v]]]];
  A = Z;
  l = Length[A];
  v++ ]];
  i++]
  ```

- Now, All we need paths which contain cycles, so we have to omit the others. This step represents us the number of components.

```
t=0;
d=0;
While[t < i,
t++;
If[Cases[$b_t$, f[Last[$b_t$]]] == {f[Last[$b_t$]]},
d++;
$x_d$ = $b_t$]]
```

- To determine the cycles and their number, we have to cut the vertices which are not included in any cycle, and then to measure thier length. That leads us to our request.

```
k=0;
While[k < d,
k++;
While[f[Last[$x_k$]] $\neq$ f[First[$x_k$]],
$y_k$ = DeleteCases[$x_k$, First[$x_k$]];
$x_k$=$y_k$]]
```

- The longest cycles are the cycles which have the largest length, measuring all the cycles, then keeping the longest ones is shown in the following command.

```
h = 0;
While[h < k,
h++;
$j_h$ = Length[$x_h$]];
q=1;
p=0;
m={1};
While[q < k,
q++;
m=Append[m, $j_q$]];
While[p < k,
p++;
s=Max[m]];
u= Position[m, s];
r = Length[u];
e = 0;
```

While[e < r, e++; Print[$\mathtt{x}_{u[[e,1]]}$]]

- The output data $\mathtt{x}_{u[[e,1]]}$ refers to the form of the longest cycles, `d` refers to the number of components, `s` refers to the length of longest cycles, and `r` refers to the number of longest cycles.

Example 4.2.1. *The following is an excution of the algorithm for five randome values.*

```
n=3
{{0,0}}
{{1,0}}
{{2,0}}
3
1
3
n=11
{{1,9},{10,9},{8,2},{10,5},{4,6},{10,2}}
12
6
1
n=19
{{18,15},{14,4},{18,18},{17,1},{18,17},{16,2},{18,13},{12,6}}
20
8
1
n=55
{{54,53},{52,2},{54,49},{48,6},{54,13},{12,42},{54,9},{8,46},{54,38},{37,17},
{54,24},{23,31}}
{{4,28},{32,2},{34,9},{43,31},{19,13},{32,27},{4,39},{43,46},{34,53},{32,42},
{19,24},{43,16}}
73
12
2
n=100
{{11,30},{41,30},{71,30},{1,30},{31,30},{61,30},{91,30},{21,30},{51,30},{81,30}}
{{1,10},{11,10},{21,10},{31,10},{41,10},{51,10},{61,10},{71,10},{81,10},{91,10}}
{{51,70},{21,70},{91,70},{61,70},{31,70},{1,70},{71,70},{41,70},{11,70},{81,70}}
{{21,90},{11,90},{1,90},{91,90},{81,90},{71,90},{61,90},{51,90},{41,90},{31,90}}
271
```

10

4

Next, we are proposing another part of the algorithm to calculate the longest path in the graph. This part is seperated in order to avoid having stored values in the memory during the first excution, which generate huge erors. Furthermore, this seperation shortens the run-time to get fast results.

The idea of this algorithm is to pick up the irreducible vertices, because they correspond to the start of any component, then to map those vertices. That can be shown in the following.

- Create the A and define the mapping φ.

```
L1 = Table[i, i, 0, n - 1];
A = CartesianProduct[L1, L1];
l = Length[A];
f[a] := Mod[a[[1]] + a[[2]], n], Mod[a[[1]]*a[[2]], n];
```

- Determine the vertices which are reducible, then remove them from A.

```
A1 = Table[f[A[[t]]], t, 1, l];
c = Union[A1];
A1 = c;
m = Length[A1];
t = 0;
While[t < m,
t++;
Z = DeleteCases[A, A1[[t]]];
A = Z];
```

- Now, start mapping the rest of vertices in A to get the full paths.

```
i = 1;
While[l > 0,
b_i = A[[1]];
Z = DeleteCases[A, A[[1]]];
A = Z;
l = Length[A];
v = 1;
While[Cases[b_i, f[b_i[[v]]]] ≠ f[b_i[[v]]],
AppendTo[b_i, f[b_i[[v]]]] ;
v++ ];
If[l == 0, Break[]]; i++];
```

- To get the longest paths we need to the length of every path we get, then to omit the shorter ones.

```
l = Length[A];
h = 0;
While[h < i,
h++;
j_h = Length[b_h]];
q = 1;
p = 0;
m = 1;
While[q < i,
q++;
m = Append[m, j_q]];
While[p < i,
p++;
s = Max[m]];
u = Position[m, s];
r = Length[u];
e = 0;
While[e < r,
e++; Print[b_u[[e,1]]]];
Print[s]
```

- The output data Print[$b_u[[e,1]]$] refers to the form of the longest paths, Print[s] refers to thier length, and Print[s] refers to thier number.

Example 4.2.2. *The longest path in the digraph $G(\mathbb{Z}_7)$ is shown as below.*
$\{\{2,6\},\{8,1\},\{9,8\},\{6,6\},\{1,3\},\{4,3\},\{7,1\},\{8,7\},\{4,1\},\{5,4\},\{9,9\},\{7,4\},\{0,6\},$
$\{6,0\}\}$
$\{\{6,2\},\{8,1\},\{9,8\},\{6,6\},\{1,3\},\{4,3\},\{7,1\},\{8,7\},\{4,1\},\{5,4\},\{9,9\},\{7,4\},\{0,6\},$
$\{6,0\}\}$
14
2

Remark. In this example we have two longest paths in one component.
We go forward to view another algorithm, where two input values are involved. In this case alittle changes is needed in the beginning such as;

