Bounds on the Diameter of Some Families of Linear Congruential Graphs

Rogelio Pabros

A Thesis
in
The Department
of
Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements
for the Degree of Master of Science in Mathematics at
Concordia University
Montreal, Quebec, Canada

August 1995

ISBN 0-612-10884-8

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the thesis prepared

By: Rogelio Pabros

Entitled: Bounds on the Diameter of Some Families of Linear Congruential Graphs

and submitted in partial fulfillment of the requirements for the degree of

Master of Science in Mathematics

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

______________________________ Chair

______________________________ External Examiner

______________________________ Examiner 2

______________________________ Examiner 3

______________________________ Thesis Supervisor

Approved by ______________________________

Chair of Department or Graduate Program Director

______________ 19 ______ ______________________________

Dean of Faculty

Abstract

Bounds on the Diameter of Some Families of Linear Congruential Graphs

Rogelio Pabros

A *linear congruential graph* (LCG) on n vertices, denoted by $G(F, n)$ where F is a set of linear functions, is a graph whose vertex set is $\{0, 1, \ldots, (n-1)\}$ in which two vertices x and y are adjacent if $y \equiv f(x) \bmod n$ for some f in F. This family of graphs is known to generalize the de Bruijn graph and to contain large graphs with diameter smaller than those of known graphs with the same degree and order. However, no explicit bounds on the diameter of these graphs have been known.

If the functions in F have the same multiplier, then we call the graph *uniform-multiplier LCG*, or UM-LCG. The case when $n = 2^p$ and the functions have an odd multiplier $\neq 1$ is studied. For $|F| = 2$, a classification according to connectivity is given and an upper bound of order $O(\log n)$ on the diameter is obtained.

We then consider the case of $|F| = 2$ when the functions do not have the same multiplier. When the functions are noncommutative modulo n, again we obtain an upper bound of order $O(\log n)$ on the diameter of some of the graphs. When the functions are commutative modulo n, we obtain a lower bound on the diameter which, on the contrary, is of order $O(\sqrt{n})$.

Acknowledgment

It is a great honor to have worked with Dr. J. Opatrny on this thesis. I would like to thank him for giving me the right motivations from Day One to do the research, for guiding me with all the right directions to achieve our goals, for being patient with me in our long discussions, for being a source of encouragement as results came out one by one, for being supportive of the decisions I made regarding the organization of the paper, and for being instrumental in acquiring partial financial support from NSERC and from an FCAR team grant. Most of all I appreciate the opportunity of learning from him a variety of things that range from computer knowledge to scientific research writing.

I would like to thank C. Cayouette for telling me invaluable words of wisdom at times when I didn't make sense of what I was doing and at times when I did, for understanding the hardships I was going through while I was doing the thesis, for wholeheartedly lending me a hand whenever I needed it, for helping me shape up when I was down and out, and for telling me to be proud of the accomplishments I have in life. I really appreciate all that.

I would like to thank my family for giving me the inspiration to go on with my studies, for understanding why I couldn't write to them as often as I should until I finished the thesis, and for being loving and proud of me as ever.

To Carlos and Proceso,
my late grandfathers

To Dan and Rose,
my parents

Contents

List of Figures

List of Tables

Chapter 1

PRELIMINARIES

1.1 Introduction and Motivation

A *distributed computer system* is made up of processing elements (or processors) that communicate with each other by means of physical links. A typical example is a local area network that consists of several computing stations placed at short distances and exchanging data information at very high speeds [2]. These distributed systems have many properties that can be studied using graph models. In particular, each processing element can be represented by a vertex of a graph and each direct link between two of these elements by an edge of the same graph. Hence, in the design and implementation of distributed computer systems, the study of interconnection networks in graph theoretical setting is an indispensable tool.

To develop realistic and feasible network models of these systems, a lot of consideration is given to the switching mechanism used between a processor and a link, the transmission delay between any two processors, and the reliability and fault tolerance of the whole system. The switching mechanism should be relatively easy to install, and since there can be thousands of switches to be used in the system, it is desirable to use a uniform type, e.g. one that can attach a fixed number of cables to a processing element. Correspondingly, the graph model should be regular. When one processing element communicates with another in the system, the closer they are, i.e. the less number of intermediary processing elements between them, the faster the information is exchanged. Thus to minimize the transmission delay, the distance between any two elements should be small. This means that the graph used to model the interconnection network should have a small diameter. Distributed systems should function even if there is an accidental failure of some of its elements. For example, in case of a breakdown of a number of processors, the whole system should be able to continue its task. To realize this, the graph representing the interconnection network should be highly connected.

Because of this relation between computer systems and graph theory, the problem that has been the subject of several scientific papers is to find a large graph to be used as an effective interconnection model with the desired properties, particularly small diameter, regularity and high connectivity. Hypercubes and de Bruijn graphs, for example, have been shown to have interesting properties, such as low diameter, high connectivity, and recursive structure. The Moore bound, which gives the minimum diameter that a graph of a given order and degree can have, has never been achieved for large graphs, although a random regular graph has been shown to have a lower bound on its diameter which is fairly close to the Moore bound [8].

Recently, a new family of graphs called *linear congruential graphs*, or *LCG* for short, was proposed in [21]. It has been shown in [21] that it contains large graphs of low diameter. A subfamily of LCG called *disjoint consecutive cycles* [22], abbreviated to *DCC-LCG*, contains networks that are k-regular (for any positive integer k), larger than other graph constructions of the same degree and diameter, of maximum connectivity for even degrees, and have a recursive property reminiscent of hypercubes. However, the results concerning the diameter were obtained by calculating it for specific graphs, and the question of a general bound on the diameter of these graphs was left open. Using the Moore bound [8] for graphs with $n = 2^p$ vertices and degree 4, the diameter of LCG is greater than or equal to $\log_3 2^p - 1/2$. Observing the results in [21] and [22], it is reasonable to conjecture that the diameter of the LCG in general, and of the UM-LCG in particular, has a logarithmic bound.

The main contribution of this thesis is the study on the bounds on the diameter of some subfamilies of LCG. We define a subfamily of LCG called *uniform-multiplier LCG*, or *UM-LCG* for short. We study some of the properties of graphs in this subfamily and give an upper bound on their diameter which is of order $O(\log n)$, where $n = 2^p$ is the order of the graph. We also give upper and lower bounds on the diameter of other graphs in the LCG family, and generalize the recursive property of the LCG.

For the rest of this chapter we will review some graph theoretic terms, give the formal definitions and examples of *LCG* and *UM-LCG*, and cite some graph network constructions related to UM-LCG's. Chapter 2 deals with the classification of UM-LCG's with 2 generators and order 2^p according to connectivity. Chapter 3 introduces some operations on the vertices of UM-LCG's. Chapter 4 uses the results in the preceding two chapters to obtain our main results. And lastly, Chapter 5 discusses the general cases of LCG's with 2 generators. When the generators are noncommutative, the results of Chapter 4 are used to obtain the diameter upper bound of some graphs. When the generators are commutative, the diameter lower bound is obtained. The generalization of the recursive property of LCG is also given.

1.2 A Review of Definitions from Graph Theory

Using the definitions and terminologies of [7], we define a **graph** G to be an ordered triple $(V(G), E(G), \psi_G)$ that consists of a nonempty set $V(G)$ of **vertices**, a set $E(G)$, disjoint from $V(G)$, of **edges** and an **incidence function** ψ_G that associates with each edge of G an unordered pair of (not necessarily distinct) vertices of G.

If e is an edge and u and v are vertices such that $\psi_G(e) = uv$, then e is said to **join** u and v, and the vertices u and v are called the **ends** of e. Moreover, we say that the ends of an edge are **incident** with the edge, and vice versa. An edge with identical ends is called a **loop** and an edge with distinct ends is called a **link**. A graph is **simple** if it has no loops and no two of its links join the same pair of vertices.

A graph H is a **subgraph** of G, written $H \subseteq G$ if $V(H) \subseteq V(G)$, $E(H) \subseteq V(G)$ and ψ_H is the restriction of ψ_G to $E(H)$. If H is a subgraph of G such that $V(H) \subset$

$V(G)$ or $E(H) \subset E(G)$, we write $H \subset G$.

The **degree** $d(v)$ of a vertex v in a graph is the number of edges of the graph incident with v, each loop counting as two edges. A graph G is **k-regular** if $d(v) = k$ for all $v \in V(G)$. If for some k a graph is k-regular, then it is a **regular graph.**

For any positive integer k, a **walk** of length k in a graph G is a finite non-null sequence $W = v_0e_1v_1e_2v_2 \cdots e_kv_k$ whose terms are alternately vertices and edges such that for $1 \leq i \leq k$ the ends of e_i are v_{i-1} and v_i. We say that W is a (v_0, v_k)**-walk** traversing $v_0, e_1, v_1, \ldots, e_k, v_k$ and we call v_0 and v_k the **origin** and **terminus** of W, respectively. If the edges $e_1, e_2, \cdots, e_k$ are distinct, then W is called a **trail.** If, in addition, the vertices $v_0, v_1, \cdots, v_k$ are distinct, W is called a **path.** The walk W is **closed** if its origin and terminus are the same. If W is a closed trail such that $v_0, v_1, \ldots, v_{k-1}$ are distinct, then W is called a **cycle** of length k.

In this paper we will use the term **path** a little bit loosely in the sense that we will allow it to mean a **walk.** In this regard we define a **cycle** to be a closed path. Two other notations that we will use for a (v_0, v_k)-path are $(v_0, v_1, \ldots, v_k)$ and $v_0 \longrightarrow v_1 \longrightarrow \cdots \longrightarrow v_k$.

A **Hamilton path** of G is a path that contains every vertex of G, and a **Hamilton cycle** of G is a cycle that contains every vertex of G. If the graph G contains a Hamilton cycle, then it is said to be **hamiltonian.**

Two vertices u and v of G are said to be **connected** if there is a (u, v)-path in G. The vertex set $V(G)$ can be partitioned into nonempty subsets $V_1(G), V_2(G), \ldots, V_n(G)$ such that two vertices u and v are connected if and only if both v and v belong to the same set $V_i(G)$. The subgraphs whose vertex sets are $V_1(G), V_2(G), \ldots, V_n(G)$ are called **components** of G. If $n = 1$, then G is said to be **connected.**

If vertices u and v are connected in a graph G, the **distance** between u and v in G, denoted by $d_G(u, v)$ or simply by $d(u, v)$, is the length of a shortest (u, v)-path in G. If there is no path connecting u and v, we define $d(u, v)$ to be infinite. The **diameter** of G, denoted by **Diam(G),** is the maximum distance between any two vertices of G.

1.3 Definition of *LCG* and *UM-LCG*

We now give the formal definition of the two families of graphs studied in this thesis.

Definition 1.3.1 [21] *Let N denote the set of nonnegative integers. Let n be a positive integer and $F = \{f_i(x) = a_i x + c_i : 1 \leq i \leq t$, and $a_i, c_i \in N\}$ be a set of linear functions. A* **linear congruential graph** $G(F,n)$ **on** n **vertices** *is the graph whose vertex set is $V = \{0, 1, \ldots, (n-1)\}$ in which each vertex x is adjacent to $f_i(x) \bmod n$ for every i. The functions in F are called the* **generators** *of $G(F,n)$ and in turn $G(F,n)$ is said to be* **generated by** *the functions in F.*

We abbreviate the word *linear congruential graph* by *LCG*. Using the terminologies of Knuth [18], if $f(x) = ax + b$ is a generator of an LCG, we call a the **multiplier** and b the **constant** of the function f.

Definition 1.3.2 *A* **uniform-multiplier LCG on** n **vertices**, *or* **UM-LCG** *for short, is an LCG on n vertices whose generators have the same multiplier.*

Figures 1.1 and 1.2 give us the diagrams for the graphs $G_1 = G(\{x+19, 7x+1\}, 30)$ and $G_2 = G(\{5x+3, 5x+11\}, 32)$. We also see that $G(\{x+19\}, 30) \subset G_1$ is a Hamilton cycle and that $G(\{7x+1\}, 30) \subset G_1$ is not connected. On the other hand both $G(\{5x+3\}, 32)$ and $(\{5x+11\}, 32)$ are Hamilton cycles of G_2. Moreover, the generators $f_1(x) = 5x+3$ and $f_2(x) = 5x+11$ commute with each other, i.e. $f_1 f_2(x) \equiv f_2 f_1(x) \equiv 25x + 26 \bmod 32$, which may not be true if the order of G is $n > 32$. Both graphs G_1 and G_2 are said to be *cyclically symmetric* because we can move each figure in a cyclical (clockwise or counterclockwise) fashion, with a turn of less than 360 degrees, and come up with one identical to the original. For example, G_2 can be turned such that vertex 0 assumes the position of vertex 3 which assumes the position of vertex 18, etc., and the resulting graph is G_2 itself.

For suitable multipliers and constants, LCG's are shown in [22] to be regular and of degree $2t$. Although LCG's that are of odd degree can also be defined, we will not consider them in this paper.

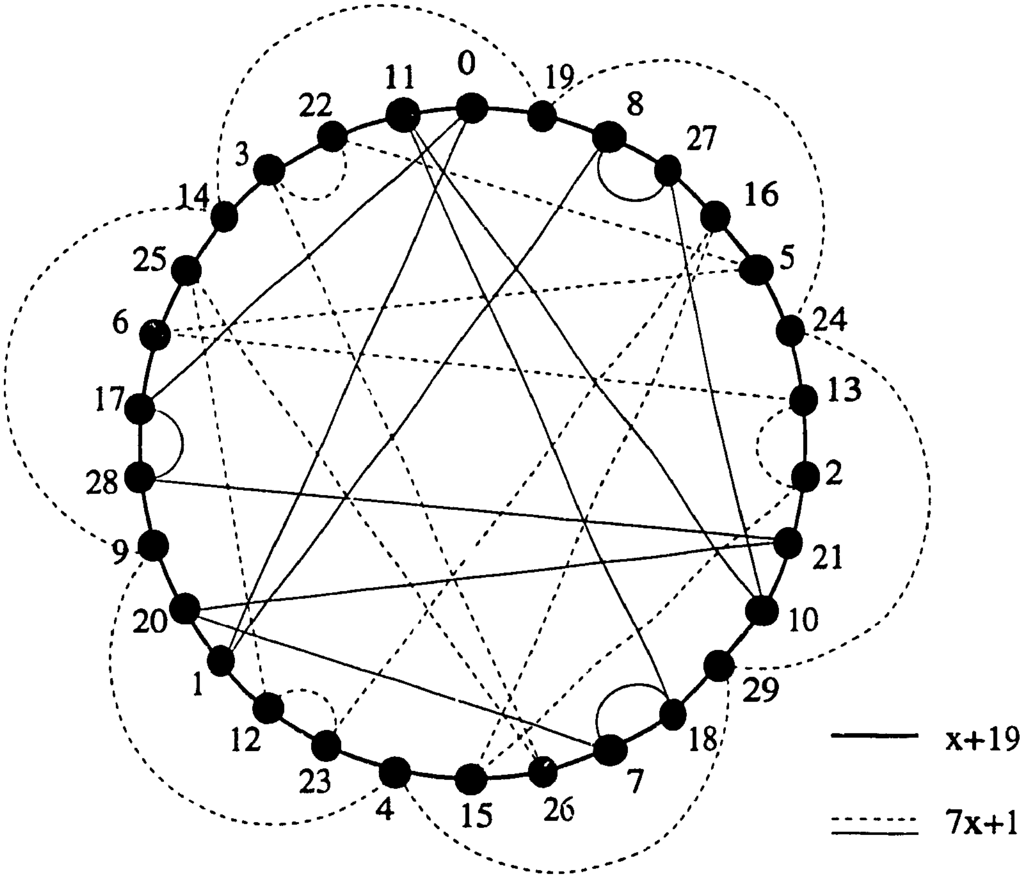


Figure 1.1: $G_1 = G(\{x+19, 7x+1\}, 30)$

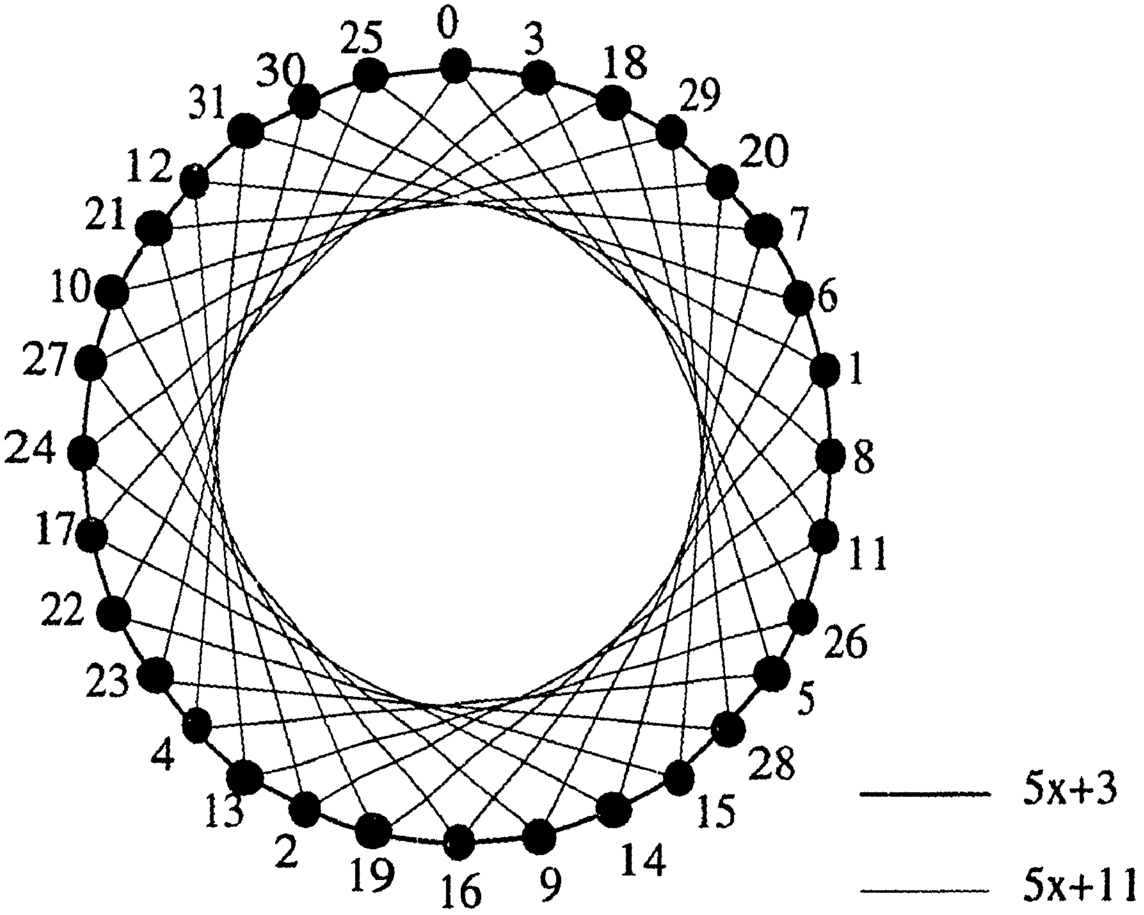


Figure 1.2: $G_2 = G(\{5x + 3, 5x + 11\}, 32)$

In particular, our study is mainly on UM-LCG's with 2 generators on $n = 2^p$ vertices where p is any positive integer. This is a good start in the study of this family of graphs because a UM-LCG with 2 generators is always contained in a UM-LCG with more than 2 generators, and in general, the results on 2^p vertices may be extended to m^p vertices, where m is a prime number, which in turn may be extended to $m_1^{p_1} m_2^{p_2} \cdots m_k^{p_k}$ vertices, where $m_1, m_2, \ldots, m_k$ are prime and $p_1, p_2, \ldots, p_k$ are positive integers.