```
L1 = Table[i, i, 0, n_1 - 1];
L2 = Table[i, i, 0, n_2 - 1];
A1 = CartesianProduct[L1, L2];
A = CartesianProduct[A1, A1];
f[a] := {{Mod[a[[1, 1]] + a[[2, 1]], n_1], Mod[a[[1, 2]] + a[[2, 2]],
n_2]},
{Mod[a[[1, 1]]*a[[2, 1]], n_1], Mod[a[[1, 2]]*a[[2, 2]], n_2]}};
```

The symboles n_1 and n_2 are input data, and the rest of the algorithm is similar to the first algorithm.

Example 4.2.3. *Consider the values* n_1*=5,* n_2*=11. Then the longest cycles in the graph is,*

```
{{{4,10},{3,9}},{{2,8},{2,2}},{{4,10},{4,5}},{{3,4},{1,6}},{{4,10},{3,2}},
{{2,1},{2,9}},{{4,10},{4,9}},{{3,8},{1,2}},{{4,10},{3,5}},{{2,4},{2,6}},
{{4,10},{4,2}},{{3,1},{1,9}}}
{{{4,1},{3,9}},{{2,10},{2,9}},{{4,8},{4,2}},{{3,10},{1,5}},{{4,4},{3,6}},
{{2,10},{2,2}},{{4,1},{4,9}},{{3,10},{1,9}},{{4,8},{3,2}},{{2,10},{2,5}},
{{4,4},{4,6}},{{3,10},{1,2}}}
73
12
2
```

The algorithm, which calculates the longest path in this case, is quite similar to the previous one. That is:

```
L1 = Table[i, i, 0, n_1 - 1];
L2 = Table[i, i, 0, n_2 - 1];
A1 = CartesianProduct[L1, L2];
A = CartesianProduct[A1, A1];
l = Length[A];
f[a] := {{Mod[a[[1, 1]] + a[[2, 1]], n_1], Mod[a[[1, 2]] + a[[2, 2]],
n_2]},
{Mod[a[[1, 1]]*a[[2, 1]], n_1], Mod[a[[1, 2]]*a[[2, 2]], n_2]}};
A2 = Table[f[A[[t]]], t, 1, l];
```

```
c = Union[A2];
A2 = c;
m = Length[A2];
t = 0;
While[t < m,
t++;
Z = DeleteCases[A, A2[[t]]];
A = Z];
```

Example 4.2.4. *The following is the longest path in the graph* $G(\mathbb{Z}_2 \times \mathbb{Z}_3)$.
$\{\{\{0,2\},\{0,2\}\},\{\{0,1\},\{0,1\}\},\{\{0,2\},\{0,1\}\},\{\{0,0\},\{0,2\}\},\{\{0,2\},\{0,0\}\}\}$
$\{\{\{0,2\},\{1,2\}\},\{\{1,1\},\{0,1\}\},\{\{1,2\},\{0,1\}\},\{\{1,0\},\{0,2\}\},\{\{1,2\},\{0,0\}\}\}$
$\{\{\{1,2\},\{0,2\}\},\{\{1,1\},\{0,1\}\},\{\{1,2\},\{0,1\}\},\{\{1,0\},\{0,2\}\},\{\{1,2\},\{0,0\}\}\}$
$\{\{\{1,2\},\{1,2\}\},\{\{0,1\},\{1,1\}\},\{\{1,2\},\{0,1\}\},\{\{1,0\},\{0,2\}\},\{\{1,2\},\{0,0\}\}\}$
5
4

4.3 Introduction to Matlab

MATLAB is a numerical computing environment and fourth-generation programming language. The name MATLAB stands for MATrix LABoratory, because its basic data element is a matrix (array), MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C + +, Java, and Fortran.

Three men, J. H. Wilkinson, George Forsythe, and John Todd, played important roles in the origins of MATLAB. Our account begins more than 50 years ago. Cleve Moler, the chairman of the computer science department at the University of New Mexico, started developing MATLAB in the late 1970s. It soon spread to other universities and found a strong audience within the applied mathematics community. Jack Little, an engineer, was exposed to it during a visit Moler made to Stanford University in 1983. Recognizing its commercial potential, he joined with Moler and Steve Bangert. They rewrote MATLAB in C and founded MathWorks in 1984 to continue its development. These rewritten libraries were known as JACKPAC. In 2000, MATLAB was rewritten to use a newer set of libraries for matrix manipulation, LAPACK.

MATLAB was first adopted by researchers and practitioners in control engineering, Little's specialty, but quickly spread to many other domains. It is now also used in education, in particular the teaching of linear algebra and numerical analysis, and is popular amongst scientists involved in image processing. MATLAB can be used for math computations, modeling and simulations, data analysis and processing, visualization and graphics, and algorithm development. The standard MATLAB program has tools (functions) that can be used to solve common problems. In addition, MATLAB has optional toolboxes that are a collection of specialized programs designed to solve specific types of problems. Examples include toolboxes for signal processing, symbolic calculations, and control systems.

4.3.1 Algorithm Construction

In Matlab the ordered pairs is represented as matrices of type 1 × 2. i.e, the pair (a, b) has the form $[a, b]$. A different way has been done to construct this algorithm, where we obligated to sperate the algorithm into several M-files. The main M-file calls the rest in order make the excution. That is done as next.
The first step is to creat the Cartesian product of A. Note that the notation S is used instead of A in this algorithm

```
function A=cartesianprod(n)
D=zeros([n*n 2]);
t=0;
for i=0:n-1
for j=0:n-1
t=t+1;
D(t, [1 2])=[i j];
end
end
A=D;
```

Next, we have to define the mapping φ by

```
function [f]=myfunc(A,n)
s=A(1,1);
r=A(1,2);
f=[mod(s+r,n),mod(s.*r,n)];
end
```

Similarly, we create paths by mapping the first vertex in A, then remove it from A. A new path is chosen when the image of a vertex is not found in A(it means that the vertex is already mapped).

```
function [R]=prepaths(n)
A2=cartesianprod(n);
S=A2;
r=0;
q=0;
m=n*n;
while q<m
r=r+1;
Sn=myfunc(S(1,[1 2]),n);
T(1,[2*r-1 2*r])=S(1,[1 2]);
S=checkpair(S,T(1,[2*r-1 2*r]));
v1=size(S);
v=v1(1,1);
if v==1
q=m;
end
a=checkloop(S,Sn);
if a==0
T(2,[2*r-1 2*r])=Sn;
S=checkpair(S,T(2,[2*r-1 2*r]));
v1=size(S);
v=v1(1,1);
if v==1
q=m;
end
t=1;
b=0;
while b<m
t=t+1;
Snj=myfunc(Sn,n);
a=checkloop(S,Snj);
if a==1
b=m;
T(t+1,[2*r-1 2*r])=Snj;
```

```
end
if a==0
Sn=Snj;
T(t+1,[2*r-1 2*r])=Snj;
S=checkpair(S,T(t+1,[2*r-1 2*r]));
v1=size(S);
v=v1(1,1);
end
if v==1
q=m;
end
end
end
end
r1=r+1;
T(1,[2*r1-1 2*r1])=S(1,[1 2]);
R=T;
end
```

Two M-files are needed in this file for execution. The first one removes the pair which is chosen to be in R from S.

```
function [S]=checkpair(S1,T)
m=size(S1);
n=m(1,1);
if T==S1(1,[1 2])
S2=S1(2:n,:);
end
if T==S1(n,[1 2])
S2=S1(1:n-1,:);
end
for i=2:n-1
if T==S1(i,[1 2])
k=i;
S2=S1([1:k-1 k+1:n],:);
end
end
S=S2;
```

```
end
```

The second one tests whether the element in R(The matrix which include all paths) or not.

```
function [w]=checkloop(S,T)
c=size(S);
a=c(1,1);
B=zeros(1,a);
for j=1:a
if T==S(j,[1 2]);
k=j;
B(1,k)=1;
end end
w=isequal(B,zeros(1,a)); end
```

Here is the main algorithm, which presents the required output data.

```
function [L1,N]=graphloop(n)
[R]=longestloop(n);
c=size(R);
n1=c(1,2);
F1(1,[1 2])=[1 0];
for j=2:n1/2
M=longcolumn(R(:,[2*j-1 2*j]));
M1=checkpath(M);
g1=size(M1);
g2=g1(1,1);
F1(j,[1 2])=[j g2];
end
m=max(F1(:,2));
F3=checkrow(F1);
a1=size(F3);
a=a1(1,1);
N=a;
F4=F3(:,1);
L1=F3(1,2)-1;
for i=1:a
```

```
j=F4(i,1);
M=longcolumn(R(:,[2*j-1 2*j]));
M1=checkpath(M)
end
```

During the calculation, some entries were ignored, so that [00] occupied these entries(property in matlab). THis led us to creat the following file.

```
function [V]=longcolumn(S)
c=size(S);
m=c(1,1);
b=0;
while b<m
if S(m-b,1)+S(m-b,2)==0
b=b+1;
S=S(1:m-b,:);
else b=m;
end
end
V=S;
end
```

Another M-file is requested in the main algorithm. This file is responsible for collecting the cycles which are included in R.