1.4 Related Constructions

UM-LCG's are an interesting class of LCG graphs. Some of them are not entirely new subjects of research and have been studied extensively, with some in slightly different context. In this section we will cite some of the network constructions closely related to UM-LCG's. But first let us review the definition of a *directed* graph.

As in [7] we define a **directed graph** D as an ordered triple $(V(D), A(D), \psi_D)$ consisting of a nonempty set $V(D)$ of **vertices**, a set $A(D)$, disjoint from $V(D)$, of **arcs**, and an **incidence function** ψ_D that associates with each arc of D an ordered pair of (not necessarily distinct) vertices of D. If a is an arc and u and v are vertices such that $\psi_D(a) = (u, v)$, then a is said to **join** u to v. We abbreviate 'directed graph' to **digraph**.

We can have a *directed* version of an LCG by replacing each of its edges by an arc in the following manner: if uv is an edge such that $v \equiv f(u) \bmod n$, where $f(x) = ax + b$ is a generator of the LCG, then it is replaced by the arc (u, v). We shall call the resulting digraph LCD. We can conversely say that an LCG is an *undirected* version of an LCD.

1.4.1 Loop networks and circulant graphs

Loop networks are graph networks with at least one Hamilton cycle [2]. We observe that some LCG's are loop networks because apart from those with hamiltonian cycles

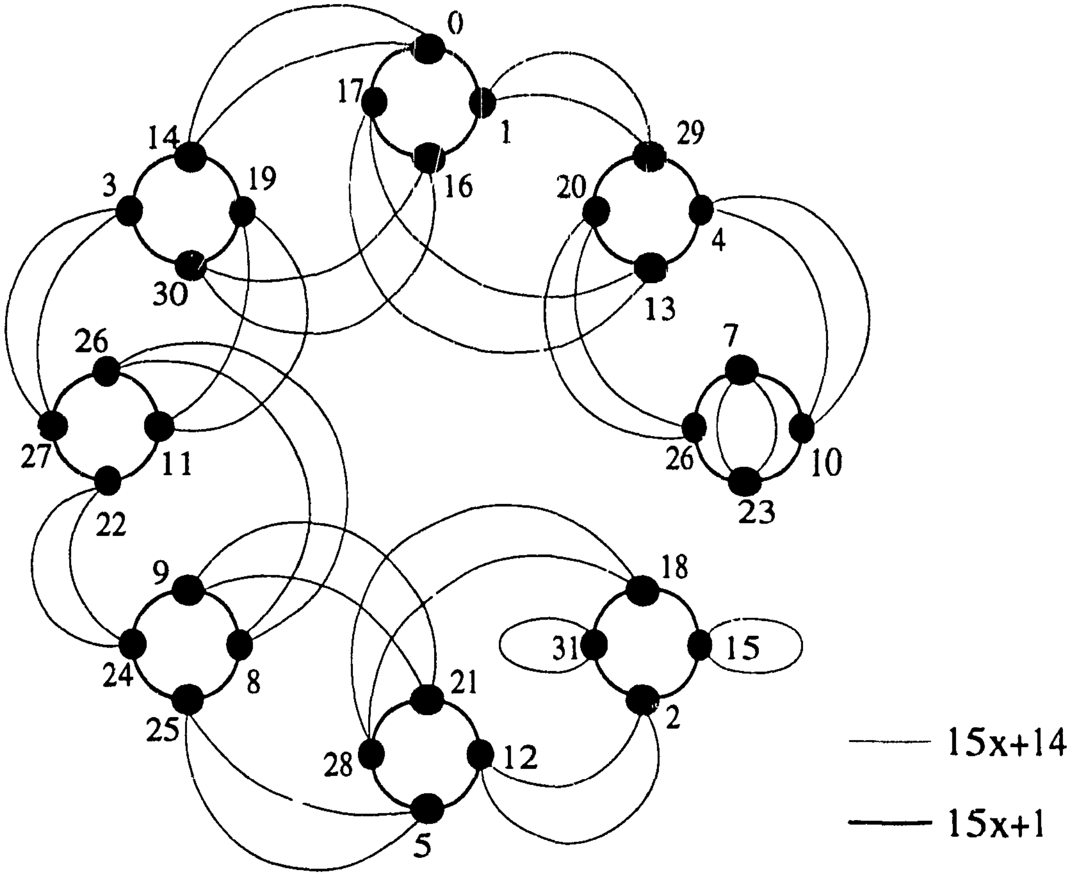


Figure 1.3: $G(\{15x+1, 15x+14\}, 32)$

there are connected LCG's without hamiltonian cycles. An example is the UM-LCG on 32 vertices with generators $f_1(x) = 15x + 1$ and $f_2(x) = 15x + 14$ whose diagram appears in Figure 1.3. The **multiple fixed step digraph** denoted by $G(n; s_1, s_2, \ldots, s_k)$, is a digraph on n vertices 0, 1, ..., $(n-1)$ where vertex x is adjacent to k other vertices $x + s_1, x + s_2, \ldots, x + s_k \bmod n$. The undirected version of this digraph, denoted by $G(n; \pm s_1, \pm s_2, \ldots, \pm s_k)$, is called **multiple fixed step graph**, also known as **circulant graph** (see [5]). We see that these are identical to the UM-LCD and the UM-LCG, respectively, on n vertices with generators $f_i(x) = x + s_i$, $i = 1, 2, \ldots, k$, where the uniform multiplier is 1.

The UM-LCG $G(\{x+1\}, n)$, also known as **distributed double loop computer network** [19, 27, 28] has a diameter of $\lfloor n/2 \rfloor$. The UM-LCD $G(\{x+1, x-2\}, n)$,

generators	order	diameter
$x+1, x+3t$	$3t^2+t$	$3t-1$
$x+1, x-3t$	$3t^2+2t$	$3t-1$
$x+1, x+3t+1$	$3t^2+2t+1$	$3t$
$x+1, x+3t+2$	$3t^2+3t+1$	$3t$
$x+1, x-3t-2$	$3t^2+4t+1$	$3t$
$x+1, x+3t+3$	$3t^2+4t+2$	$3t+1$
$x+1, x+3t+4$	$3t^2+5t+2$	$3t+1$
$x+1, x-3t+4$	$3t^2+6t+2$	$3t+1$

Table 1.1: Diameters of some LCD's

also known as **daisy chain loop**, has diameter $\lfloor n/3 \rfloor + 1$ (see [12]). The diameter of UM-LCD $G(\{x+1, x+\sqrt{n}\}, n)$ is approximately $2\sqrt{n}$ (see [29, 24, 23, 25]). In fact, the diameter is exactly $2\sqrt{n}-2$ (see [29]). Some UM-LCD's given by Fiol *et al* [10] and cited by Bermond *et al* [2] are listed on Table 1.1. The diameter upper bound for the UM-LCD $G(\{x+1, x+s\}, n)$ has been found by Hwang and Xu [16]. For any s and for $n \geq 6348$, the diameter of this graph is less than $\sqrt{3n} + 2\sqrt[4]{3n} + \lfloor 3\sqrt{n-1}/\sqrt{n} \rfloor - 3\lfloor \sqrt{n}/3 \rfloor$. Erdös and Hsu [9] proved that for any $\varepsilon > 0$ there exists $n_0(\varepsilon)$ such that if $n > n_0(\varepsilon)$ then there exists a number s such that $Diam(G(\{x+1, x+s\}, n)) < (1+\varepsilon)\sqrt{3n}$.

In the case of the UM-LCG $G(\{x+s_1, x+s_2\}, n)$, the minimum diameter over s_1 and s_2 is found to have been greater than or equal to $\lceil(\sqrt{2n-1}-1)/2\rceil$ (see [3, 6, 29, 30]). This lower bound can be achieved by taking $s_1 = \lceil(\sqrt{2n-1}-1)/2\rceil$ and $s_2 = s_1 + 1$ (see [6, 3, 1]). Another interesting and important result is in [3, 30], that $Diam(G(\{x+s_1, x+s_2\}, 2t^2+2t+1)) = t$ if and only if $s_1 \equiv tp \bmod n$ and $s_2 \equiv (t+1)p \bmod n$ where $p < n$ and $\gcd(p, n) = 1$. For the more difficult problem of solving $\min_s Diam(G(\{x+1, x+s\}, n))$, Hsu and Shapiro [14] showed that an upper bound is given by $\sqrt{n/2} + \sqrt[4]{n/8} + 2$.

We observe in the preceding examples that the diameter upper bound for a UM-LCG with multiplier $a = 1$ is in the order $O(\sqrt{n}) + O(\sqrt[4]{n})$. In contrast, we will show later that for many UM-LCG's with multiplier $a \neq 1$ and with order $n = 2^r$ the diameter upper bound is in the order of $O(\log_a n)$.

1.4.2 The k-ary de Bruijn graph and related networks

The **r-dimensional k-ary de Bruijn graph**, or $DBG(r,k)$ for short, is a $2k$-regular graph with k^r vertices, each of which corresponds to an r-digit number $x_1x_2\cdots x_r$ with $0 \leq x_1, x_2, \ldots, x_r \leq (k-1)$ (see [19, 13]). The vertex $x_1x_2\cdots x_r$ is adjacent to $yx_1x_2\cdots x_{r-1}$ and to $x_2x_3\cdots x_rz$, where $0 \leq y, z \leq (k-1)$. If each edge $(x_1x_2\cdots x_r, x_2x_3\cdots x_rz)$ is changed into an arc, then we have the **k-ary de Bruijn digraph**, abbreviated $DBD(r,k)$, where each vertex has indegree and outdegree equal to k.

We observe in the $DBD(r,k)$ that two vertices $x_1x_2\cdots x_r$ and $y_1y_2\cdots y_r$ are connected by a path

$$x_1x_2\cdots x_r \rightarrow x_2\cdots x_ry_1 \longrightarrow x_3\cdots x_ry_1y_2 \longrightarrow \ldots \longrightarrow x_ry_1y_2\cdots y_{r-1} \rightarrow y_1y_2\cdots y_r$$

which is of length r, and, in addition to this in $DBG(r,k)$, by a path

$$\begin{aligned} x_1x_2\cdots x_r &\rightarrow y_rx_1x_2\cdots x_{r-1} \rightarrow y_{r-1}y_rx_1\cdots x_{r-2} \rightarrow \ldots \longrightarrow y_2\cdots y_rx_1 \\ &\rightarrow y_1y_2\cdots y_r \end{aligned}$$

which is also of length r. Hence, both $DBG(r,k)$ and $DBD(r,k)$ have a diameter of $r = \log_k n$. This is the least possible for the case of a regular digraph with the same order, indegree and outdegree as the $DBD(r,k)$ [19].

The **generalized de Bruijn digraph** has been defined in many different ways. The definition of Reddy *et al* [26] and Imaseh and Itoh [17] fits that of a UM-LCD of order n with generators $f_i(x) = kx + i$, where $0 \leq i \leq (k-1)$. The digraph $DBD(r,k)$ is obtained when $n = k^r$, while the **generalized de Bruijn graph** is obtained if each arc is changed to an edge.

The **r-dimensional k-ary Kautz graph** is a subgraph of the $DBG(r,k)$. The main difference is that in each vertex $x_1x_2\cdots x_r$ no consecutive digits are the same [4]. There is a definition for the **generalized Kautz digraphs** proposed by Imaseh and Itoh [17] which can be presented as a UM-LCD on n vertices with generators $f_i(x) = -kx - i$, where $1 \leq i \leq k$. We obtain the **Kautz digraph** by setting $n = k^D + k^{D-1}$, for some D, in which case the diameter is D.

Both the generalized de Bruijn digraph and the generalized Kautz digraph have in- and outdegree equal to k and diameter at most $\lceil \log_k n \rceil$. We can define an undirected version of these digraphs by replacing each arc by an edge, each vertex having a degree equal to $2k$. The diameter of these undirected graphs is still of order $\log n$ (see [2]).

Chapter 2

CLASSIFICATION OF UM-LCG's

It is not surprising that some aspects of LCG's can be studied using the properties of linear congruential sequences and functions. So the first part of this chapter is a review of their definitions and properties. A natural extension of these properties is apparent on LCG's with one generator and are discussed in the second section. We extend these properties further in Section 2.3 to discuss the classification of UM-LCG's with two generators. We will give tables to summarize the results in Sections 2.2 and 2.3.

The scope of our study of UM-LCG's is restricted to those with order $n = 2^p$ and with a maximum of 2 generators.

2.1 Linear Congruential Sequences and Functions

Let N denote the set of natural numbers and let $n \in N$. If $a, b \in N$, we say that a **is congruent to b modulo** n, written $a \equiv b \bmod n$, if $n|(a-b)$. If $n \not| (a-b)$, we say that a and b are incongruent modulo n. A **complete system of residues** mod n is a set of integers such that every integer is congruent modulo n to exactly one integer from the set.

Let us denote by Z_n the ring of least nonnegative residues modulo n, which is precisely the set $\{0, 1, \ldots, n-1\}$ equipped with the operations of addition and multiplication modulo n. Z_n is a commutative group under addition modulo n, while the set $U_n = \{u \in Z_n \mid \gcd(u, n) = 1\}$ of units in Z_n is a commutative group under multiplication modulo n. We denote the additive inverse of $m \in Z_n$ by $-m$, while the multiplicative inverse of $u \in U_n$ by u^{-1}. In particular, if $n = 2^p$ then U_n consists of all the odd integers in Z_n.

A function $f(x) = ax + b \bmod n$ is called a **linear congruential function** on Z_n where $a \in N$ is the **multiplier** and $b \in N$ the **constant** of f. Given $x_0 \in Z_n$, this function produces a **linear congruential sequence** of integers $x_0, x_1, x_2, \ldots$ from Z_n, where $x_{i+1} \equiv ax_i + b \bmod n$. The number $x_0 \in N$ is called the **starting point** of the sequence which we denote by $\{ax_i + b \bmod n; x_0 \in Z_n\}$. We say that f **forms a sequence of period** k, where $1 \leq k \leq n$, if k is the least integer such that $x_{i+k} = x_i$ for some i. In particular, if $k = 1$, we say that f generates a **loop** at x_i.

We have the following proposition for an even multiplier of a linear congruential function.

PROPOSITION 2.1.1 *Let $n = 2^p$ and $a, b \in N$. If a is even, then*

(i) $f(x) = ax + b \bmod n$ forms exactly one loop, which is at $x \equiv (a-1)^{-1}(-b) \bmod n$.

(ii) $f(x) = ax + b \bmod n$ does not form a sequence of period greater than 1.

Proof. *(i)* If a is even, then $x \equiv f(x) = ax + b \bmod n \Leftrightarrow ax - x \equiv -b \bmod n \Leftrightarrow x(a-1) \equiv -b \bmod n \Leftrightarrow x \equiv (a-1)^{-1}(-b) \bmod n$.

(ii) Suppose f forms a sequence of period k, for some integer $k > 1$. Then $x \equiv f^k(x) = a^k x + b(a-1)^{-1}(a^k - 1) \bmod n$ has a solution. Solving for x, we have $(a^k - 1)x \equiv -b(a-1)^{-1}(a^k - 1) \bmod n \Leftrightarrow x \equiv -b(a-1)^{-1} \bmod n$ since $\gcd(n, a^k - 1) = 1$. But by *(i)* this is precisely the point where f forms a loop. Hence $k = 1$, a contradiction. □

The preceding proposition guarantees that if a is even then the sequence $\{ax_i + b \bmod n; x_0\}$ terminates into a loop at $x \equiv (a-1)^{-1}(-b) \bmod n$ for any starting point $x_0 \in Z_n$. To illustrate this, let us look at the following example.

Example 2.1.1 Let $n = 16, a = 6, b = 3$. We have $(a-1)^{-1}(-b) \equiv (13)(13) \equiv 169 \equiv 9 \bmod 16$. The elements of the sequence $\{6x_i + 3 \bmod 16; x_0\}$ are the following:

1. when $x_0 = 0$: $0, 3, 5, 1, 9, 9, 9, \ldots$

2. when $x_0 = 1$: $1, 9, 9, 9, \ldots$

3. when $x_0 = 2$: $2, 15, 13, 1, 9, 9, 9, \ldots$

The function $f(x) = 6x + 3 \bmod 16$ forms a loop at $x = 9$. ◇

If a is odd then it is of the form $a = 2^i k + 1$ or $a = 2^i k - 1$ for some $i \geq 2, k \in N$ where k is odd. In other words, $(a-1)$ is either divisible by 4 or divisible by 2 but not by 4. We will cite a theorem from [11] in order to prove the next proposition for an odd integer a.

THEOREM 2.1.1 [11] *The linear congruence* $ax \equiv b \bmod n$ *has a solution if and only if* $\gcd(a, n) | b$. *If there is a solution, then there are exactly* $s = \gcd(a, n)$ *incongruent solutions. In particular, if* $s = 1$, *then the congruence has a unique solution.*

This theorem tells us that for $n = 2^p$, a has inverse modulo n (which is unique up to modulo n) if and only if a is odd.

PROPOSITION 2.1.2 *Let* $f(x) = ax + b \bmod 2^p$ *and* $a, b \in N$ *such that* a *is odd. Let* $i, k \in N$ *with* $i \geq 2$ *and* k *odd. If* $a = 2^i k + 1$, *then*

(i) f *does not form a loop if and only if* $2^i \nmid b$.