```
function [L]=checkpath(S)
c=size(S);
m=c(1,1);
k=0;
for i=1:m-1
if S(m,[1 2])==S(m-i,[1 2])
k=m-i;
end
end
if k==0
L=[0 0];
else L=S(k:m,[1 2]);
end
```

```
end
```

The Last M-file in this algoritm keeps the longest path(cycle) and check whether other paths(cycles) have the same length.

Example 4.3.1. *>> [L1,N]=graphloop(11)*

```
M1 =
  1   9
 10   9
  8   2
 10   5
  4   6
 10   2
  1   9

L1 = 6
N = 1
```

The following diagram describes the construction of the whole algorithm in Matlab and the way how it works.

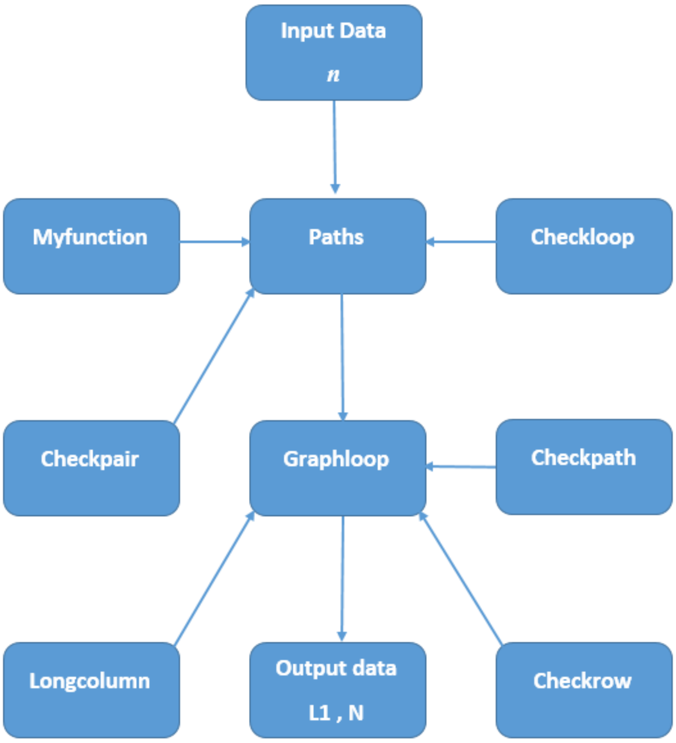

Figure 4.1: Diagram of Algorithm

Chapter 5

Computer Calculations

In the present chapter, we are going to present the calculations of digraphs associated with the quadratic polynomials with coefficients in R. Some notations are used, such as c_n (number of components), l_c (length of the longest cycle), $N.l_c$ (number of lengest cycles), and p_n (the longest path).

5.1 Digraphs Associated with Quadratic Polynomials in $\mathbb{Z}_n[x]$

Since R is finite, it has integer characteristic $char R \in \mathbb{N}$. If n is not a prime, then R has zero-divisors and $R[x]$ is not a unique factorization ring. If $n = p$ is prime, then A nevertheless could have zero-divisors. However, if R is a (finite) domain, then it must be a field. One can see some interesting results in Tables 5.1 and 5.2, where the the associated digraphs of the ring $\mathbb{Z}_n$ for $1 \leq n \leq 200$ are considered, such as:

1. For any prime number p, if $G(\mathbb{Z}_p)$ has cycles of length greater than 1, then the longest is unique. However, the opposite is not neccessary true. For instance, the digraph $G(\mathbb{Z}_{172})$ has a unique longest cycle of length 22, while 172 is not prime.
2. With respect to the prime numbers, the cycles in digraphs $G(\mathbb{Z}_2)$, $G(\mathbb{Z}_3)$, and $G(\mathbb{Z}_7)$ are all cycles of length 1. Furthermore, the digraph $G(\mathbb{Z}_{pq})$ has p longest cycles, in which $q \neq p = 2, 3, 7$.
3. The longest paths in $G(\mathbb{Z}_{p_1^{n_1}})$, $G(\mathbb{Z}_{p_2^{n_2}})$, ..., and $G(\mathbb{Z}_{p_k^{n_k}})$ are not divisors of the longest paths in $G(\mathbb{Z}_n)$, $n = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$.
4. The relation between paths and number of components are inverse relationship. i.e, longer paths appear in the digraphs with lower components and vice versa.

Table 5.1: Table of Results for $1 \leq n \leq 100$

n	c_n	l_c.	N. l_c	p_n	n	c_n	l_c.	N. l_c	p_n
1	1	1	1	1	51	57	10	3	18
2	2	1	2	3	52	71	4	6	22
3	3	1	3	5	53	56	14	1	67
4	5	2	1	4	54	126	9	6	11
5	6	4	1	6	55	73	12	2	18
6	6	1	6	5	56	84	4	14	12
7	7	1	7	9	57	60	8	3	34
8	12	4	2	6	58	64	14	2	35
9	14	3	2	6	59	65	17	1	130
10	12	4	2	6	60	93	4	18	8
11	12	6	1	14	61	64	17	1	92
12	15	2	3	6	62	64	18	2	44
13	14	4	1	22	63	98	3	14	11
14	14	1	14	9	64	176	32	16	34
15	18	4	3	8	65	87	4	22	22
16	30	8	4	10	66	72	6	6	14
17	19	10	1	18	67	71	39	1	103
18	28	3	4	6	68	97	10	6	18
19	20	8	1	34	69	72	10	3	32
20	31	4	6	6	70	84	4	14	12
21	21	1	21	9	71	74	10	1	96
22	24	6	2	14	72	180	12	4	14
23	24	10	1	32	73	76	30	1	153
24	36	4	6	8	74	78	24	2	49
25	50	5	4	12	75	150	5	12	12
26	28	4	2	22	76	101	8	6	34
27	63	9	3	10	77	84	6	7	14
28	35	2	7	10	78	84	4	6	22
29	32	14	1	35	79	81	28	1	96
30	36	4	6	8	80	206	8	36	12
31	32	18	1	44	81	252	27	9	28
32	72	16	8	18	82	90	22	2	63
33	36	6	3	14	83	85	12	1	144
34	28	10	2	18	84	105	2	21	10
35	42	4	7	12	85	118	20	2	24
36	73	6	2	8	86	96	11	2	98
37	39	24	1	49	87	96	14	3	35
38	40	8	2	34	88	148	12	4	18
39	42	4	3	22	89	95	51	1	149
40	80	4	30	8	90	174	12	4	14
41	45	22	1	63	91	98	4	7	22
42	42	1	42	9	92	121	10	6	32
43	48	11	1	98	93	96	18	3	44
44	61	6	6	15	94	100	12	2	60
45	87	12	2	14	95	123	8	9	34
46	48	10	2	32	96	216	16	24	20
47	50	12	1	60	97	102	23	1	139
48	90	8	12	12	98	236	7	12	10
49	118	7	6	10	99	175	6	21	16
50	100	5	8	12	100	271	10	4	14

Table 5.2: Table of Results for $101 \leq n \leq 200$

n	c_n	$l_c.$	$N.l_c$	p_n	n	c_n	$l_c.$	$N.l_c$	p_n
101	104	10	1	127	151	155	30	1	221
102	114	10	6	18	152	248	8	20	34
103	106	22	1	135	153	272	30	2	34
104	176	4	46	22	154	168	6	14	14
105	126	4	21	12	155	193	36	2	62
106	112	14	2	67	156	213	4	18	22
107	109	13	1	155	157	160	63	1	178
108	333	18	3	20	158	162	28	2	96
109	113	30	1	157	159	168	14	3	67
110	146	12	4	18	160	520	16	72	20
111	117	24	3	49	161	168	10	7	32
112	210	8	28	16	162	504	27	18	29
113	116	8	1	200	163	169	34	1	206
114	120	8	6	34	164	229	22	6	64
115	145	20	2	42	165	219	12	6	18
116	163	14	6	35	166	170	12	2	144
117	199	12	2	30	167	170	56	1	290
118	130	17	2	130	168	252	4	42	12
119	133	10	7	18	169	552	208	3	226
120	240	4	90	8	170	236	20	4	24
121	343	30	24	36	171	283	24	2	50
122	128	17	2	92	172	243	22	1	98
123	135	22	3	63	173	180	50	1	219
124	161	18	6	44	174	192	14	6	35
125	406	25	20	29	175	350	5	28	13
126	196	3	28	11	176	374	24	8	30
127	132	79	1	205	177	195	17	3	130
128	416	64	32	66	178	190	51	2	149
129	144	11	3	98	179	184	20	1	241
130	174	4	44	22	180	467	12	12	14
131	132	18	1	168	181	185	22	1	203
132	183	6	18	15	182	196	4	14	22
133	140	8	7	34	183	192	17	3	92
134	142	39	2	103	184	292	20	4	42
135	396	36	3	38	185	240	24	9	49
136	240	20	4	24	186	192	18	6	44
137	144	26	1	106	187	230	30	2	36
138	144	10	6	32	188	253	12	6	61
139	142	9	1	219	189	441	9	21	17
140	217	4	42	12	190	246	8	18	34
141	150	12	3	60	191	196	21	1	305
142	148	10	2	96	192	528	32	48	36
143	169	12	2	30	193	198	151	1	303
144	462	24	8	26	194	204	23	2	139
145	197	28	2	49	195	261	4	66	22
146	152	30	2	153	196	625	14	6	16
147	354	7	18	11	197	205	33	1	285
148	197	24	6	49	198	350	6	42	16
149	155	22	1	197	199	202	40	1	275
150	300	5	24	12	200	728	20	8	24

5.2 Digraphs Associated with Quadratic Polynomials in $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}[x]$

The ring of integers modulo n is a field if and only if n is a prime number. Otherwise, it is not even a domain. However, the direct product of the rings R_i, for i some index set I has zero divisors. For instance, in the ring $\mathbb{Z}_p \times \mathbb{Z}_q$, the elements $(1,0)$ and $(0,1)$ satisfy that $(1,0).(0,1) = 0$. That means $\mathbb{Z}_p \times \mathbb{Z}_q$ can't be domain, so that can't be field.

Similar observations can be seen in the Table 5.4 and 5.3 such as;

1. In the case, when $n_1 = n_2$; the construction of the digraphs $G(\mathbb{Z}_{n_1 n_2})$ and $G(\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2})$ is completley different.
2. In the construction of the digraphs $G(\mathbb{Z}_{pq})$ and $G(\mathbb{Z}_p \times \mathbb{Z}_q)$, we have that both have the same number of component, number of longest cycles, length of longest cycle, and length of longest path, which has been partly proved in chapter 3.
3. In the digraph $G(\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2})$, where n_1 is prime and $n_2 = 2, 3, 7$; the number of components $c_{n_1 n_2} = c_{n_1} \times c_{n_2}$; the longest cycle $l_{n_1 n_2} = l_{n_1}$; the number of cycles N.$l_{n_1 n_2} = n_2$ the length of the longest path $p_{n_1 n_2} = p_{n_1}$.

TABLE 5.3: Table of Results for $1 \leq n \leq 20$

n	c_n	l_c.	$N.l_c$	p_n
1	1	1	1	1
2	4	1	4	3
3	9	1	9	5
4	26	2	10	4
5	39	4	14	8
6	36	1	36	5
7	49	1	49	9
8	168	4	64	8
9	213	6	12	10
10	156	4	56	8
11	149	6	28	19
12	234	2	90	6
13	199	4	30	22
14	196	1	196	9
15	351	4	126	8
16	1232	8	448	10
17	375	20	4	34
18	852	6	48	10
19	704	8	46	34
20	1154	4	504	8

Table 5.4: Table of Results for $1 \leq n_1, n_2 \leq 20$

n_1	n_2	c_n	$l_c.$	$N.l_c$	p_n	n_1	n_2	c_n	$l_c.$	$N.l_c$	p_n
2	3	6	1	6	5	4	13	71	4	6	22
2	4	10	2	2	4	4	14	70	2	14	9
2	5	12	4	2	6	4	15	93	4	18	8
2	6	12	1	12	5	4	16	164	8	24	10