(ii) f *forms* 2^i *distinct loops if and only if* $2^i | b$.

(iii) f *does not form a sequence of period* 2 *if and only if* $2^i \nmid b$.

(iv) f *forms at most* 2^{i+1} *distinct sequences of period* 2 *if and only if* $2^i | b$.

If $a = 2^i k - 1$, then

(v) f does not form a loop if and only if b is odd.

(vi) f forms 2 distinct loops if and only if b is even.

(vii) f does not form a sequence of period 2 if and only if b is odd.

(viii) f forms at most 2^{i+1} distinct sequences of period 2 if and only if b is even.

Proof. Let $n = 2^p$. The function f forms a loop if and only if $x \equiv ax + b \bmod n$ or $x(a-1) \equiv -b \bmod n$ has a solution. By Theorem 2.1.1, there is a solution if and only if $D = \gcd(a-1, n) | b$. If a is of the form $a = 2^i k + 1$, then $D = 2^i$. Hence, we have *(i)* and *(ii)*. If a is of the form $a = 2^i k - 1$, then $D = 2$. Hence, we have *(v)* and *(vi)*.

Consider the congruence $x \equiv f^2(x) = a(ax+b)+b \bmod n = a^2x + b(a+1) \bmod n$, or equivalently, $x(a^2-1) \equiv -b(a+1) \bmod n$. Let $D' = \gcd(a^2-1, n)$. If $a = 2^i k + 1$, then $D' = \gcd((a-1)(a+1), n) = \gcd(2^i k(2^i k + 2), n) = 2^{i+1}$. By Theorem 2.1.1, there are 2^{i+1} solutions if and only if 2^{i+1} divides $-b(a+1) = -2b(2^{i-1}k + 1)$, i.e. if and only if $2^i | b$. Hence we have *(iii)*. However, if y is a solution, it can also mean that $y \equiv f^k(y) \bmod n$ for all k. Hence we can only conclude assertion *(iv)*, that f forms at most 2^{i+1} distinct sequences of period 2. Similarly, if $a = 2^i k - 1$, then $D' = \gcd((a-1)(a+1), n) = \gcd(2(2^{i-1}k - 1)2^i k, n) = 2^{i+1}$ and $-b(a+1) = -2^i bk$. Hence, there is a solution to the congruence $x \equiv f^2(x) \bmod n$ if and only if $2^{i+1} | -2^i bk$, i.e. if and only if b is even. Thus we have *(vii)* and *(viii)*. □

To illustrate assertion *(iv)* of Proposition 2.1.2, we have:

Example 2.1.2 Suppose $a = 2^2(3) + 1 = 13$, $b = 8$, and $n = 16$. We have $\gcd(a^2 - 1, n) = \gcd(168, 16) = 8$ dividing $b(a+1) = 8(14)$. By Proposition 2.1.2, $f(x) = 13x + 8 \bmod 16$ forms at most 8 sequences of period 2. Indeed, the following are the sequences formed by f:

$(0, 8, 0, \ldots), (8, 0, 8, \ldots), (1, 5, 9, 13, 1, \ldots),$

$(2,2,\ldots),(3,15,11,7,3,\ldots),(4,12,4,\ldots),$
$(12,4,12,\ldots),(6,6,\ldots),(10,10,\ldots),$
$(14,14,\ldots).$

Only four of these sequences are of period 2. Four others are loops. ◇

The following is a special case of a theorem in [18] for $n = 2^p$. It gives the requirements for a linear congruential function modulo n to form a sequence of period n.

THEOREM 2.1.2 **[18]** *Let $n = 2^p$ with $2 \leq p \in N$. The linear congruential sequence formed by the function $f(x) = ax + b \bmod n$ has a period n if and only if*

(i) b is odd, and

(ii) $(a-1)$ is a multiple of 4, i.e. $a = 2^ik + 1$ for some $i \geq 2$ and positive odd integer k.

By this theorem we can always say that if a is odd and of the form $a = 2^ik - 1$, i.e. if $a - 1$ is divisible by 2 but not by 4, then $f(x) = ax + b \bmod n$ does not form a sequence of period n, hence it must form one of a lesser period. To illustrate this, we have the following examples.

Example 2.1.3 Since $5 = 2^2(1)+1$ and 3 is odd, the function $f(x) = 5x+3 \bmod 16$ forms a sequence of period 16. With starting point $x_0 = 0$, the elements are:

$$0,3,2,13,4,7,6,1,8,11,10,5,12,15,14,9,0,\ldots$$

◇

Example 2.1.4 Since $7 = 2^3(1)-1$, $f(x) = 7x+3 \bmod 16$ does not form a sequence of period 16. In fact, the sequences it forms are all of period 4. With starting point x_0, these sequences are:

1. when $x_0 = 0$: $0,3,8,11,0,\ldots$

2. when $x_0 = 1$: $1,10,9,2,1,\ldots$

3. when $x_0 = 4$: $4, 15, 12, 7, 4, \ldots$

4. when $x_0 = 5$: $5, 6, 13, 14, 5, \ldots$

◇

2.2 Linear Congruential Graphs with One Generator

By definition, a linear congruential graph $G(F, n)$ is generated by the elements of a set F of linear functions. If we take any $f \in F$, where $f(x) = ax + b$, and consider the subgraph $G = G(\{f\}, n)$ of $G(F, n)$, we see that there is a natural association between G and the linear congruential sequence $S = \{ax_i + b \bmod n; x_0 \in Z_n\}$ formed by f. In particular, for any starting point x_0, each element x_i of S corresponds to a vertex x_i of G, and each pair (x_i, x_{i+1}) of consecutive elements x_i and x_{i+1} of S corresponds to an edge $x_i x_{i+1}$ of G where $x_{i+1} \equiv f(x_i) \bmod n$. Conversely, each vertex x and each edge xy in G such that $y \equiv ax + b \bmod n$ correspond to an element and a pair of consecutive elements, respectively, of a linear congruential sequence S formed by f. In general, if $x_i, x_{i+1}, \ldots, x_{i+k}$ are consecutive elements of S, then there exists a corresponding path in G that traverses the vertices $x_i, x_{i+1}, \ldots, x_{i+k}$, in that order. In this regard, S itself corresponds to a walk in G. Hence, if S is a sequence of period k, it corresponds to a walk with a cycle of length k in G, e.g. a loop formed by f corresponds to a loop in G. Therefore, in studying LCG's with one generator, the properties of linear congruential sequences are an important tool.

The proposition and the last theorem in the preceding section were about linear congruential sequences. In this section we give their versions for LCG's with one generator.

PROPOSITION 2.2.1 *Let $G = G(\{ax + b\}, n)$ where $n = 2^p, a, b \in N$. If a is even, then*

(i) G has exactly one loop which is located at the vertex $x \equiv (a-1)^{-1}(-b) \bmod n$.

(ii) G contains no cycle of length ≥ 2.

Proof. *(i)* By Proposition 2.1.1 the linear congruential function $f(x) = ax + b \bmod n$ forms one and only one loop at $x \equiv (a-1)^{-1}(-b) \bmod n$. This loop, as a sequence $(x, x, \ldots)$, corresponds to a loop at the vertex of the same label in G.

(ii) By Proposition 2.1.1 there is no sequence formed by $f(x) = ax + b \bmod n$ that is of period greater than 1. Hence G contains no cycle of length 2. □

Recall that a simple graph is one that has no loop and no cycle of order 2. The preceding proposition tells us that if a is even then $G = G(\{ax+b\}, 2^r)$ is not simple because it contains a loop. However, it is connected because each sequence formed by $f(x) = ax + b \bmod n$ terminates into the loop. When a is odd, the following gives the requirements in order for G to be simple.

PROPOSITION 2.2.2 *Let $G = G(\{ax+b\}, 2^p)$ where a is an odd number and b is an integer. Let $i, k \in N$ such that $i \geq 2$ and k is odd.*

(i) If a is of the form $a = 2^i k + 1$: G is a simple graph if and only if b is odd or b is of the form $b = 2^j h$ for some $j, h \in N$ such that h is odd and $j < i$.

(ii) If a is of the form $a = 2^i k - 1$: G is a simple graph if and only if b is odd.

Proof. *(i)* By parts (i) and (iii) of Proposition 2.1.2, G does not have a loop and cycle of period 2 if and only if 2^i does not divide b. This leaves us with the two possibilities: b is odd, and b factors into $2^j h$, where $j < i$ and h is odd.

(ii) follows directly from parts (v) and (vii) of Proposition 2.1.2. □

The linear congruential graph $G(\{f\}, n)$ is connected if and only if every sequence formed by f has period n. Rephrasing Theorem 2.1.2, we have:

THEOREM 2.2.1 **[18]** *Let a be an odd integer. Then $G(\{ax+b\}, 2^p)$ is connected if and only if b is odd and $a = 2^i k + 1$, where $i, k \in N$ with $i \geq 2$, k odd.*

Thus far we have explored all the possibilities regarding the connectivity and simplicity of $G = G(\{ax+b\}, 2^p)$. If a is even, then G is connected but not simple.

	$G(\{ax+b\},n)$	
b	$a = 2^i k + 1$	$a = 2^i k - 1$
odd	Simple Connected	Simple Not Connected
even	$(b = 2^j h, j < i)$ Simple Not Connected	Not Simple Not Connected
	$(b = 2^j h, j \geq i)$ Not Simple Not Connected	

Table 2.1: Classification of $G(\{ax + b\}, n)$ according to simplicity and connectivity

If a is odd, we summarize the results in Table 2.1 where $n = 2^p$, $i \geq 2$, $j \in N$ and h, k are odd integers.

2.3 UM-LCG's with Two Generators

Let $f(x) = ax + b \bmod n$ be a linear congruential function on Z_n, where $n = 2^p$. If there exists a linear congruential function $g(x) = cx + d \bmod n$ on Z_n such that $f(g(x)) = g(f(x)) = x \bmod n$ for all $x \in Z_n$, then we say that f is **invertible** and that g is the **inverse function of f on Z_n**. We observe that if g is the inverse of f then f is the inverse of g on Z_n. We sometimes write the inverse of f as f^{-1}.

For g to be the inverse of f, we must have solutions for c and d in terms of a, b and n in the congruence $x \equiv f(g(x)) = acx + ad + b \bmod n$ that also satisfy the congruence $x \equiv g(f(x)) = acx + bc + d \bmod n$. These solutions exist if and only if a is a unit in Z_n, which is true if and only if a is odd. Therefore f is invertible if and only if a is odd, in which case we have $c \equiv a^{-1} \bmod n$ and $d \equiv -a^{-1}b \bmod n$. Since the values of c and d are unique up to modulo n, it is clear that the inverse g

of f is also unique up to modulo n. We observe that if g is the inverse of f on Z_n, then $G(\{f\}, n) = G(\{g\}, n)$. We shall say that two invertible functions f_1 and f_2 are **distinct modulo** n if $f_1 \not\equiv f_2 \bmod n$ and $f^{-1} \not\equiv f_2 \bmod n$.

We restrict our study of UM-LCG to thos whose generators are invertible and have a multiplier a not equal to 1. We will see in the next chapter the importance of the existence of the inverse of a generator in the calculation of the diameter bound. We will not cover the case when the multiplier is equal to 1 as there have already been studies made on the subject (See Bermond *et al* [2] for a survey).

In this section we will classify the two-generator UM-LCG according to its connectivity. The parity of the constants of the generators and whether a is of the form $2^ik + 1$ or $2^ik - 1$, where k is odd and $i \geq 2$, are the two most important factors to be considered in the classifications. Another factor that may also be important is the classification of the LCG generated by each of the generators, as shown in the following proposition.

PROPOSITION 2.3.1 *Let $G = G(\{f_1, f_2\}, n)$, $G_1 = G(\{f_1\}, n)$ and $G_2 = G(\{f_2\}, n)$ be LCG's where f_1 and f_2 are linear functions. Then G is connected if either G_1 or G_2 is connected.*

Proof. It is easy to see that $V(G) = V(G_1) = V(G_2)$ and $E(G) = E(G_1) \cup E(G_2)$. Hence, a path in G_1 or G_2 is also a path in G. This means that if vertices x and y are connected in G_1 or G_2 then they are connected in G. □

Remark 2.3.1 We observe that the above proposition is true in general for any $n \in N$. In particular, for $n = 2^p$, G is connected if at least one of the generators has an odd multiplier of the form $2^ik + 1$ and an odd constant.

When both G_1 and G_2 are not connected, it is possible that G is not connected, as shown in the following:

PROPOSITION 2.3.2 *Let $f_1 = ax + b$ and $f_2 = ax + c$ be distinct invertible linear functions on Z_{2^p} where a is odd, and b, c are even. Then $G = G(\{f_1, f_2\}, 2^p)$ is not connected.*

Proof. If $x_{odd}, x_{even} \in V(G)$ such that x_{odd} is odd and x_{even} is even, then $f_1(x_{even})$ and $f_2(x_{even})$ are even and $f_1(x_{odd})$ and $f_2(x_{odd})$ are odd. This means that G is made up of at least two components, one that is composed of vertices which are even and another one that is composed of vertices which are odd. In other words, there are no edges in G that are incident to a pair of vertices of different parity. Hence, G is not connected. □

If both G_1 and G_2 are not connected, it may still be possible for G to be connected, particularly when the multiplier is of the form $2^ik - 1$. For instance, as shown on Figure 2.1 $G(\{11x+1, 11x+3\}, 16)$ is connected although $G(\{11x+1\}, 16)$ and $G(\{11x+3\}, 16)$ are both not connected. In Proposition 2.3.3 we will give the criteria for a UM-LCG G to be connected even if G_1 and G_2 are not. But first let us consider the following theorems used in the proof of that proposition.

THEOREM 2.3.1 [20]. *If $\gcd(a,n) = 1$, then the period of the sequence $\{ax_i + b \bmod n; x_0 \in Z_n\}$ is the period of the sequence $\{y_i + 1 \bmod (n/d); y_0 = 0\}$ where $d = \gcd(n, x_0(a-1) + b)$.*

THEOREM 2.3.2 [15]. *Let Z denote the set of integers. Every subgroup H of the additive group Z is cyclic. Either $H = \langle 0 \rangle = \{0\}$ or $H = \langle m \rangle = \{mt : t \in Z\}$, where m is the least positive integer in H.*

PROPOSITION 2.3.3 *Let $n = 2^p$, $a, b \in N$ be odd and $d = 2^jh$ where $j \geq 0$ and h is odd. Let $G = G(\{f_1, f_2\}, n)$ be an LCG with distinct generators $f_1 = ax+b$ and $f_2 = ax+b+d$ whose inverses are $g_1 = a^{-1}x - a^{-1}b$ and $g_2 = a^{-1}x - a^{-1}(b+d)$, respectively. Define $A = \{[f_2g_1]^t(0) \bmod n : t = 0, 1, 2, \ldots\}$, $g_1(A) = \{g_1[f_2g_1]^t(0) \bmod n : t = 0, 1, 2, \ldots\}$, and $A^* = A \cup g_1(A)$. Then*

(i) $A = \{2^jt \bmod n : t = 0, 1, 2, \ldots\}$ and $|A| = 2^{p-j}$. Hence, if d is odd, i.e., if $j = 0$, then $A = V(G)$.

(ii) $g_1(A) = \{g_1(2^jt_1) + 2^jt_2 \bmod n : t_1, t_2 \in N\}$ and $|g_1(A)| = |A|$.

(iii) $A \cap g_1(A) = \emptyset$, and hence $|A^*| = 2|A| = 2^{p-j+1}$, for $j \geq 1$.

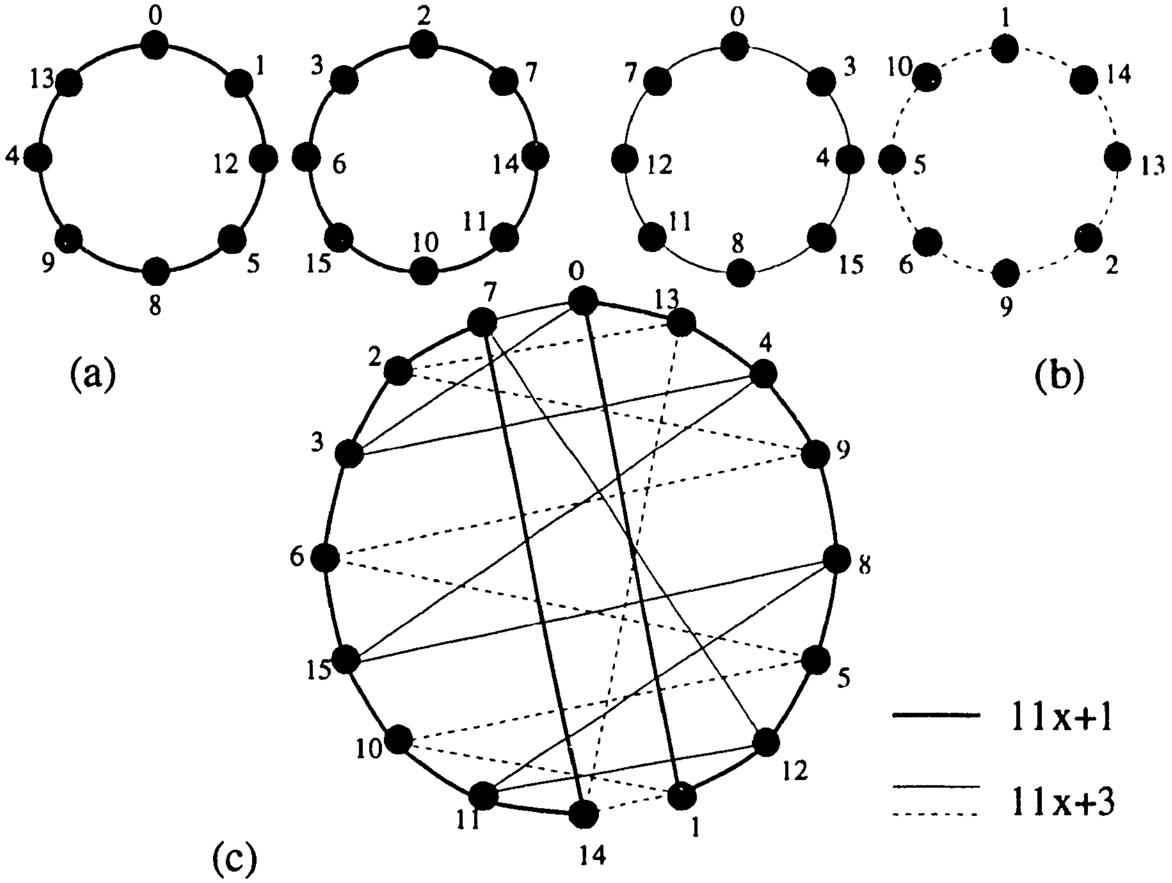


Figure 2.1: (a) $G(\{11x+1\}, 16)$; (b) $G(\{11x+3\}, 16)$; (c) $G(\{11x+1, 11x+3\}, 16)$

(iv) *For $a = 2^i k - 1 \in N$ where $i \geq 2$ and k is odd, and and for $j > 0$, the elements of A^*, together with the edges in G that are incident with them, form a component of G if and only if $d | b(a+1)$, i.e. $j \leq i$.*

(v) *For $a = 2^i k - 1 \in N$ where $i \geq 2$ and k is odd, G is connected if and only if $d = 2h$.*

Proof. *(i)* For any x, $[f_2 g_1](x) \equiv x + d \bmod n$. Hence $[f_2 g_1]^t(0) \equiv td \bmod n$ for any nonnegative integer t. So the elements of A are those of the sequence $\{x_i + d \bmod n; x_0 = 0\}$. By Theorem 2.3.1, the period of this sequence is the period of the sequence $\{y_i + 1 \bmod m; y_0 = 0\}$ where $m = n/\gcd(n,d) = 2^{p-j}$. Since this period is precisely 2^{p-j}, we must have $|A| = 2^{p-j}$. We can think of the elements of A as numbers forming a cyclic subgroup of Z_n. Since $2^j ht \bmod n \in A$ for any integer t, when $ht \equiv 2^{p-j} + 1 \bmod n$, i.e. when $t \equiv 2^{p-j}h^{-1} + h^{-1} \bmod n$, we must have $2^j ht \equiv 2^j(2^{p-j} + 1) \equiv 2^j \bmod n \in A$. This means that the smallest positive element of A is 2^j. By Theorem 2.3.2, $A = \langle 2^j \rangle = \{2^j t \bmod n : t = 0, 1, 2, \ldots\}$.

(ii) From *(i)*, $A = \{2^j t \bmod n : t \in N\}$. So we have $g_1(A) = \{g_1(2^j t) \bmod n : t \in N\}$. For any $t_1, t_2 \in N$, $|g_1(2^j t_1) - g_1(2^j t_2)| = |a^{-1}(2^j t_1) - a^{-1}b - a^{-1}(2^j t_2) + a^{-1}b| = |a^{-1}2^j(t_1 - t_2)| = 2^j |a^{-1}(t_1 - t_2)|$. Hence, if $x, y \in g_1(A)$, then $|x - y|$ is a multiple of 2^j.

Let $y \in N$ and $x \equiv a^{-1}(2^j t) - a^{-1}b \bmod n \in g_1(A)$ for some t. Then $|x - y| \equiv 2^j s \bmod n$ for some $s \Rightarrow a^{-1}2^j t - a^{-1}b - y \equiv \pm 2^j s \bmod n \Rightarrow y \equiv a^{-1}2^j t - a^{-1}b \pm 2^j s \bmod n = a^{-1}(2^j(t \pm as)) - a^{-1}b \bmod n$. Hence, if $x \in g_1(A)$ and $|x - y|$ is a multiple of 2^j, then $y \in g_1(A)$.

That $|g_1(A)| = |A|$ follows from the fact that g_1 as a linear function is a bijection on Z_n.

(iii) Suppose $A \cap g_1(A) \neq \emptyset$. Then by *(i)* and *(ii)*, there exist $t_1, t_2, t_3 \in N$ such that $2^j t_1 \equiv g_1(2^j t_2) + 2^j t_3 \bmod n \Leftrightarrow 0 \equiv g_1(2^j t_2) + 2^j(t_3 - t_1) \bmod n \Leftrightarrow 0 \in g_1(A) \Leftrightarrow$ there exists $t \in N$ such that $0 \equiv g_1(2^j t) \equiv a^{-1}(2^j t) + a^{-1}b \bmod n \Leftrightarrow a^{-1}b \equiv -a^{-1}(2^j t) \bmod n \Leftrightarrow b \equiv -2^j t \bmod n \Leftrightarrow b$ is even, which is a contradiction. Hence, $A \cap g_1(A) = \emptyset$. By *(i)* and *(ii)*, we have $|A^*| = |A \cup g_1(A)| = |A| + |g_1(A)| =$

$2^{p-j}+2^{p-j}=2^{p-j+1}$ for $j\geq 1$.

(iv) Each $x\in A^*$ is of the form $[f_2g_1]^t(0) \bmod n\in A$ or $g_1[f_2g_1]^t(0) \bmod n\in g_1(A)$ for some $t\in N$. We would like to show that A^* is closed under f_1, f_2, g_1, and g_2 if and only if $d|b(a+1)$. We take note that $d|b(a+1)\Leftrightarrow 2^jh|2^ikb\Leftrightarrow 2^j|2^ikbh^{-1}\Leftrightarrow j\leq i$. Moreover, $d|b(a+1)\Leftrightarrow d|b(a+1)a^{-1}=b(a^{-1}+1)$; hence, $d|b(a^{-1}+1)\Leftrightarrow j\leq i$.

Suppose $x\equiv[f_2g_1]^t(0)\equiv td \bmod n\in A$. Then for some $s\in N$, $f_1(x)\equiv g_1[f_2g_1]^s(0) \bmod n\in g_1(A)\Leftrightarrow atd+b\equiv g_1(sd)\equiv a^{-1}sd-a^{-1}b \bmod n\Leftrightarrow atd+b+a^{-1}b\equiv a^{-1}sd \bmod n\Leftrightarrow a^2td+b(a+1)\equiv sd \bmod n$. By Thm. 2.1.1, there is a solution for s if and only if $d|b(a+1)$, i.e. $j\leq i$. Hence, $f_1(x)\in g_1(A)$ if and only if $j\leq i$. We know that $f_2(x)=f_1(x)+d$. Since d is a multiple of 2^j, by *(ii)* we have $f_2(x) \bmod n\in g_1(A)$. By definition, $g_1(x)\equiv g_1[f_2g_1]^t(0) \bmod n\in g_1(A)$, and by *(ii)*, $g_2(x)\equiv g_1(x)-a^{-1}d \bmod n\in g_1(A)$.

Suppose $x\equiv g_1[f_2g_1]^t(0)\equiv g_1(td)\equiv a^{-1}td-a^{-1}b\equiv a^{-1}(td-b) \bmod n\in g_1(A)$. Then $g_1(x)=g_1(a^{-1}(td-b))=a^{-1}(a^{-1}(td-b))-a^{-1}b=a^{-2}(td-b)-a^{-1}b=a^{-2}td-a^{-1}b(a^{-1}+1)$. There exists a solution for r in the congruence $a^{-2}td-a^{-1}b(a^{-1}+1)\equiv dr \bmod n$ if and only if $d|b(a^{-1}+1)$, i.e. $j\leq i$. Hence, $g_1(x) \bmod n\in A$ if and only if $j\leq i$. We also have $g_2(x)\equiv g_1(x)-a^{-1}d \bmod n\in(A)$ by *(i)*. By definition $f_1(x)\equiv[f_2g_1]^t(0) \bmod n\in A$, and by *(i)*, $f_2(x)\equiv f_1(x)+d\equiv f_1(x)+2^jh \bmod n\in A$.

Hence, we have shown the closure of A^* .

(v) By *(iii)* and *(iv)*, the 2^{p-j+1} vertices of A^* together with the edges incident to them comprise a component of G if and only if $1\leq j\leq i$. Hence, $A^*=V(G)$ if and only if $j=1$, i.e. $d=2h$. This means that G is connected if and only if $d=2h$. □

Example 2.3.1 We illustrate parts (i)-(iv) of the preceeding proposition using $n=2^5$, $a=2^ik-1=7$ where $i=3$ and $k=1$, $b=1$ and $d=2^jh$ where $h=3$.

1. For $j=2$: We have $d=2^2(3)=12$, $f_1=7x+1$, $f_2=7x+13$, $A=\{0,12,24,4,16,28,8,20\}=\{4t:t=0,\ldots,7\}, g_1(A)=\{9,29,17,5,25,13,1,21\}$ $=\{1+4t:t=0,\ldots,7\}$. Part (a) of Figure 2.2 shows $A^*=A\cup g_1(A)$, together with the incident edges, as a component of $G(\{7x+1,7x+13\},32)$.

2. For $j=3$: We have $d=2^3(3)=24$, $f_1=7x+1$, $f_2=7x+25$, $A=$

$\{0,24,16,8\} = \{8t : t = 0,\ldots,3\}$, $g_1(A) = \{9,17,25,1\} = \{1+8t : t = 0,\ldots,3\}$. Part (b) of Figure 2.2 shows $A^* = A \cup g_1(A)$, together with the incident edges, as a component of $G(\{7x+1, 7x+25\}, 32)$.

3. For $j = 4$: We have $d = 2^4(3) \equiv 16 \bmod 32$, $f_1 = 7x+1$, $f_2 = 7x+17$, $A = \{0,16\} = \{16t : t = 0,1\}$, $g_1(A) = \{9,25\} = \{9+16t : t = 0,1\}$. Part (c) of Figure 2.2 shows that $A^* = A \cup g_1(A)$, together with the incident edges, does *not* form a component of $G(\{7x+1, 7x+17\}, 32)$.

◇

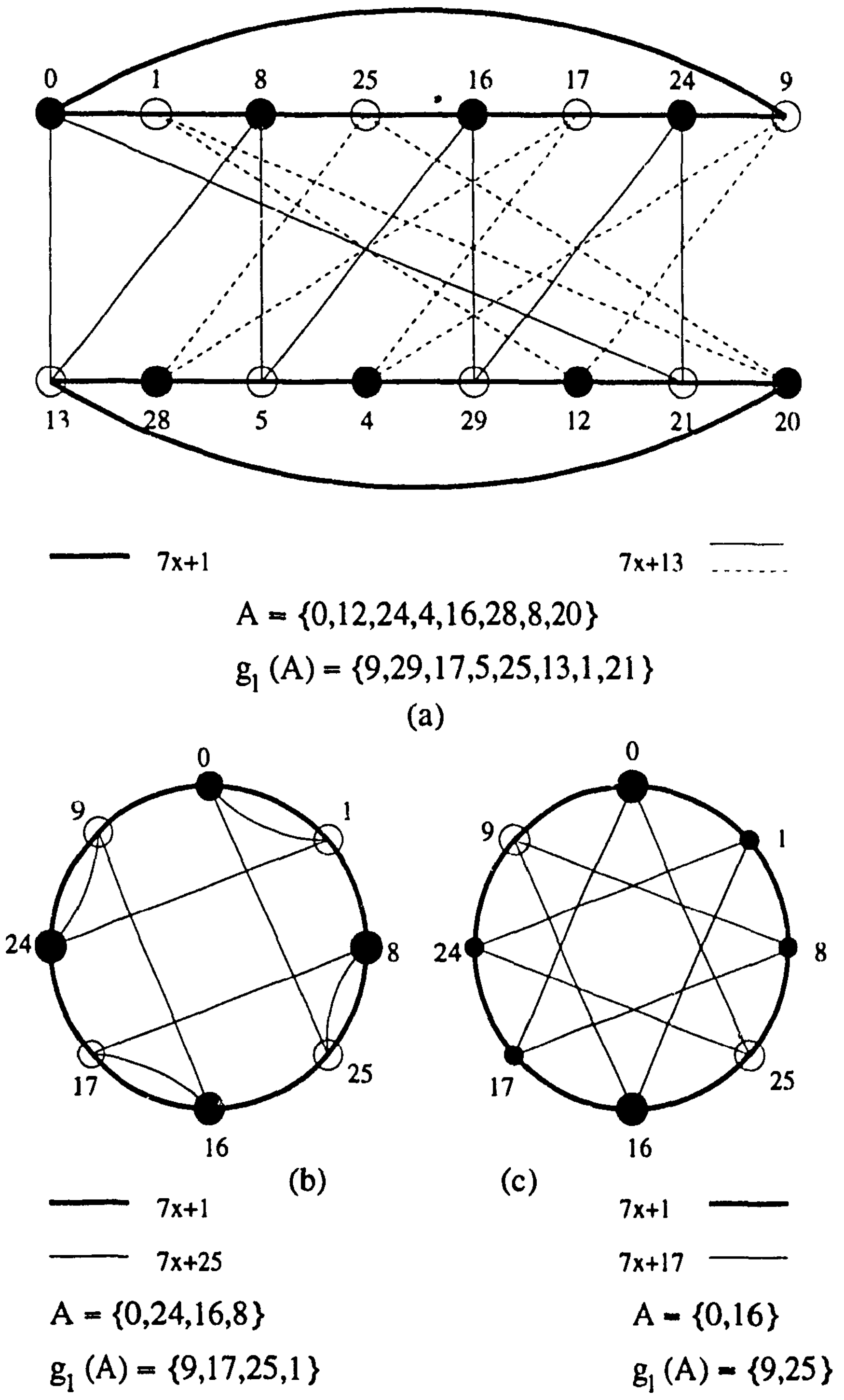
Lastly, when the multiplier is odd and the constants are of different parity, it turns out that G is connected even if the multiplier is not of the form 2^ik+1, as proved by the following:

PROPOSITION 2.3.4 *Let $f_1 = ax + b \bmod n$, $f_2 = ax + b + d \bmod n$ be distinct invertible linear congruential functions on Z_n where $n = 2^p$ and $a, d \in N$ are odd. Then $G = G(\{f_1, f_2\}, n)$ is connected.*

Proof. Let the inverse of f_1 be g_1. Then we have $[f_2g_1](x) \equiv f_2(a^{-1}x - a^{-1}b) \bmod n = x - b + (b+d) \bmod n = x + d \bmod n$. Since d is odd, $[f_2g_1](0) = d$ generates all elements of Z_n, i.e., $\langle f_2g_1(0)\rangle = \langle d\rangle = Z_n$. This means that if $x, y \in Z_n$, then there exists $t \in N$ with $0 \leq t \leq n-1$ such that $y \equiv [f_2g_1]^t(x) \bmod n$. Hence, vertices x and y are connected in G, and G is a connected graph. □

We summarize the results in Table 2.2. Here we have $f_1 = ax + b$ and $f_2 = ax + c$, $n = 2^p$, a is the odd multiplier, $c = b + d$, and h is an odd integer. 'Case 1' refers to $a = 2^ik + 1$ and 'Case 2' refers to $a = 2^ik - 1$, where $i \geq 2$ and k is an odd integer. In each of these cases are four subcases according to the parity of the constants. For example, Case 1.3 refers to $a = 2^ik + 1$, b is even and d is odd whereby $G(\{ax + b, ax + b + d\}, n)$ is connected.

In the classification, Case 1.1 is by Remark 2.3.1, Cases 1.2, 1.3, 2.2, and 2.3 are by Proposition 2.3.4, Cases 1.4 and 2.4 are by Proposition 2.3.2 and Case 2.1 is by Part (v) of Proposition 2.3.3.



A = {0,12,24,4,16,28,8,20}

g_1 (A) = {9,29,17,5,25,13,1,21}

(a)

(b)

A = {0,24,16,8}

g_1 (A) = {9,17,25,1}

(c)

A = {0,16}

g_1 (A) = {9,25}

Figure 2.2: Components of UM-LCG's containing A and $g_1(A)$

				$G(\{f_1, f_2\}, n)$	
Subcase	b	c	d	Case 1	Case 2
0.1	odd	odd	even	connected	($d = 2h$) connected
					($d \neq 2h$) not connected
0.2	odd	even	odd	connected	connected
0.3	even	odd	odd	connected	connected
0.4	even	even	even	not connected	not connected

Table 2.2: Classification according to connectivity of UM-LCG's with two generators

Example 2.3.2 We illustrate Case 2.1 in Figure 2.3 where $d = 6$ and in Figure 2.4 where $d = 8$. Note that $G(\{11x+3, 11x+9\}, 32)$ is a connected graph while $G(\{11x+3, 11x+11\}, 32)$ has two components. The figures also illustrate how a small difference in the constants of the generators can mean a big difference in the appearance of the graphs.