2	7	14	1	14	9	4	17	97	10	6	18
2	8	24	4	4	6	4	18	146	6	4	6
2	9	28	3	4	6	4	19	101	8	6	34
2	10	24	4	4	6	4	20	166	4	36	6
2	11	24	6	2	14	5	6	36	4	6	8
2	12	30	2	6	6	5	7	42	4	7	12
2	13	28	4	2	22	5	8	80	4	30	8
2	14	28	1	28	9	5	9	87	12	2	14
2	15	36	4	6	8	5	10	78	4	28	8
2	16	60	8	8	10	5	11	73	12	2	18
2	17	38	10	2	18	5	12	93	4	18	8
2	18	56	3	8	6	5	13	87	4	22	22
2	19	40	8	2	34	5	14	84	4	14	12
2	20	62	4	12	6	5	15	117	4	42	8
3	4	15	2	3	6	5	16	206	8	36	12
3	5	18	4	3	8	5	17	118	20	2	24
3	6	18	1	18	5	5	18	174	12	4	14
3	7	21	1	21	9	5	19	132	8	9	34
3	8	36	4	6	8	5	20	209	4	84	8
3	9	42	3	6	7	6	7	42	1	42	9
3	10	36	4	6	8	6	8	72	4	12	8
3	11	36	6	3	14	6	9	84	3	12	7
3	12	45	2	9	6	6	10	72	4	12	8
3	13	42	4	3	22	6	11	72	6	6	14
3	14	42	1	42	9	6	12	90	2	18	6
3	15	54	4	9	8	6	13	84	4	6	22
3	16	90	8	12	12	6	14	84	1	84	9
3	17	57	10	3	18	6	15	108	4	18	8
3	18	84	3	12	7	6	16	180	8	24	12
3	19	60	8	3	34	6	17	114	10	6	18
3	20	93	4	18	8	6	18	168	3	24	7
4	5	31	4	6	6	6	19	120	8	6	34
4	6	30	2	6	6	6	20	186	4	36	8
4	7	35	2	7	10	7	8	84	4	14	12
4	8	64	4	12	6	7	9	98	3	14	11
4	9	73	6	2	8	7	10	84	4	14	12
4	10	62	4	12	6	7	11	84	6	7	14
4	11	61	6	6	15	7	12	105	2	21	10
4	12	78	2	30	6	7	13	98	4	7	22

n_1	n_2	c_n	l_c.	$N.l_c$	p_n	n_1	n_2	c_n	l_c.	$N.l_c$	p_n
7	14	98	1	98	9	11	15	219	12	6	18
7	15	126	4	21	12	11	16	374	24	8	30
7	16	210	8	28	16	11	17	230	30	2	36
7	17	133	10	7	18	11	18	350	6	42	16
7	18	196	3	28	11	11	19	241	24	2	50
7	19	140	8	7	34	11	20	383	12	12	18
7	20	217	4	42	12	12	13	213	4	18	22
8	9	180	12	4	14	12	14	210	2	42	10
8	10	160	4	60	8	12	15	279	4	54	8
8	11	148	12	4	18	12	16	492	8	72	12
8	12	192	4	36	8	12	17	291	10	18	18
8	13	176	4	46	22	12	18	438	6	12	10
8	14	168	4	28	12	12	19	303	8	18	34
8	15	240	4	90	8	12	20	498	4	108	8
8	16	440	8	80	10	13	14	196	4	14	22
8	17	240	20	4	24	13	15	261	4	66	22
8	18	360	12	8	14	13	16	446	8	68	26
8	19	248	8	20	34	13	17	270	20	2	38
8	20	440	4	180	8	13	18	398	12	4	30
9	10	174	12	4	14	13	19	283	8	17	34
9	11	175	6	21	16	13	20	457	4	132	22
9	12	219	6	6	10	14	15	252	4	42	12
9	13	199	12	2	30	14	16	420	8	56	16
9	14	196	3	28	11	14	17	266	10	14	18
9	15	261	12	6	16	14	18	392	3	56	11
9	16	462	24	8	26	14	19	280	8	14	34
9	17	272	30	2	34	14	20	434	4	84	12
9	18	426	6	24	10	15	16	618	8	108	12
9	19	283	24	2	50	15	17	354	20	6	24
9	20	467	12	12	14	15	18	522	12	12	16
10	11	146	12	4	18	15	19	369	8	27	34
10	12	186	4	36	8	15	20	627	4	252	8
10	13	174	4	44	22	16	17	610	40	8	34
10	14	168	4	28	12	16	18	924	24	16	66
10	15	234	4	84	8	16	19	642	8	148	34
10	16	412	8	72	12	16	20	1156	8	216	12
10	17	236	20	4	24	17	18	544	30	4	34
10	18	348	12	8	14	17	19	384	40	2	66
10	19	246	8	18	34	17	20	623	20	12	24
10	20	418	4	168	8	18	19	566	24	4	50
11	12	183	6	18	15	18	20	934	12	24	14
11	13	169	12	2	30	19	20	643	8	54	34
11	14	168	6	14	14	20	20	-	-	-	

Chapter 6

Discussion

The main part of this thesis concentrates on a relation between digraphs and finite commutative rings, which is presented as coeffitients of the rings of quadratic polynomial. In doing so, we provided theorems, lemmas and corollaries which aimed to support the understanding of the construction and the main idea of this association. Moreover, Another reason to study this idea of directed graphs resulted from the study of *Unitary Cayley Graph* (e.g [1]). We discussed some graphical terminologies such as vertex degree, triangles, ... etc. starting with special cases then general.

This kind of connections is studied and detialed in chapter 3, That is summarized in constructing a mapping $\varphi : A^2 \to A^2$ by $(a, b) \longmapsto (a + b, ab)$, where A represents the coeffitients of the quadratic polynomial $x^2 - ax + b$ modulo n. The vertices are the elements $(a, b) \in A^2$ and the edges are defined by the mapping φ. Intuitively, this mapping reflects the ring structure of A.