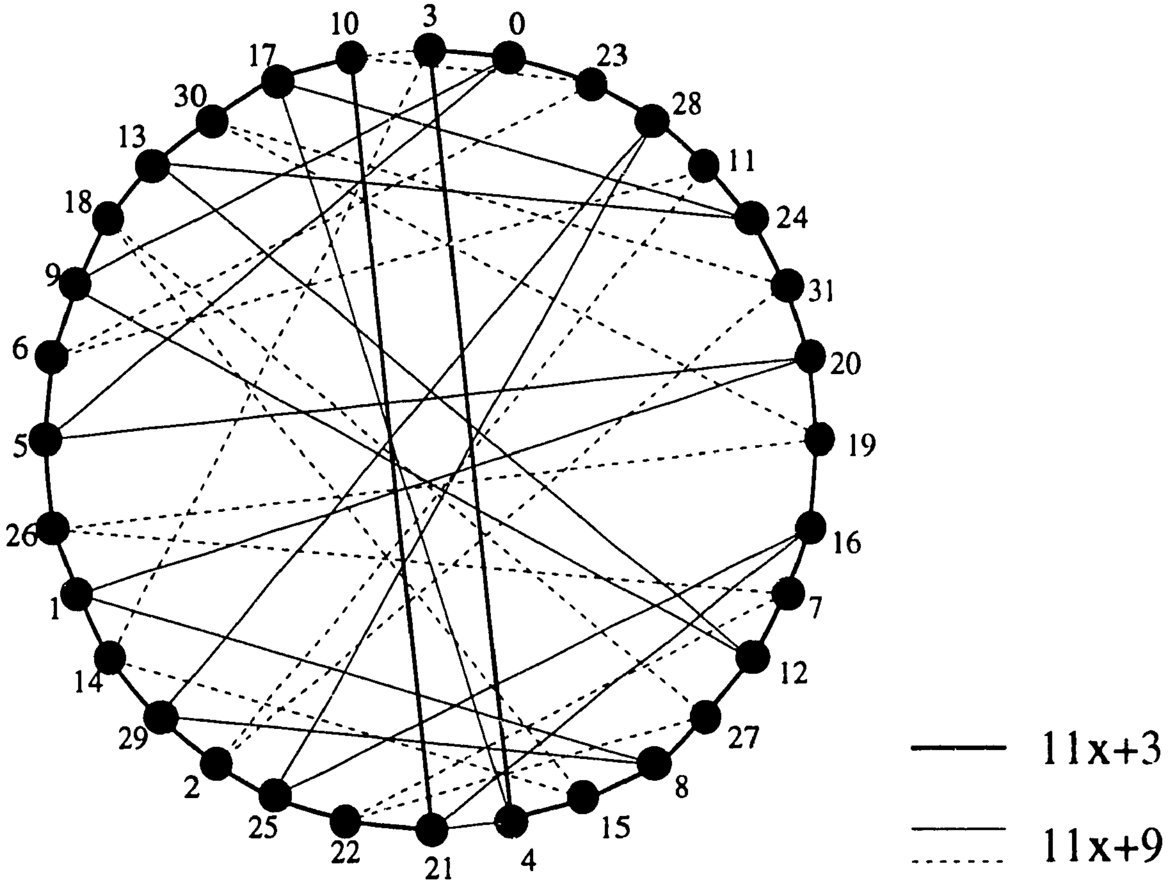


Figure 2.3: $G(\{11x + 3, 11x + 9\}, 32)$

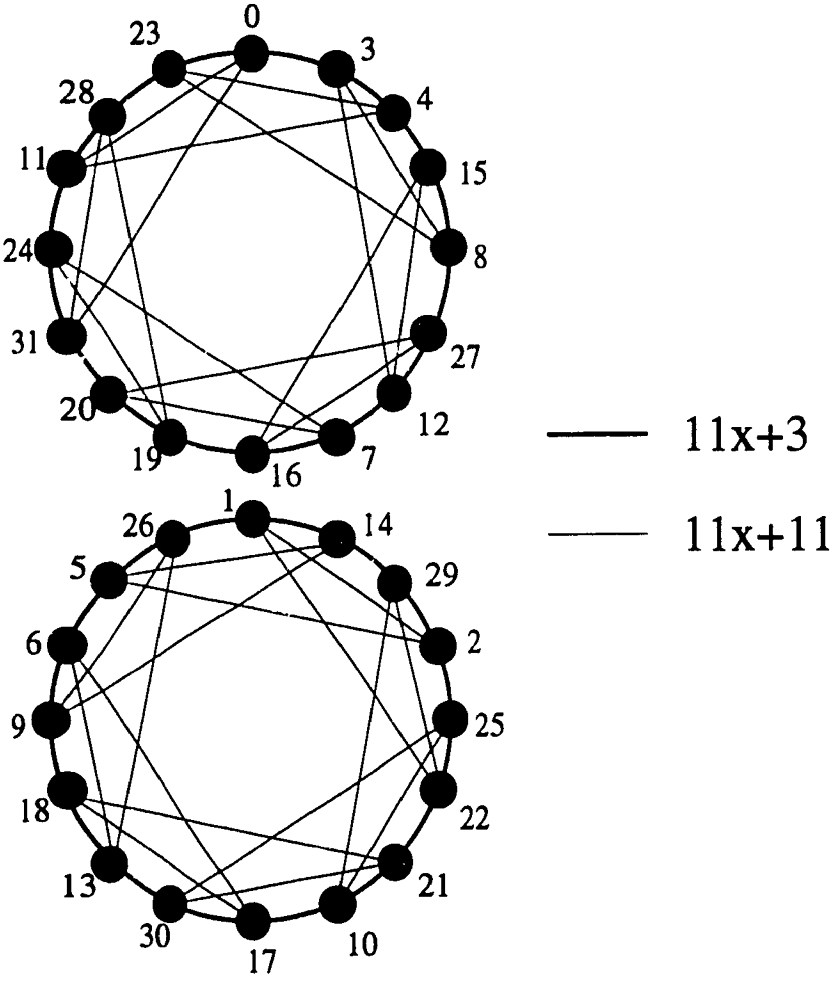


Figure 2.4: $G(\{11x+3, 11x+11\}, 32)$

Chapter 3

OPERATORS ON THE VERTICES OF A UM-LCG

In this chapter we will define operations on numbers in base a notation in preparation for the computation of the diameter bound of the UM-LCG in Chapter 4.

Let $n = 2^p$. Given the graph $G = G(\{f_1, f_2\}, n)$, where $f_1 = ax + b$ and $f_2 = ax + b + d$ are invertible functions with inverses $g_1 = a^{-1}x - a^{-1}b$ and $g_2 = a^{-1}x - a^{-1}(b+d)$ on Z_n and odd integer $a \neq 1$, we know that the vertices are precisely the elements of Z_n and we can represent each vertex x by a number in base a of the form $(x_k, \ldots, x_2, x_1)_a$ modulo n, where $x \equiv x_k a^{k-1} + \ldots + x_2 a + x_1 \bmod n$. We shall adopt the notation $(x_k, \ldots, x_2, x_1)$ without the subscript a to mean that the digits $x_k, \ldots, x_2, x_1$ can be any integer and the notation $(x_k, \ldots, x_2, x_1)_a$ with the subscript a to mean that $0 \leq x_i \leq a - 1$ for $1 \leq i \leq k$. In each case we will drop the notation 'modulo n' as we will always refer to the number as an element of Z_n.

First we observe that the value of k in the notation $(x_k, \ldots, x_1)$ depends on a and n. Let $n = (n_k, n_{k-1}, \ldots, n_1)_a$. Then $n_k a^{k-1} \leq n \Rightarrow a^{k-1} \leq n \Rightarrow k - 1 \leq \log_a n \Rightarrow k \leq 1 + \log_a n$. Maximizing the value of k, we have

$$k = 1 + \lfloor \log_a n \rfloor = \lceil \log_a n \rceil$$

since $\gcd(a, n) = 1$.

Example 3.0.3 If $a = 21$ and $n = 2^{11}$, then $k = \lceil \log_{21} 2^{11} \rceil = 3$ and we have $2^{11} = 4(21)^2 + 13(21) + 11$. $\diamond$

3.1 Shift Operators

Definition 3.1.1 *An invertible function f on Z_n is called a* **shift operator** *if $f(x) = (x_k, \ldots, x_1, x_0)$ for any $x = (x_k, \ldots, x_1)$ and for some integer x_0, i.e. if f shifts $(x_k, \ldots, x_1)$ one place to the left and puts an integer x_0 in the last digit.*

Linear functions with multiplier a, in particular f_1 and f_2, fall in this category. We have, for example,

$$\begin{aligned} f_1(x) &= a(x_k, \ldots, x_1) + b \\ &= a(x_k a^{k-1} + \cdots + x_2 a + x_1) + b \\ &= (x_k a^k + \cdots + x_2 a^2 + x_1 a) + b \\ &= (x_k, \ldots, x_2, x_1, b). \end{aligned}$$

Definition 3.1.2 *An invertible function g on Z_n is called the* **inverse** *of a shift operator if $g(x) = (x_k, \ldots, x_2) + a^{-1}c$ for any $x = (x_k, \ldots, x_1)$ and for some integer c, i.e. if g drops x_1, shifts the rest of the digits to the right and adds an integer $a^{-1}c$.*

For instance, if $x_1 = b$, then $c = 0$ and $g = g_1$, the inverse shift operator of f_1. We have

$$\begin{aligned} g_1(x) &= a^{-1}(x_k, \ldots, x_2, b) - a^{-1}b \\ &= a^{-1}(x_k a^{k-1} + \cdots + x_2 a + b) - a^{-1}b \\ &= x_k a^{k-2} + \cdots + x_3 a + x_2 \\ &= (x_k, \ldots, x_3, x_2). \end{aligned}$$

3.2 Last-Digit Operators

Definition 3.2.1 *A function f is called a* **last-digit operator** *if $f(x) = (x_k, \ldots, x_2,$

$x_1 + c$) for any $x = (x_k, \ldots, x_1)$, or in other words, if $f(x) = x + c$, for some integer c.

In particular, the composite functions $[f_2g_1]$ and $[f_1g_2]$ are last-digit operators on all the elements of Z_n. Applying the functions from right to left, we have:

$$\begin{aligned}
[f_2g_1](x) &= f_2(a^{-1}x - a^{-1}b) \\
&= a(a^{-1}x - a^{-1}b) + (b + d) \\
&= x + d \\
&= (x_k, \ldots, x_2, x_1) + d \\
&= (x_k, \ldots, x_2, x_1 + d)
\end{aligned}$$

and

$$\begin{aligned}
[f_1g_2](x) &= f_1(a^{-1}x - a^{-1}(b + d)) \\
&= a(a^{-1}x - a^{-1}(b + d)) + b \\
&= x - d \\
&= (x_k, \ldots, x_2, x_1) - d \\
&= (x_k, \ldots, x_2, x_1 - d).
\end{aligned}$$

Similarly, $[g_1f_2]$ and $[g_2f_1]$ are last-digit operators because $[g_1f_2](x) = x + a^{-1}d$ and $[g_2f_1](x) = x - a^{-1}d$. We also classify the identity operator $[i]$, where $[i] = [f_1g_1] = [g_1f_1] = [f_2g_2] = [g_2f_2]$, as a last-digit operator because $[i](x) = x + 0 = x$ for all x.

3.3 r-Digit Operators

Definition 3.3.1 *A function f is called an* **r-digit operator**, *where $1 \leq r \leq k$, if $f(x) = (x_k, \ldots, x_r, \ldots, x_1) + (c_r, \ldots, c_1) = (x_k, \ldots, x_{r+1}, x_r + c_r, \ldots, x_1 + c_1)$ for any $x = (x_k, \ldots, x_1)$ and for some integers $c_r, \ldots, c_1$; in other words, if f operates on the last r digits of x by adding the constants $c_r, \ldots, c_1$.*

In particular, a last-digit operator is a '1-digit' operator, and the composite function $[f_2[f_1g_2]g_1]$ is a 2-digit operator. We have

$$\begin{aligned}
[f_2[f_1g_2]g_1](x) &= f_2[f_1g_2](a^{-1}x - a^{-1}b) \\
&= f_2(a^{-1}x - a^{-1}b - d) \\
&= a(a^{-1}x - a^{-1}b - d) + b + d \\
&= x - b - ad + b + d \\
&= (x_k, \ldots, x_2, x_1) - ad + d \\
&= (x_k, \ldots, x_2 - d, x_1 + d).
\end{aligned}$$

In general, from a 1-digit operator $[f_{j_1}g_{k_1}]$ where $j_1, k_1 \in \{1,2\}$ we can build up an r-digit operator as given by the following proposition:

PROPOSITION 3.3.1 *Let $f_{j_i}(x) = ax + b_{j_i}$ and $g_{k_i}(x) = a^{-1}x - a^{-1}b_{k_i}$, where $j_i, k_i \in \{1,2\}$ for any positive integer i, such that $f_{j_i}g_{k_i}(x) = x + c_i$ is a last-digit operation on x, where $c_i = b_{j_i} - b_{k_i}$. Then for any integer r, with $1 \leq r \leq k$,*

$$[f_{j_1}[f_{j_2}[\cdots[f_{j_{r-1}}[f_{j_r}g_{k_r}]g_{k_{r-1}}]\cdots]g_{k_2}]g_{k_1}](x)$$

$$= (x_k, \ldots, x_{r+1}, x_r + c_r, x_{r-1} + c_{r-1}, \ldots, x_1 + c_1).$$

Proof. We can prove this by induction on r. We have seen that the assertion is true for $r = 1$. Let us suppose that it is also true for the first i positive integers. Then

$$\begin{aligned}
&f_{j_1}[f_{j_2}[\cdots[f_{j_i}[f_{j_{i+1}}g_{k_{i+1}}]g_{k_i}]\cdots]g_{k_2}]g_{k_1}](x) \\
&\quad = f_{j_1}[f_{j_2}[\cdots[f_{j_i}[f_{j_{i+1}}g_{k_{i+1}}]g_{k_i}]\cdots]g_{k_2}](a^{-1}x - a^{-1}b_{k_1}) \\
&\quad = f_{j_1}[(a^{-1}x - a^{-1}b_{k_1}) + (0, \ldots, 0, c_{i+1}, c_i, \ldots, c_3, c_2)] \\
&\quad = x + (b_{j_1} - b_{k_1}) + (0, \ldots, 0, c_{i+1}, c_i, \ldots, c_3, c_2, 0) \\
&\quad = x + (0, \ldots, 0, c_{i+1}, c_i, \ldots, c_3, c_2, c_1).
\end{aligned}$$

Hence, the assertion is also true for $i + 1$. □

Since the proof is by induction, the proposition is true for any value of k and for any value of r, with $r \leq k$.

Example 3.3.1 Let $n = 2^{13} = 8192$, $f_1(x) = 9x + 5$, and $f_2(x) = 9x + 8$. We have $\lceil \log_9 2^{13} \rceil = 5$, $g_1(x) = 9^{-1}x - 9^{-1}(5) \equiv 3641x + 6371 \bmod n$, $g_2(x) = 9^{-1}x + 9^{-1}(8) \equiv 3641x + 3640 \bmod n$, $[f_1 g_2](x) = x - 3$, and $[f_2 g_1](x) = x + 3$. Since $2172 = 2(9)^3 + 8(9)^2 + 7(9) + 3$, we can write $2172 = (0, 2, 8, 7, 3)$ and we have

$$\begin{aligned}
&[f_2 f_1 f_1 g_2 g_1 g_1](2172)\\
&\quad = [f_2[f_1[f_1 g_2] g_1] g_1](0, 2, 8, 7, 3)\\
&\quad = (0, 2, 8 - 3, 7 + 0, 3 + 3)\\
&\quad = (0, 2, 5, 7, 6) = 1932.
\end{aligned}$$

To check, we have:

$$\begin{aligned}
&[f_2 f_1 f_1 g_2 g_1 g_1](2172)\\
&\quad \equiv f_2 f_1 f_1 g_2 g_1(1151)\\
&\quad \equiv f_2 f_1 f_1 g_2(2858)\\
&\quad \equiv f_2 f_1 f_1(5778)\\
&\quad \equiv f_2 f_1(2855)\\
&\quad \equiv f_2(1124) \equiv 1932 \bmod 8192.
\end{aligned}$$

◇

In the above example we see that $[f_2[f_1[f_1 g_2] g_1] g_1]$ is a 3-digit operator and is actually a cluster of three last-digit operators — $[f_1 g_2]$ acting on the third digit, $[f_1 g_1]$ on the second and $[f_2 g_1]$ on the first.

Note that for each last-digit operator $[f_{j_i} g_{k_i}]$, the functions f_{j_i} and g_{k_i} can be permuted, and so it is possible to have an r-digit operator which is a permuted version of the one given in the proposition.

3.4 Mixed Operators

Definition 3.4.1 *A* **mixed operator** *on $x = (x_k, \ldots, x_1)$ is any combination of the above operators.*

We pay close attention to the fact that an inverse operator adds a constant $a^{-1}c$ after shifting $(x_k, \ldots, x_2, x_1)$ to $(x_k, \ldots, x_2)$. Hence, the result of a mixed operation may not be conveniently expressed as a k-bit sequence in terms of $x_1, \ldots, x_k$, particularly when $c \neq 0$. We will try to avoid this case by considering only mixed operators in which the number of shift operators is greater than or equal to the number of their inverse shift operators.

Example 3.4.1 The operator $h = f_2g_1f_2f_2f_2g_1g_2f_1g_2f_1$ can be thought of as the combination, denoted by square brackets, $[h] = [f_2g_1][f_2][f_2f_2g_1g_2][f_1g_2][f_1]$. To compute for the value of x under this operation, we have:

$$\begin{aligned}
(x_k, \ldots, x_2, x_1) &\xrightarrow{[f_1]} (x_k, \ldots, x_2, x_1, b) \\
&\xrightarrow{[f_1g_2]} (x_k, \ldots, x_2, x_1, b-d) \\
&\xrightarrow{[f_2f_2g_1g_2]} (x_k, \ldots, x_2, x_1+d, b-d) \\
&\xrightarrow{[f_2]} (x_k, \ldots, x_2, x_1+d, b-d, b+d) \\
&\xrightarrow{[f_2g_1]} (x_k, \ldots, x_1+d, b-d, b+d+d)
\end{aligned}$$

where $(x_k, \ldots, x_2, x_1, b)$ is the image of $(x_k, \ldots, x_2, x_1)$ under the operation $[f_1]$, $(x_k, \ldots, x_2, x_1, b-d)$ is the image of $(x_k, \ldots, x_2, x_1, b)$ under the operation $[f_1g_2]$, and so on. We apply modulo n for the final step. $\diamond$

Chapter 4

AN UPPER BOUND ON THE DIAMETER OF $G\big(\{ax+b, ax+b+d\}, 2^p\big)$

The main objective of this chapter is to give an upper bound on the diameter of a connected UM-LCG, of order $n = 2^p$ and with 2 generators, which is in the order of $O(\log n)$. By definition, for any function $B(n)$, we have $B(n) = O(\log n)$ if and only if there exist α and n_0 such that $B(n) \leq \alpha \log n$ for all $n \geq n_0$. We are not concerned so much about the value of α or any other constant in the formula, as our goal is to show the logarithmic nature of the bound.

Normally, to find the diameter of a connected graph G we start with an arbitrary vertex and calculate its maximum distance from any other vertex. Repeating this process for all the vertices in the graph, we then get the diameter of the graph which is equal to the maximum distance over all the vertices. However, since we are interested only on the upper bound on the diameter of G, it suffices to find the upper bound on the distance $d(\overline{x}, x)$ of a fixed vertex $\overline{x}$ from any other vertex x in G. This is because if y and z are vertices in G and G is connected, then

$$d(y,z) \leq d(\overline{x},y) + d(\overline{x},z)$$

by the triangle inequality. Hence, we have

$$Diam(G) \leq 2\{\max_{x \in V(G)} d(\overline{x}, x) : \overline{x} \in V(G)\}$$

where $\max_{x \in V(G)} d(\overline{x}, x)$ denotes the maximum distance of $\overline{x}$ from any vertex x in G.

We have to consider, of course, only the case when G is a connected graph, so we pay attention to the properties discussed in Chapter 2. We will find the upper bound on the diameter of G in each of the cases in which G is connected as presented on Table 2.2.

4.1 The Set $A = \{[f_2 g_1]^t(0) \bmod n : t = 0, 1, \ldots\}$

Let G be a UM-LCG on $n = 2^p$ vertices generated by $f_1 = ax + b$ and $f_2 = ax + b + d$ with inverses $g_1 = a^{-1}x - a^{-1}b$ and $g_2 = a^{-1}x - a^{-1}(b + d)$, respectively. We first considered the set $A = \{[f_2 g_1]^t(0) \bmod n : t = 0, 1, \ldots\} = \{td \bmod n : t = 0, 1, \ldots\}$ in our study of the connectivity of G in Chapter 2. Since it plays an important role in our computations, in this section we study some of its properties.