This idea is studied and proposed by Aleksandar Lipkovski (e.g [15]), then it is improved and presented in some conferences(e.g [16]) and in the joint work with O. Shafah and A. Lipkovski (e.g [18]). In this thesis, it is presented with more detials.

A computer calculations is used to see the behaviour(cycles) of this digraph by creating an algorithm in Mathematica and Matlab softwares to calculate the number of components(the paths and the cycles). This algorithm represents the number of components, the number of cycles(the shortest and the longest ones), and the longest paths.

The calculations show us some intersting results, like the cycles in digraph $G(\mathbb{Z}_n)$ are determened by the cycles in the the digraphs of its prime factories. One might notice correspondence to the fundamental theorem of arithmetic. In addition, the digraphs of $\mathbb{Z}_{p^m}$ for some $m > 0$, is not isomorphic to the digraph $G(\mathbb{Z}_p \times .... \times \mathbb{Z}_p)(m\ times)$.

At the moment there is no answer how the cycles in $G(\mathbb{Z}_{p^m})$ are determened. A different construction of cycles are apperead in the table of results for different primes. For instance, when $n = 5$, 5-cycle is the longest cycle in $G(\mathbb{Z}_{25})$. At the same time, 4-cycle is the longest cycle in $G(\mathbb{Z}_5)$. When $n = 11$, 30-cycle is the longest cycle in $G(\mathbb{Z}_{121})$. At the same time, 6-cycle is the longest cycle in $G(\mathbb{Z}_{11})$. So in this work this is an open problem one can work on.

Bibliography

[1] R. Akhtar, M. Boggess, T. Jackson-Henderson, I. Jimenez, R. Karpman, A. Kinzel, D. Pritikin. On the unitary cayley graph of a finite ring. *Electronic Journal of Combinatorics*, 16:R117, 2009.

[2] Linda Gilbert, Jimmie Gilbert. *Elements of Modern Algebra.* Brooks/Cole, Cengage Learning., 2009.

[3] David S. Dummit, Richard M. Foote. *Abstract Algebra.* John Wiley and Sons, Inc., 2004.

[4] Hamza Daoub. The fundamental theorem on symmetric polynomials. *The Teaching of Mathematics.*, (1):55–59, 2012.

[5] G.Chartrand. *Graphs and Digraphs.* Chapman and Hall/CRC, 1996.

[6] Richard A. Brualdi, Dragos Cvetkovic. *A Combinatorial Approach to Matrix Theory and Its Applications.* Taylor and Francis Group, LLC, 2009.

[7] Pavol Hell*, Xuding Zhu. Homomorphisms to oriented paths. *Discrete Mathematics*, 132:107–114, 1994.

[8] J. Ball, D. Welsh. *Graphs and Homomorphisms.* Oxford University Press, New York, 2004.

[9] Pavol Hell, Huishan Zhou, Xuding Zhu. Homomorphisms to oriented cycles. *Combinatorica*, 13:421–433, 1993.

[10] Megan Boggess, Tiffany Jackson-Henderson, Isidora Jimenez, Rachel Karpman. *The Structure of Unitary Cayley Graphs.* http://www.units.muohio.edu/sumsri/sumj/2008/CayleyGraphs.pdf., 15.06.2013 (20:23pm).

[11] Paul Erdös , Anthony B. Evans. Representations of graphs and orthogonal latin square graphs. *J. Graph Theory*, 13:593–595, 1989.

[12] Anthony B. Evans, G. Fricke, C. Maneri. Representations of graphs modulo n. *J. Graph Theory*, 8:801–815, 1994.

[13] Walter Klotz, Torsten Sander. Some properties of unitary cayley graphs. *Electronic Journal of Combinatorics*, 14:Research Paper 45, 2007.

[14] Douglas B. West. *Introduction to Graph Theory.* Pearson Education, Inc., 2001.

[15] Aleksandar T. Lipkovski. Digraphs associated with finite rings. *Publications De L'institut Mathematique.*, 92(106):35–41, 2012.

[16] A. Lipkovski, O. Shafah, H. Daoub. Vychislenie grafov konechnyh kolec. international conference. Technical Report Report 177, August 2011.

[17] Henri Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag Berlin Heidelberg., 1993.

[18] H. Daoub, O. Shafah, A. Lipkovski. An association between digraphs and rings. *Filomat Jurnal, preprinted.*

Prilog 1.

Izjava o autorstvu

Potpisani Hamza Elhadi Daoub
broj indeksa 2009/2002

Izjavljujem

da je doktorska disertacija pod naslovom

”Finite Rings and Digraphs: Further development of Theory and Algorithms”

- rezultat sopstvenog istraživačkog rada,
- da predložena disertacija u celini ni u delovima nije bila predložena za dobijanje bilo koje diplome prema studijskim programima drugih visokoškolskih ustanova,
- da su rezultati korektno navedeni i
- da nisam kršio autorska prava i koristio intelektualnu svojinu drugih lica.

Potpis doktoranda

U Beogradu, ________________

____

Prilog 2.

Izjava o istovetnosti štampane i elektronske verzije doktorskog rada

Ime i prezime autora: *Hamza Elhadi Daoub*
Broj indeksa: 2002/2009
Studijski program: ________________________
Naslov rada: *"Finite Rings and Digraphs: Further development of Theory and Algorithms"*
Mentor: *redovni prof. dr. Aleksandar Lipkovski*

Potpisani *Hamza Elhadi Daoub*

Izjavljujem da je štampana verzija mog doktorskog rada istovetna elektronskoj verziji koju sam predao za objavljivanje na portalu **Digitalnog repozitorijuma Univerziteta u Beogradu**.

Dozvoljavam da se objave moji lični podaci vezani za dobijanje akademskog zvanja doktora nauka, kao što su ime i prezime, godina i mesto rodjenja i datum odbrane rada.

Ovi lični podaci mogu se objaviti na mrežnim stranicama digitalne biblioteke, u elektronskom katalogu i u publikacijama Univerziteta u Beogradu.

Potpis doktoranda

U Beogradu, ____________

____

Prilog 3.

Izjava o korišćenju

Ovlašćujem Univerzitetsku biblioteku ”Svetozar Marković” da u Digitalni repozitorijum Univerziteta u Beogradu unese moju doktorsku disertaciju pod naslovom:

”Finite Rings and Digraphs: Further development of Theory and Algorithms”

koja je moje autorsko delo.

Disertaciju sa svim prilozima predao sam u elektronskom formatu pogodnom za trajno arhiviranje.

Moju doktorsku disertaciju pohranjenu u Digitalni repozitorijum Univerziteta u Beogradu mogu da koriste svi koji poštuju odredbe sadržane u odabranom tipu licence Kreativne zajednice (Creative Commons) za koju sam se odlučio.

1. Autorstvo
2. [✓ Autorstvo - nekomercijalno]
3. Autorstvo - nekomercijalno - bez prerade
4. Autorstvo - nekomercijalno - deliti pod istim uslovima
5. Autorstvo - bez prerade
6. Autorstvo - deliti pod istim uslovima

(Molimo da zaokružite samo jednu od šest ponudjenih licenci, kratak opis licenci dat je na poledjini lista).

Potpis doktoranda

U Beogradu, ________________

____

1. Autorstvo - Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način odredjen od strane autora ili davaoca licence, čak i u komercijalne svrhe. Ovo je najslobodnija od svih licenci.

2. Autorstvo - nekomercijalno. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način odredjen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela.

3. Autorstvo - nekomercijalno - bez prerade. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način odredjen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela. U odnosu na sve ostale licence, ovom licencom se ograničava najveći obim prava korišćenja dela.

4. Autorstvo - nekomercijalno - deliti pod istim uslovima. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način odredjen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca ne dozvoljava komercijalnu upotrebu dela i prerada.

5. Autorstvo - bez prerade. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način odredjen od strane autora ili davaoca licence. Ova licenca dozvoljava komercijalnu upotrebu dela.

6. Autorstvo - deliti pod istim uslovima. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način odredjen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca dozvoljava komercijalnu upotrebu dela i prerada. Slična je softverskim licencama, odnosno licencama otvorenog koda.