We observe that $A \subseteq V(G)$, with $A = V(G)$ if d is odd. Since the function $[f_2 g_1] = x + d$ forms a periodic sequence on Z_n, the elements of A are traversed by a closed path in G, namely the path

$$0 \rightarrow g_1(0) \rightarrow f_2 g_1(0) \rightarrow g_1 f_2 g_1(0) \rightarrow [f_2 g_1]^2(0) \rightarrow \cdots [f_2 g_1]^s(0) \equiv 0 \bmod n$$

for some $s > 0$. Hence any two elements of A are connected in G.

Using the notations from Chapter 3, the elements of A can be written in the form of a k-bit sequence $(x_k, \ldots, x_1)$ modulo n, where $k = \lceil \log_a n \rceil$, as follows:

$$(0, \ldots, 0), (0, \ldots, d), (0, \ldots, 2d), \ldots$$

$$(0, \ldots, (a-1)d), (0, \ldots, ad) = (0, \ldots, d, 0),$$

$$(0, \ldots, d, d), (0, \ldots, d, 2d), \ldots, (0, \ldots, d, (a-1)d),$$

$$(0, \ldots, d, ad) = (0, \ldots, 2d, 0), \cdots$$

$$\vdots$$

$$((a-1)d, 0, \ldots, 0), \cdots$$

$$\vdots$$

$$((a-1)d, (a-1)d, \ldots, (a-1)d).$$

Hence we can think of A as

$$A = \{(j_k d, \ldots, j_1 d) : 0 \leq j_i \leq a-1, 1 \leq i \leq k\}.$$

If we fix an element $\overline{x} = (\frac{1}{2}(a-1)d, \ldots, \frac{1}{2}(a-1)d)$, we observe that any other element x of A can be expressed as

$$x = \overline{x} + (j_k d, \ldots, j_1 d)$$

where $-\frac{1}{2}(a-1) \leq j_i \leq \frac{1}{2}(a-1)$ for $1 \leq i \leq k$. Hence, we can also think of A as

$$A = \{x \in V(G) : x = \overline{x} + (j_k d, \ldots, j_1 d), \text{ where } -\tfrac{1}{2}(a-1) \leq j_i \leq \tfrac{1}{2}(a-1)$$
$$\text{for } 1 \leq i \leq k \text{ and } \overline{x} = (\tfrac{1}{2}(a-1)d, \ldots, \tfrac{1}{2}(a-1)d)\}$$

Let us use the notation

$$(x_k, \ldots, x_1) \xrightarrow{[h]} (y_k, \ldots, y_1)$$

to indicate that the image of $x = (x_k, \ldots, x_1)$ under the operation $[h]$ is $y = (y_k, \ldots, y_1)$. With this notation we say that y *can be obtained from* x *in one step* using the operator $[h]$, where $[h]$ is either a shift, a last-digit or an r-digit operator. This means that x and y are connected in G via a path defined by $[h]$. For example, if $[h] = [f_2 f_1 g_2 g_1]$ then, in the graph G, x is connected to y via the path

$$\begin{aligned} x &\rightarrow g_1(x) \bmod 2^p \rightarrow g_2 g_1(x) \bmod 2^p \rightarrow f_1 g_2 g_1(x) \bmod 2^p \\ &\rightarrow f_2 f_1 g_2 g_1(x) \bmod 2^p \equiv y. \end{aligned}$$

Hence, there exists a path from x to y of length 4, which is equal to the number of functions in $[h]$. This, however, does not mean that $d(x, y)$ is equal to 4 because 4 is merely an upper bound on $d(x,y)$. In general, the length of a path from x to y is an upper bound on $d(x,y)$.

We give the maximum distance between any two elements of A in the following proposition.

PROPOSITION 4.1.1 *Let $G(\{f_1 = ax + b, f_2 = ax + b + d\}, 2^p)$ be a UM-LCG such that $a \neq 1$ is odd and b, d are positive integers, and let the inverse of f_1 on Z_{2^p} be $g_1 = a^{-1}x - a^{-1}b$. Define $A = \{[f_2g_1]^t(0) \bmod 2^p : t = 0, 1, \dots\}$. If $x, y \in A$, then*

$$d(x,y) \leq 2(a-1)\lceil \log_a 2^p \rceil.$$

Proof. Let $\overline{x} = (\frac{1}{2}(a-1)d, \dots, \frac{1}{2}(a-1)d) \in A$. If $x, y \in A$, then by the triangle inequality, $d(x,y) \leq d(\overline{x},x) + d(\overline{x},y)$. So, to prove the proposition we only have to show that $d(\overline{x},x) \leq k(a-1)$ for any x, where $k = \lceil \log_a 2^p \rceil$. We use Proposition 3.3.1 in our calculations.

<u>CASE 1:</u> If $x = \overline{x} + (j_kd, \dots, j_1d)$ where $-1 \leq j_i \leq 1$ for $1 \leq i \leq k$ then we apply one of the following operations to the vertex $\overline{x}$ in order to obtain x.

(Case 1.1) If $j_k, \dots, j_2 = 0$ and $j_1 \neq 0$,

$$\overline{x} \xrightarrow{[h_1]} \overline{x} + (0, \dots, j_1d)$$

where

$$h_1 = \begin{cases} f_2g_1 & \text{if } j_1 = 1 \\ f_1g_2 & \text{if } j_1 = -1 \end{cases}$$

(Case 1.2) If $j_k, \dots, j_3 = 0$ and $j_2 \neq 0$,

$$\overline{x} \xrightarrow{[h_2]} \overline{x} + (0, \dots, 0, j_2d, j_1d)$$

where

$$h_2 = \begin{cases} f_{t_1}[f_2g_1]g_{s_1} & \text{if } j_2 = 1 \\ f_{t_1}[f_1g_2]g_{s_1} & \text{if } j_2 = -1 \end{cases}$$

in which the last-digit operator $[f_{t_1}g_{s_1}]$, where $t_1, s_1 \in \{1,2\}$, is used to obtain j_1d.

(Case 1.3) If $j_k, \ldots, j_4 = 0$ and $j_3 \neq 0$,

$$\overline{x} \xrightarrow{[h_3]} \overline{x} + (0, \ldots, j_3d, j_2d, j_1d)$$

where

$$h_3 = \begin{cases} f_{t_1} f_{t_2} [f_2 g_1] g_{s_2} g_{s_1} & \text{if } j_3 = 1 \\ f_{t_1} f_{t_2} [f_1 g_2] g_{s_2} g_{s_1} & \text{if } j_3 = -1 \end{cases}$$

in which the 2-digit operator $[f_{t_1} f_{t_2} g_{s_2} g_{s_1}]$ is used to obtain the digits j_2d and j_1d.

⋮

(Case 1.k) If $j_k \neq 0$,

$$\overline{x} \xrightarrow{[h_k]} \overline{x} + (j_kd, \ldots, j_1d)$$

where

$$h_k = \begin{cases} f_{t_1} f_{t_2} \cdots f_{t_{k-1}} [f_2 g_1] g_{s_{k-1}} \cdots g_{s_2} g_{s_1} & \text{if } j_k = 1 \\ f_{t_1} f_{t_2} \cdots f_{t_{k-1}} [f_1 g_2] g_{s_{k-1}} \cdots g_{s_2} g_{s_1} & \text{if } j_k = -1 \end{cases}$$

in which the $(k-1)$-digit operator $[f_{t_1} \cdots f_{t_{k-1}} g_{s_{k-1}} \cdots g_{s_1}]$ is used to obtain the digits $j_{k-1}d, \ldots, j_1d$.

Thus, in order to obtain vertex x from vertex $\overline{x}$ in one step, we need an r-digit operator $[h_r]$, where $r \leq k$, which contains at most $2k$ functions. Hence we have $d(\overline{x}, x) \leq 2k$.

<u>CASE 2:</u> If $x = \overline{x} + (j_kd, \ldots, j_1d)$, where $-2 \leq j_i \leq 2$ for $1 \leq i \leq k$, we do the following steps:

(Step 1) Use the results of Case 1:

$$\overline{x} \xrightarrow{[h']} \overline{x} + (j'_kd, \ldots, j'_1d)$$

where $[h']$ is an r-digit operator, $r \leq k$, and $-1 \leq j'_i \leq 1$ for $1 \leq i \leq k$. Here we have $j'_i = 0$ if $j_i = 0$, $j'_i = 1$ if $j_i = 1$ or 2, and $j'_i = -1$ if $j_i = -1$ or -2.

(Step 2) Apply an r-digit operator $[h'']$ to $(j'_kd, \ldots, j'_1d)$:

$$\overline{x} + (j'_kd, \ldots, j'_1d) \xrightarrow{[h'']} \overline{x} + (j_kd, \ldots, j_1d)$$

where $[h''] = [f_{t_1} \cdots f_{t_k} g_{s_k} \cdots g_{s_1}]$ with

$$f_{t_m} g_{s_m} = \begin{cases} f_2 g_1 & \text{if } j_m = 2 \\ i & \text{if } j_m = j_r' \\ f_1 g_2 & \text{if } j_m = -2 \end{cases}$$

for $1 \leq m \leq k$. Since each of $[h']$ and $[h'']$ contains at most $2k$ functions, we have $d(\overline{x}, x) \leq 2(2k) = 4k$. Hence, we can obtain x from $\overline{x}$ in two steps, each step consisting of at most $2k$ functions.

$\vdots$

CASE t: Similarly, for any value of t, if $x = \overline{x} + (j_k d, \ldots, j_1 d)$ where $-t \leq j_i \leq t$ for $1 \leq i \leq k$, we can obtain x from $\overline{x}$ in t steps, each consisting of at most $2k$ functions. In particular, if $t = (a-1)/2$, in which case all the elements of A are represented, we can obtain x from $\overline{x}$ in $(a-1)/2$ steps using at most $2k[(a-1)/2] = k(a-1)$ functions. Hence, $d(\overline{x}, x) \leq k(a-1)$, where $k = \lceil \log_a 2^r \rceil$. □

The following example will illustrate the above proposition and the method used in its proof.

Example 4.1.1 Consider $G = G(\{f_1 = 9x+3, f_2 = 9x+8\}, 2^{21} = 2097152)$ in which $a = 9$ and $d = 5$. We have $k = \lceil \log_9 2^{21} \rceil = 7$. By Proposition 4.1.1, if $x, y \in A = \{[f_2 g_1]^t(0) \bmod 2^{21} : t = 0, 1, \ldots\} = \{5t \bmod 2^{21} : t = 0, 1, \ldots\}$, then $d(x, y) \leq 2(8)(7) = 112$. Let $\overline{x} = (\frac{1}{2}(a-1)d, \ldots, \frac{1}{2}(a-1)d) = (4(5), \ldots, 4(5)) \equiv 1471660 \bmod 2^{21}$, and consider $x = (0, 8(5), 4(5), 5(5), 7(5), 2(5), 1(5)) \equiv 417183 \bmod 2^{21}$. We observe that $x = \overline{x} + (-4(5), 4(5), 0, 1(5), 3(5), -2(5), -3(5))$. To find an operator $[h]$ such that $[h](\overline{x}) = x$, we use the result of Proposition 3.3.1 and do the following steps:

$$\overline{x} \xrightarrow{[h_1]} \overline{x} + (-1(5), 1(5), 0, 1(5), 1(5), -1(5), -1(5))$$

$$\text{where } [h_1] = [f_1 f_1 f_2 f_2 f_1 f_2 f_1 g_2 g_1 g_1 g_1 g_1 g_2 g_2]$$

$$\xrightarrow{[h_2]} \overline{x} + (-2(5), 2(5), 0, 1(5), 2(5), -2(5), -2(5))$$

$$\text{where } [h_2] = [f_1 f_1 f_2 f_1 f_1 f_2 f_1 g_2 g_1 g_1 g_1 g_1 g_2 g_2]$$

$$\xrightarrow{[h_3]} \overline{x} + (-3(5), 3(5), 0, 1(5), 3(5), -2(5), -3(5))$$

$$\text{where } [h_3] = [f_1 f_1 f_2 f_1 f_1 f_2 f_1 g_2 g_1 g_1 g_1 g_1 g_1 g_2]$$

$$\xrightarrow{[h_4]} \overline{x} + (-4(5), 4(5), 0, 1(5), 3(5), -2(5), -3(5))$$

$$\text{where } [h_4] = [f_1^5 f_2 f_1 g_2 g_1 g_1^5]$$

Hence, we have $[h] = [h_4 h_3 h_2 h_1]$ which consists of 56 functions since each $[h_i]$, $i = 1, 2, 3, 4$, consists of 14 functions from the set $\{f_1, f_2, g_1, g_2\}$. We conclude that there exists a path from $\overline{x}$ to x of length 56. ◇

In general, the set A can presented in other ways. Since $[f_2 g_1](0) = d$ generates the whole set as a cyclic additive group, we have $A = \langle d \bmod 2^p \rangle = \langle -d \bmod 2^p \rangle = \{[g_2 f_1]^t(0) \bmod 2^p : t = 0, 1, \ldots\}$. This enables us to see the closed path traversing the elements of A in terms of the edges formed by g_2 and f_1. In the preceding proposition, for instance, we could use this last definition for A.

We observe that the closed path traversing the elements of A also traverses in between two elements of A a vertex not in A. In particular, if $x \in A$, then $g_1(x) \notin A$ is traversed by the path. Hence, we have the following corollary.

COROLLARY 4.1.1 *Let $G = G(\{f_1 = ax + b, f_2 = ax + b + d\}, 2^p)$ be a UM-LCG where $a \neq 1$ is odd. Define $A = \{[f_2 g_1]^t(0) \bmod 2^p : t = 0, 1, \ldots\}$, $g_1(A) = \{g_1 [f_2 g_1]^t(0) \bmod 2^p : t = 0, 1, \ldots\}$, and $A^* = A \cup g_1(A)$ where g_1 is the inverse of f_1 on Z_{2^p}. If $x, y \in A^*$, then $d(x, y) \leq 2(a-1)\lceil \log_a 2^p \rceil$.*

Proof. This follows from the fact that the closed path traversing the elements of A also traverses the elements of A^*. □

Other properties of A are given by the next proposition. But first we need the prove the following two lemmas.

LEMMA 4.1.1 *If $a = 2^i k + 1$ for some integer $i \geq 2$ and positive odd integer k, then for all nonnegative integer t, $a^t + 1$ is divisible by 2 but not by 4.*

Proof. By the Binomial Theorem, we have

$$a^t + 1 = (2^i k + 1)^t + 1 = 1 + \sum_{j=0}^{t} \binom{t}{j} (2^i k)^j$$

$$= 2 + \sum_{j=1}^{t} \binom{t}{j} (2^i k)^j = 2\{1 + \sum_{j=1}^{t} \binom{t}{j} 2^{ij-1} k^j\}.$$

□

LEMMA 4.1.2 *If $a = 2^i k + 1$ for some integer $i \geq 2$ and positive odd integer k, then $\frac{a^{2^j}-1}{a-1}$ is divisible by 2^j for any positive integer j.*

Proof. We use induction on j. If $j = 1$, then

$$\frac{a^{2^j} - 1}{a - 1} = \frac{a^2 - 1}{a - 1} = a + 1 = 2^i k + 2 = 2(2^{i-1} k + 1)$$

is divisible by $2^j = 2$.

If $j = 2$, then

$$\begin{aligned} \frac{a^{2^j} - 1}{a - 1} &= \frac{a^4 - 1}{a - 1} = a^3 + a^2 + a + 1 = a^2(a + 1) + (a + 1) \\ &= (a + 1)(a^2 + 1) = (2^i k + 2)(2^{2i} k^2 + 2^{i+1} k + 2) \end{aligned}$$

is divisible by $2^j = 4$.

In general, for any positive integer j, we have the following formula:

$$\begin{aligned} \frac{a^{2^j} - 1}{a - 1} &= \overbrace{a^{2^j-1} + \cdots + a^{2^{j-1}+1} + a^{2^{j-1}}}^{2^{j-1}} + \overbrace{a^{2^{j-1}-1} + \cdots + a + 1}^{2^{j-1}} \\ &= a^{2^{j-1}}(a^{2^{j-1}-1} + \cdots + a + 1) + (a^{2^{j-1}-1} + \cdots + a + 1) \\ &= (a^{2^{j-1}-1} + \cdots + a + 1)(a^{2^{j-1}} + 1) \end{aligned}$$

Assume that $\frac{a^{2^j}-1}{a-1}$ is divisible by 2^j for $j = 1, 2, \ldots, r$ for some r, and consider

$$\frac{a^{2^{r+1}} - 1}{a - 1} = (a^{2^{(r+1)-1}-1} + \cdots + a + 1)(a^{2^{(r+1)-1}} + 1).$$

By hypothesis, $(a^{2^r-1} + \cdots + a + 1) = \frac{a^{2r}-1}{a-1}$ is divisible by 2^r, and by Lemma 4.1.1, $(a^{2^r} + 1)$ is divisible by 2 but not by 4. Hence, $\frac{a^{2^{r+1}}-1}{a-1}$ is divisible by 2^{r+1}. By the hypothesis of induction, $\frac{a^{2^j}-1}{a-1}$ is divisible by 2^j for any positive integer j. □

PROPOSITION 4.1.2 *Let $G(\{f_1 = ax+b, f_2 = ax+b+d\}, 2^p)$ be a UM-LCG such that $a = 2^ik+1$, b is odd and $d = 2^jh$ where $i \geq 2$, $j > 0$ and h and k are positive odd integers. Define $A = \{[f_2g_1]^t(0) \bmod 2^p : t = 0, 1, \ldots\}$ and $f_1^s(A) = \{f_1^s(x) \bmod 2^p : x \in A\}$ for $s = 0, 1, \ldots$. Then*

(i) $A = f_1^{2^j}(A)$, and hence $f_1^r(A) = f_1^{2^j+r}(A)$ for any integer r.

(ii) $A \cap f_1^m(A) = \emptyset$ for all $m \in N$ such that $0 < m < 2^j$.

(iii) $f_1^t(A) \cap f_1^q(A) = \emptyset$ for integers t and q such that $0 \leq t < q < 2^j$. (In other words, A, $f_1(A)$, ..., $f_1^{2^j-1}(A)$ are pairwise disjoint.)

(iv) $V(G) = A \cup f_1(A) \cup \cdots \cup f_1^{2^j-1}(A)$.

Proof. *(i)* For any integer j we have $f_1^{2^j}(A) = \{f_1^{2^j}(x) \bmod 2^p : x \in A\} = \{a^{2^j}x + b(a^{2^j} - 1)/(a-1) \bmod 2^p : x \in A\}$. If $x \in A$, then x is divisible by 2^j by Proposition 2.3.3 (i). By Lemma 4.1.2, $(a^{2j} - 1)/(a-1)$ is divisible by 2^j. Hence, if $x \in A$ then $f_1^{2^j}(x) \in A$, i.e., $f_1^{2^j}(A) \subset A$. Since $f_1^{2^j}$ is a bijection, we have $|A| = |f_1^{2^j}(A)|$ and hence $A = f_1^{2^j}(A)$. Moreover, if r is any integer, we have $f_1^r(A) = f_1^r f_1^{2^j}(A) = f_1^{2^j+r}(A)$. (Note that $g_1(A) = f_1^{-1}(A)$ is the inverse of f_1 on Z_{2^p}.)

(ii) Let $m \in N$, $0 < m < 2^j$. If $x \in A$, then x is even and $f_1(x)$ is odd. This means that if m is odd, then $f_1^m(x) \cap A = \emptyset$. So let us assume that m is even. Then there exists an odd positive integer s and an integer $t \geq 1$ such that $m = 2^ts$. Since $m < 2^j$, we have $2^ts < 2^j$, or

$$t + log_2 s < j.$$

Now for any integer r, $2^jr \bmod n \in A$. We observe that

$$f_1^m(2^jr) = a^m 2^j r + \frac{b(a^m - 1)}{a-1}$$

where

$$\begin{aligned}\frac{a^m - 1}{a-1} &= \frac{a^{2^ts} - 1}{a-1} = a^{2^ts-1} + a^{2^ts-2} + \cdots + a^{2^{t-1}s} + a^{2^{t-1}s-1} + \cdots + a + 1 \\ &= (a^{2^{t-1}s} + 1)(a^{2^{t-1}s-1} + \cdots + a + 1)\end{aligned}$$

$$
\begin{aligned}
&= (a^{2^{t-1}s}+1)(a^{2^{t-2}s}+1)(a^{2^{t-2}s-1}+\cdots+a+1)\\
&\vdots\\
&= (a^{2^{t-1}s}+1)(a^{2^{t-2}s}+1)\cdots(a^{s}+1)(a^{s-1}+a^{s-2}+\cdots+a+1).
\end{aligned}
$$

The last term in the above expression is an odd integer because s is odd. By Lemma 4.1.1, each of the other t terms in the expression is divisible by 2 but not by 4. Therefore $\frac{a^m-1}{a-1}$ is divisible by 2^t but not by 2^{t+1}. But $t < j$, hence, $\frac{a^m-1}{a-1}$ is not divisible by 2^j. Therefore $f_1^m(2^j r) \bmod 2^p \notin A$ for any r, which implies that $A \cap f_1^m(A) = \emptyset$.

(iii) Suppose that $f_1^t(2^j r) \bmod 2^p \in f_1^q(A)$ for some integer r, where $2^j r \bmod 2^p \in A$. Then

$$
\begin{aligned}
& a^t 2^j r + b(a^{t-1}+\cdots+a+1) \bmod 2^p \in f_1^q(A)\\
\Longrightarrow\ & \text{there exists an integer } s \text{ such that}\\
& \quad a^t 2^j r + b(a^{t-1}+\cdots+a+1) \equiv a^q 2^j s + b(a^{q-1}+\cdots+a+1) \bmod 2^p\\
\Longrightarrow\ & a^t 2^j r \equiv a^t(a^{q-t}2^j s) + b(a^{q-1}+\cdots+a^t) \bmod 2^p\\
& \quad = a^t(a^{q-t}2^j s) + a^t b(a^{q-t-1}+\cdots+a+1) \bmod 2^p\\
\Longrightarrow\ & 2^j r \equiv (a^{q-t}2^j s) + b(a^{q-t-1}+\cdots+a+1) \bmod 2^p \text{ because } \gcd(a^t, 2^p) = 1.\\
\Longrightarrow\ & 2^j r \bmod 2^p \in f_1^{q-t}(A), \text{ where } 0 < q-t < 2^j\\
\Longrightarrow\ & A \cap f_1^{q-t}(A) \neq \emptyset.
\end{aligned}
$$

which is a contradiction to *(ii)*.

(iv) By *(iii)*, the sets $A, f_1(A), f_1^2(A), \ldots, f_1^{2^j-1}(A)$ are pairwise disjoint. Because f_1 is a bijection, we have $|A| = |f_1(A)| = \cdots = |f_1^{2^j-1}(A)|$. By Proposition 2.3.3 (i), $|A| = 2^{p-j}$. Hence, $|A \cup f_1(A) \cup f_1^2(A) \cup \cdots \cup f_1^{2^j-1}(A)| = |A| + |f_1(A)| + \cdots + |f_1^{2^j-1}(A)| = 2^j|A| = 2^j 2^{p-j} = 2^p$. Therefore, $V(G) = A \cup f_1(A) \cup \cdots \cup f_1^{2^j-1}(A)$. □

Each vertex of G is an element of a set $f_1^m(A)$ for some m, $0 \leq m < 2^j$. Hence, the implication of the preceding proposition is that we can get an upper bound on the distance between any two vertices in G if we know the distance between any two vertices in $f_1^m(A)$ and if we know how the sets A, $f_1(A)$, $\cdots$, $f_1^{2^j-1}(A)$ are interconnected. We will discuss this in more detail in the next section.

4.2 An Upper Bound on the Diameter of $G(\{ax+b, ax+b+d\}, 2^p)$

From Table 2.2, the graph $G = G(\{f_1 = ax + b, f_2 = ax + b + d\}, n = 2^p)$, where $a \neq 1$ is an odd integer, is connected if and only if one of the following conditions is satisfied:

1. d is odd
2. $a = 2^i k - 1$, b is odd and $d = 2h$ (where h is odd)
3. $a = 2^i k + 1$, b is odd and $d = 2^j h$ (where h is odd)

for $i \geq 2$, $j \geq 1$ and odd integers k and h. We will show that in each of these cases the upper bound on the diameter of G is of order $O(\log 2^p)$.

The bounds that we obtain are not necessarily close to the actual values of the diameter, but this is a significant progress in the search for the diameter of LCG's and related graphs. Because of the logarithmic nature of the bound, we can be sure that the diameter increases only in a logarithmic rate as the order of the graph is increased.

4.2.1 The case when d is odd

When d is odd, we have $A = \langle d \rangle = V(G)$ by Proposition 2.3.3 (i). By Lemma 4.1.1, if $x, y \in V(G)$, then $d(x,y) \leq 2(a-1)\lceil \log_a 2^p \rceil$. We have thus proved the following proposition.

PROPOSITION 4.2.1 *Let $G = G(\{ax+b, ax+b+d\}, 2^p)$ where $a \neq 1, d$ are odd integers and $b \in N$. Then*

$$Diam(G) \leq 2(a-1)\lceil \log_a 2^p \rceil.$$

Example 4.2.1 Let $G = G(\{f_1 = 9x+3, f_2 = 9x+8\}, n)$ where $n = 2^{21} = 2097152$, $a = 9$, $\lceil \log_9 2^{21} \rceil = 7$, and $d = 5$. Then $Diam(G) \leq 2(7)(8) = 112$.

If we change f_2 to $9x + (3 + 2^{10}(11) + 1) = 9x + 11268$, we will still have the same upper bound 112. ◇

Example 4.2.2 Let $G = G(\{f_1 = 7x + 3, f_2 = 7x + 11268\}, 2^{21})$ where $a = 7$, $\lceil \log_7 2^{21} \rceil = 8$, and $d = 2^{10}(11) + 1$. Then $Diam(G) \leq 2(6)(8) = 96$. ◇

4.2.2 The case when $a = 2^i k - 1$, b is odd and $d = 2h$

If $a = 2^i k - 1$ and $d = 2h$ for some odd integer h, by Proposition 2.3.3 (i) we have $A = \{[f_2 g_1]^t(0) \bmod 2^p : t = 0, 1, \ldots\} = \{2ht \bmod 2^p : t = 0, 1, \ldots\} = \{2t \bmod 2^p : t = 0, 1, \ldots\}$. Hence, A contains all the even integers in $V(G)$, while the set $g_1(A)$ contains all the odd one. Therefore, $V(G) = A \cup g_1(A)$. By Corollary 4.1.1, if $x, y \in V(G)$, then $d(x, y) \leq 2(a-1)\lceil \log_a 2^p \rceil$. We have proved the following:

PROPOSITION 4.2.2 *Let $G = G(\{ax + b, ax + b + d\}, 2^p)$ where $a = 2^i k - 1$, b is odd and $d = 2h$ for $0 < i \in N$ and odd integers k and h. Then*

$$Diam(G) \leq 2(a-1)\lceil \log_a 2^p \rceil.$$

Example 4.2.3 Let $G = G(\{f_1 = 7x + 3, f_2 = 7x + 3 + 6\}, 2^{21})$ where $a = 7$, $\lceil \log_7 2^{21} \rceil = 8$, and $d = 6$. Then $Diam(G) \leq 2(6)(8) = 96$. ◇

4.2.3 The case when $a = 2^k + 1$, b is odd and $d = 2^j h$

If $a = 2^i k + 1$, b is odd and $d = 2^j h$ for some $j \geq 1$ and odd integer h, consider the set $S = \{A, f_1(A), \ldots, f_1^{2^j - 1}(A)\}$, where $A = \{2^j t \bmod 2^p : t = 0, 1, \ldots\}$. By Proposition 4.1.2 (iii) and (iv), the elements of S are pairwise disjoint and that their union is equal to $V(G)$. Moreover, by Proposition 4.1.2 (i), $f_1^r(A) = f_1^{2^j + r}(A)$ for any integer r. In particular, $f_1^{-2^{j-1}}(A) = f_1^{2^j - 2^{j-1}}(A) = f_1^{2^{j-1}}(A)$. Hence, we also have

$$f_1^{-2^{j-1}}(A) = f_1^{2^{j-1}+1}(A)$$

$$f_1^{-2^{j-1}+2}(A) = f_1^{2^{j-1}+2}(A)$$

$$\vdots$$

$$f_1^{-2^{j-1}+(2^{j-1}-1)}(A) = f_1^{2^{j-1}+2^{j-1}-1}(A) = f_1^{2^j-1}(A).$$

So we can also write S as follows:

$$S = \{f_1^{-2^{j-1}+1}(A), f_1^{-2^{j-1}+2}(A), \ldots, f_1^{-1}(A), A, f_1(A), \ldots, f_1^{2^{j-1}-1}(A), f_1^{2^{j-1}}(A)\}.$$

Hence, for $x_\alpha \in f_1^\alpha(A)$ such that $\alpha \in \{-2^{j-1}+1, \ldots, -1, 0, 1, \ldots, 2^{j-1}\}$ we have $f_1^{-\alpha}(x_\alpha) \in f_1^0(A) = A$, and

$$d(x_\alpha, 0) \leq d(x_\alpha, f_1^{-\alpha}(x_\alpha)) + d(f_1^{-\alpha}(x_\alpha), 0) \leq |\alpha| + 2(a-1)\lceil \log_a 2^p \rceil$$

by the triangle inequality and Proposition 4.1.1 The maximum value of $|\alpha|$ is 2^{j-1}. Therefore, for any $x, y \in V(G)$, we have

$$d(x,y) \leq 2(\max_\alpha\{|\alpha| + 2(a-1)\lceil \log_a 2^p \rceil\}) = 2^j + 4(a-1)\lceil \log_a 2^p \rceil.$$

Hence, we have proved:

PROPOSITION 4.2.3 *Let $G = G(\{f_1 = ax + b, f_2 = ax + b + d\}, 2^p)$ where $a = 2^i k + 1$, b is odd and $d = 2^j h$ for some $i \geq 2$, $j > 0$ and odd integers k and h. Then*

$$Diam(G) \leq 2^j + 4(a-1)\lceil \log_a 2^p \rceil.$$

Example 4.2.4 Let $G = G(\{f_1 = 9x + 3, f_2 = 9x + 15\}, 2^{21})$ where $a = 9$, $d = 2^2(3) = 12$ and $\lceil \log_9 2^{21} \rceil = 7$. We have $Diam(G) \leq 4 + 4(7)(8) = 228$.

Note that if we change f_2 to $9x + 3 + (2^{10}11) = 9x + 11267$, where $2^j = 2^{10}$, we have $Diam(G) \leq 2^{10} + 224 = 1248$. ◇

4.3 Table of Upper Bounds

We summarize the results of Propositions 4.2.1-4.2.3 in Table 4.1.

a	b	d	Upper Bound on the Diameter of $G(\{ax+b, ax+b+d\}, n)$, where $n = 2^p$
2^ik+1 $(i \geq 2)$ (k is odd)	odd	odd	$2(a-1)\lceil \log_a n \rceil$
		2^jh $(j \geq 1)$ (h is odd)	$2^j + 4(a-1)\lceil \log_a n \rceil$
	even	odd	$2(a-1)\lceil \log_a n \rceil$
2^ik-1 $(i \geq 2)$ (k is odd)	odd	odd	$2(a-1)\lceil \log_a n \rceil$
		$2h$ (h is odd)	$2(a-1)\lceil \log_a n \rceil$
	even	odd	$2(a-1)\lceil \log_a n \rceil$

Table 4.1: The upper bound on the diameter of a UM-LCG with 2 generators

Chapter 5

THE GENERAL CLASSES OF LCG's

Let $n = 2^p, a, b, c, d \in N$ such that $a \neq 1$ and $c \neq 1$ are odd. The generators $f_1 = ax + b$ and $f_2 = cx + d$ of an LCG on n vertices, where a and c are not necessarily equal, can be classified in general as commutative or noncommutative. We say that f_1 and f_2 are **commutative generators** if for any vertex x we have $f_1 f_2(x) \equiv f_2 f_1(x) \bmod n$; otherwise, we say that they are **noncommutative**. A necessary and sufficient condition for j_1 and f_2 to be commutative is that $ad+b \equiv ac+d \bmod n$. This is because $f_1 f_2(x) = f_1(cx+d) = acx+ad+b$, and $f_2 f_1(x) = f_2(ax+b) = acx+cb+d$.

The first two sections of this chapter deal with these two types of generators. In Section 5.1 we apply the results that we have from Chapter 4 in order to obtain an upper bound for the diameter of some LCG's having noncommutative generators. In Section 5.2 we discuss a lower bound for the diameter of LCG's with commutative generators. Then in Section 5.3 we discuss the recursive property of the LCG family.

5.1 LCG's with Noncommutative Generators

The generators f_1 and f_2 of the graph $G = G(\{f_1, f_2\}, n)$ are noncommutative if and only if $ad + b \not\equiv cb + d \bmod n$. Hence, in this case, we can consider the graph

$H = G(\{h_1, h_2\}, n)$, where $h_1 = f_1f_2 = acx + ad + b$ and $h_2 = f_2f_1 = acx + cb + d$, as a UM-LCG generated by two distinct functions. We observe that the generators have constants of the same parity and are invertible because they have an odd multiplier. Two vertices in H are adjacent if and only if in G they are connected by a path of length 2 via the composite functions f_1f_2, f_2f_1, g_1g_2 or g_2g_1, where g_1 and g_2 are the inverse functions of f_1 and f_2, respectively.

By definition, if H is connected then G is also connected. However, the converse is not true. For example, if $n = 32$ and G has the generators $f_1 = 3x+1$ and $f_2 = 5x+7$, then H has the generators $h_1 = 15x + 22$ and $h_2 = 15x + 12$. We see from Figure 5.1 and Figure 5.2 that, indeed, G is connected but H is not. This classification of H is consistent with Table 2.2.

Now, suppose that H is connected and $x, y \in V(H)$. Denote the inverses of h_1 and h_2 by h_1^{-1} and h_2^{-1}, respectively. If $d(x, y) = k$ in H for some k, then there exists a string of functions $\theta_1, \theta_2, \ldots, \theta_k$ from the set $\{h_1, h_2, h_1^{-1}, h_2^{-1}\}$ such that $y \equiv \theta_1\theta_2\cdots\theta_k(x) \bmod n$. But $\{h_1, h_2, h_1^{-1}, h_2^{-1}\} = \{f_1f_2, f_2f_1, (f_1f_2)^{-1}, (f_2f_1)^{-1}\} = \{f_1f_2, f_2f_1, g_2g_1, g_1g_2\}$. Hence, x and y are connected in G such that $y \equiv \theta_1\theta_2\cdots\theta_k(x)$ mod n where $\theta_1, \theta_2, \ldots, \theta_k \in \{f_1f_2, f_2f_1, g_2g_1, g_1g_2\}$, i.e. the distance of x and y in G is at most $2k$. This means that if $UBD(H)$ and $UBD(G)$ are the upper bounds on the diameters of H and G, respectively, then $UBD(G) \leq 2\{UBD(H)\}$.

In summary, we have

PROPOSITION 5.1.1 *Let $G = G(\{f_1 = ax + b, f_2 = cx + d\}, 2^p)$ be a connected LCG such that f_1 and f_2 are noncommutative. Define $H = G(\{h_1 = f_1f_2, h_2 = f_2f_1\}, 2^p)$. If H is connected, then*

$$UBD(G) \leq 2\{UBD(H)\}$$

where $UBD(G)$ and $UBD(H)$ are the upper bounds on the diameter of G and H, respectively.

Thus, if there is a logarithmic formula for $UBD(H)$, then there is also a logarithmic bound on the diameter of G. Table 5.1 gives us the diameter upper bound of G whenever H is connected.

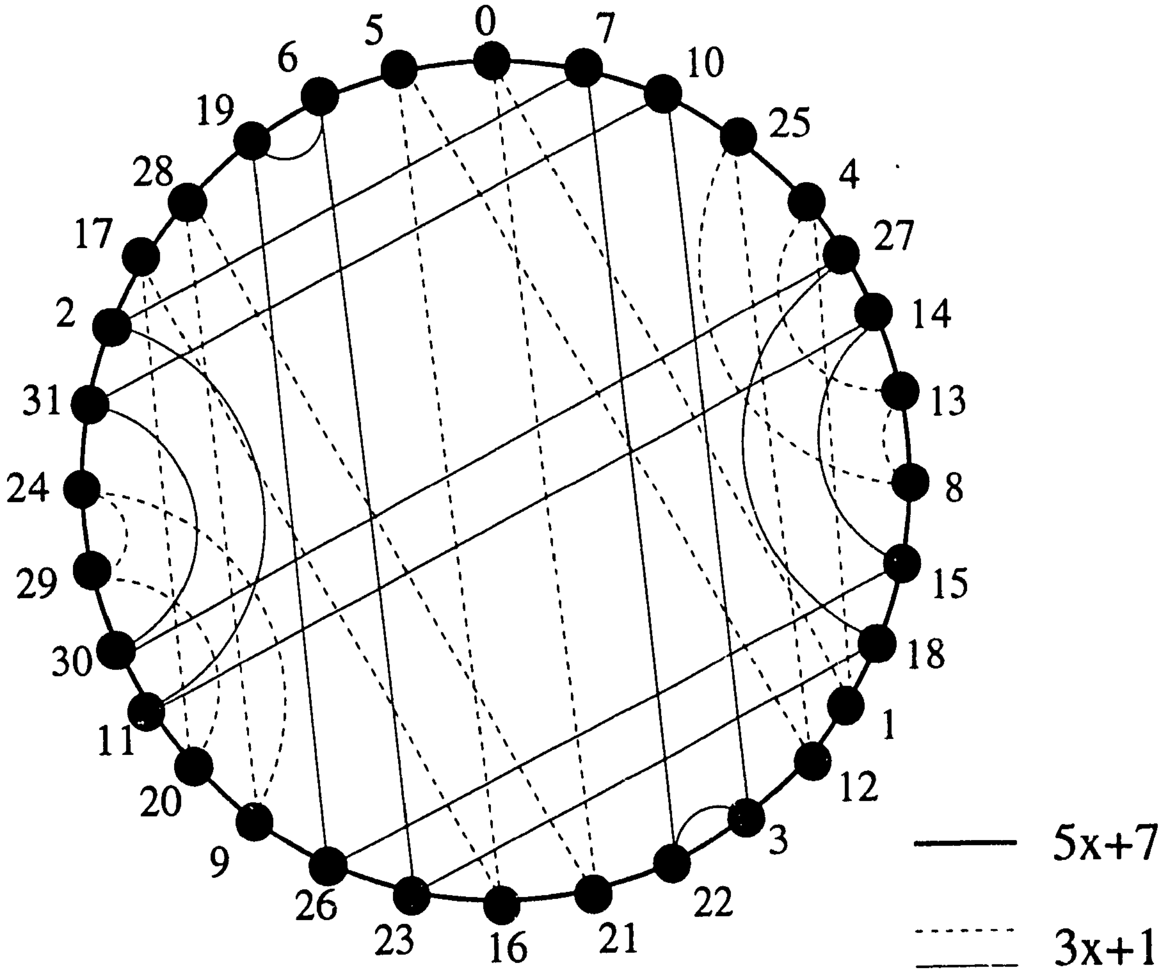


Figure 5.1: $G = G(\{f_1 = 3x + 1, f_2 = 5x + 7\}, 32)$

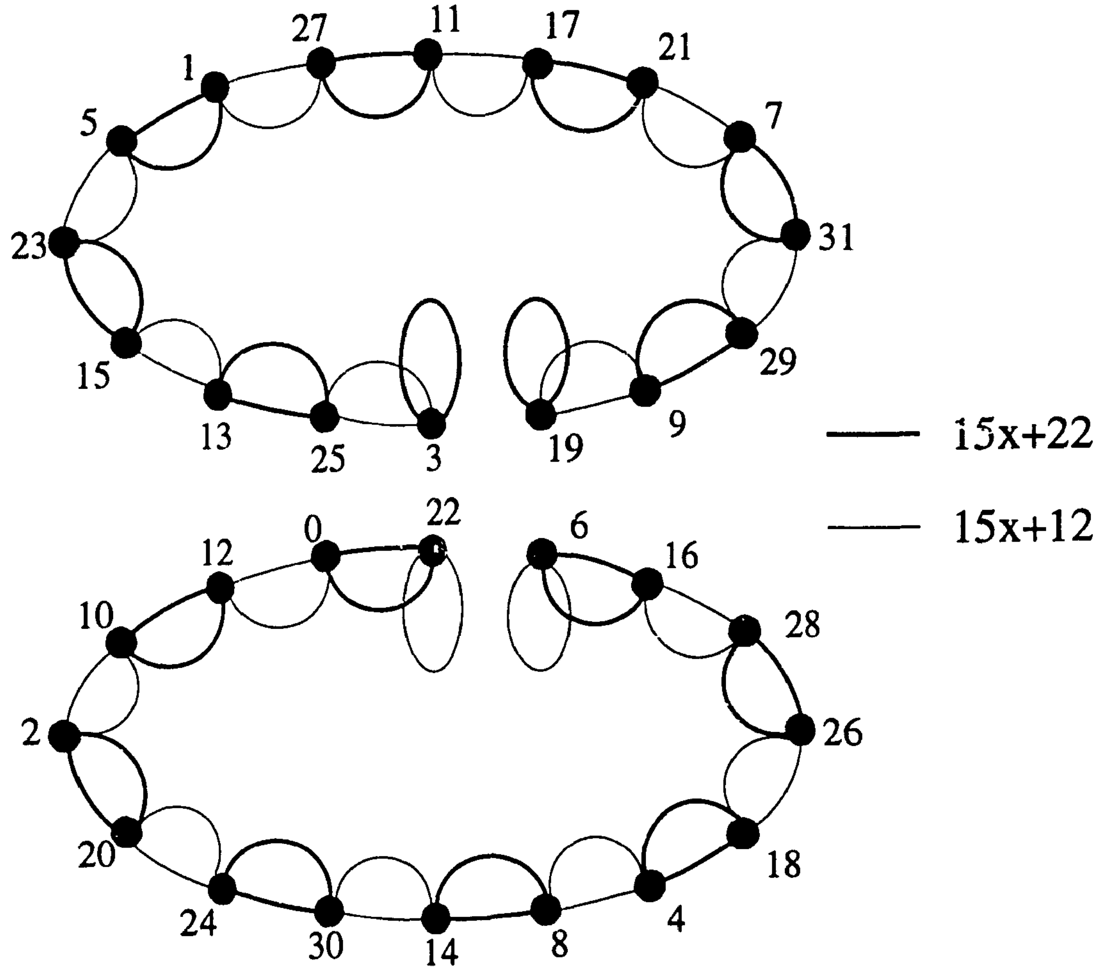


Figure 5.2: $H = G(\{h_1 = 15x + 22, h_2 = 15x + 12\}, 32)$

Case when H is connected	upper bound on the diameter of H	upper bound on the diameter of G
$ac - 1 \neq 0$ is divisible by 4 $ad + b$ is odd $ad + b - cb - d = 2^j h$ (where $j \geq 1$, h is odd)	$2^j + 4(ac-1)\lceil p \log_{ac} 2 \rceil$	$2^{j+1} + 8(ac-1)\lceil p \log_{ac} 2 \rceil$
$ac - 1 \neq 0$ is divisible by 2 but not by 4 $ad + b$ is odd $ad + b - cb - d = 2h$ (where h is an odd integer)	$2(ac-1)\lceil p \log_{ac} 2 \rceil$	$4(ac-1)\lceil p \log_{ac} 2 \rceil$

Table 5.1: Upper bounds on the diameters of $H = G(\{acx + ad + b, acx + cb + d\}, 2^p)$ and $G = G(\{ax + b, ax + b + d\}, 2^p)$

5.2 LCG's with Commutative Generators

The key element to obtain a logarithmic upper bound on the diameter of an LCG G with noncommutative generators f_1 and f_2 is the possibility of transforming this case into that of a UM-LCG H with distinct generators $h_1 = f_1f_2$ and $h_2 = f_2f_1$. If f_1 and f_2 are commutative, then $h_1 \equiv h_2 \bmod n$ and H can have a diameter as large as $n/2$. Consequently, G can have a diameter upper bound as large as n. In this regard there is no meaningful generalization for the diameter upper bound of G when its generators are commutative.

In this section, however, we will discuss a method which gives a diameter lower bound for G which is proportional to $\sqrt{n}$ if G has commutative generators.

First we observe that the commutativity of f_1 and f_2 is inherited by their inverses g_1 and g_2. We have $f_1f_2 \equiv f_2f_1 \bmod n \Rightarrow (f_1f_2)^{-1} \equiv (f_2f_1)^{-1} \bmod n \Rightarrow g_2g_1 \equiv g_1g_2 \bmod n$. Moreover, $g_2g_1 \equiv g_1g_2 \bmod n \Rightarrow (f_1g_2)g_1 \equiv g_2 \bmod n$. Since $g_2 = (g_2f_1)g_1$, we must then have $f_1g_2 \equiv g_2f_1 \bmod n$. Similarly, $f_2g_1 \equiv g_1f_2 \bmod n$. Hence, if f_1 and f_2 are commutative, for any sequence of functions $h_1h_2\cdots h_m$, where $h_i \in \{f_1, f_2, g_1, g_2\}$ with $i = 1, 2, \ldots, m$, we have

$$h_1h_2\cdots h_m(x) = \underbrace{\theta_1\cdots\theta_1}_{m_1}\underbrace{\theta_2\cdots\theta_2}_{m_2}$$

where $\theta_1 \in \{f_1, g_1\}$ and $\theta_2 \in \{f_2, g_2\}$ and m_1, m_2 are integers such that $m_1 + m_2 \leq m$.

The consequence of this in the graph G is that any vertex can be reached from a fixed vertex x using the composition function $\theta_1^{m_1}\theta_2^{m_2}$. Hence, using x as the reference vertex, each vertex of G is represented in one or more of the following forms:

- $f_1^{m_1}f_2^{m_2}(x)$
- $f_1^{m_1}g_2^{m_2}(x)$
- $g_1^{m_1}f_2^{m_2}(x)$
- $g_1^{m_1}g_2^{m_2}(x)$.

Let us define an f_1f_2-*path of length* m *from* x *to* $f_1^{m_1}f_2^{m_2}(x)$, where $m_1 + m_2 = m$, to be the path $x \to f_2(x) \to \cdots \to f_2^{m_2}(x) \to f_1f_2^{m_2}(x) \to \cdots \to f_1^{m_1}f_2^{m_2}(x) \bmod n$. For example, the f_1f_2-path of length 5 from x to $f_1^2f_2^3(x)$ is given by $x \to f_2(x) \to f_2^2(x) \to f_2^3(x) \to f_1f_2^3(x) \to f_1^2f_2^3(x) \bmod n$. Since the value of m_1 can run from 0 to m, we see that there are exactly $m+1$ distinct f_1f_2-paths of length m. Hence, the number of distinct f_1f_2-paths of length from 1 to m is given by

$$2+3+4+\cdots+m+(m+1) = \frac{m(m+3)}{2}$$

which is also the number of distinct f_1g_2-, g_1f_2- and g_1g_2-paths of length from 1 to m.

If $D = Diam(G)$, then from x the total number of distinct $\theta_1\theta_2$-paths of length at most D is given by

$$4\{\frac{1}{2}D(D+3)\} = 2D(D+3).$$

Because D is the maximum distance of any vertex from x, all the n vertices of G are reachable from x using $\theta_1\theta_2$-paths of length at most D. Hence, we have the following inequality:

$$2D(D+3) \geq n.$$

Solving for D, we have:

$$D \geq \sqrt{\tfrac{n}{2}+\tfrac{9}{4}} - \tfrac{3}{2}.$$

In summary, we have the following proposition for $n = 2^p$:

PROPOSITION 5.2.1 *Let* $G = G(\{f_1, f_2\}, 2^p)$ *where* f_1 *and* f_2 *are commutative linear functions modulo* 2^p*. Then*

$$Diam(G) \geq \sqrt{2^{p-1} + \tfrac{9}{4}} - \tfrac{3}{2}.$$

This lower bound compares well with the result from [3, 6, 28, 30] that the lower bound for the diameter of the graph $G(\{x+s_1, x+s_2\}, 2^p)$ for any integers s_1 and s_2 is

$$\sqrt{2^{p-1} - \tfrac{1}{4}} - \tfrac{1}{2}.$$

As a matter of fact, we have

$$\sqrt{2^{p-1}+\tfrac{9}{4}}-\tfrac{3}{2}\leq\sqrt{2^{p-1}-\tfrac{1}{4}}-\tfrac{1}{2}$$

for all positive values of p.

For small values of n, $\sqrt{n}$ and $\log n$ are essentially not very different. But the difference between these figures is very large if n is very large as seen from the fact that $\lim_{n\to\infty}(\log n/\sqrt{n}) = 0$. Thus, when we aim to obtain a linear congruential graph having a diameter of logarithmic bound for a large order n, we should consider the ones that have noncommutative generators. This is a reiteration of a statement from [22] and [21].

We give as an example the degree-4 DCC-LCG as given in [22]. The DCC-LCG's with degree greater than 4 have noncommutative generators, but here we show that those with degree 4 have commutative generators. Hence we can compute for the lower bound on their diameters.

Example 5.2.1 Let $n = 2^p$. A degree-4 DCC linear congruential graph G on n vertices is generated by $f_1 = ax + b$ and $f_2 = cx + d$, where $a = 2^2q + 1$, $b = 2r + 1$, $c = 2^3q + 1$ and $d = 2(2r + 1)$ for some positive integers q and r. We observe that

$$\begin{aligned} ad+b &= (2^2q+1)2(2r+1)+(2r+1) \\ &= (2r+1)(2(2^2q+1)+1) \\ &= (2r+1)(2^3q+3) \end{aligned}$$

and

$$\begin{aligned} cb+d &= (2^3q+1)(2r+1)+2(2r+1) \\ &= (2r+1)(2^3q+1+2) \\ &= (2r+1)(2^3q+3). \end{aligned}$$

Hence, f_1 and f_2 are commutative. By Proposition 5.2.1, we have $Diam(G) \geq \sqrt{2^{p-1}+\frac{9}{4}}-\frac{3}{2}$. ◇

In the next example we extend our result to the known results when the multiplier is equal to 1.

Example 5.2.2 Let $G = G(\{f_1, f_2\}, 2^p)$. If the generators are given by $f_1 = x + 1$ and $f_2 = x + d$, then they are commutative. Here we have $a = 1$, $b = 1$, $c = 1$ and $ad + b = d + 1 = d + cb$. By Proposition 5.2.1, $Diam(G) \geq \sqrt{2^{p-1} + \frac{9}{4}} - \frac{3}{2}$. Recall that Hsu and Shapiro [14] showed that the upper bound for the diameter of G is given by $\sqrt{2^{p-1}} + \sqrt[4]{2^{p-3}} + 2$. Hence, for specific values $p = 10$, 15 and 20, the diameter of G falls in the intervals $(21, 27)$, $(126, 138]$ and $(722, 746)$, respectively. $\diamond$

5.3 Recursive Property of LCG's

It is known from [22] that the DCC-LCG on 2^{p+1} vertices generated by a set F of linear functions can be constructed from two copies of DCC-LCG on 2^p vertices generated by the same set F. The same is true, as shown in [21], for an LCG in which there is a function that generates all the vertices. In what follows we will discuss some properties that will allow us to generalize this construction for LCG's generated by functions with odd multipliers on n vertices, where n is any positive integer.

PROPOSITION 5.3.1 *Let $G_n = G(F, n)$ where $n \in N$ and F is a set of linear congruential functions with odd multipliers $< n$. Suppose $(x, y) \in E(G_n)$ such that $y \equiv f(x) \bmod n$ where $f(x) = ax + b \in F$.*

(i) If $0 \leq f(x) \bmod 2n < n$, then $(x, y), (x + n, y + n) \in E(G_{2n})$.

(ii) If $n \leq f(x) \bmod 2n$, then $(x, y), (x+n, y+n) \notin E(G_{2n})$ but $(x, y+n), (x+n, y) \in E(G_{2n})$.

Proof. *(i)* The first assertion is obvious since $y \equiv f(x) \bmod n = f(x) \bmod 2n$. Now, $f(x + n) = ax + an + b = f(x) + an = f(x) + n + (a - 1)n$. Hence,

$$\begin{aligned} f(x+n) \bmod 2n &= (f(x) + n + (a-1)n) \bmod 2n \\ &= (f(x) \bmod 2n + n \bmod 2n + (a-1)n \bmod 2n) \bmod 2n \end{aligned}$$

$$\begin{aligned} &= (f(x) \bmod n + n \bmod 2n + 0) \bmod 2n \\ &\quad \text{since } (a-1) \text{ is even} \\ &= (y + n \bmod 2n) \bmod 2n \\ &= (y+n) \bmod 2n. \end{aligned}$$

By definition, $f(x+n) \equiv (y+n) \bmod 2n$ if and only if $(x+n, y+n) \in E(G_{2n})$.

(ii) $n \leq f(x) \bmod 2n$ and $y \equiv f(x) \bmod n$ if and only if there exists an integer k such that

$$f(x) = y + (2k+1)n = y + 2kn + n \tag{5.1}$$

Hence, $y \not\equiv y + n \equiv f(x) \bmod 2n$. Therefore $(x, y) \notin E(G_{2n})$ but $(x, y+n) \in E(G_{2n})$.

Now, we have $f(x+n) = ax + b + an = f(x) + an$. By formula 5.1, there is an integer k such that

$$\begin{aligned} f(x+n) \bmod 2n &= (y + 2kn + n + an) \bmod 2n \\ &= (y + 2kn + n(a+1)) \bmod 2n \\ &= y \bmod 2n. \end{aligned}$$

Hence, $(x+n, y) \in E(G_{2n})$. However, since $y \not\equiv y+n \bmod 2n$, $(x+n, y+n) \notin E(G_{2n})$.

□

Using the above proposition, we can now have:

Construction 5.3.1 *Let $n \in N$ and $G_n = G(F, n)$ where F is a family of linear functions with odd multipliers. We can construct G_{2n} from two copies of G_n in the following manner:*

1. *Relabel each vertex on the second copy of G_n by adding n.*

2. *If $(x, y) \in E(G_n)$ such that $n \leq f(x) \bmod 2n$, then replace (x, y) and its copy $(x+n, y+n)$ by $(x, y+n)$ and $(x+n, y)$, respectively.*

Example 5.3.1 We illustrate the above construction using $F = \{11x + 8, 7x + 3\}$ with $n = 25$. In Figure 5.3 we have the graph G_{25} in which the edges to be replaced are drawn concave upward. In Figure 5.4 these edges and their copies are replaced to construct G_{50}. ◇

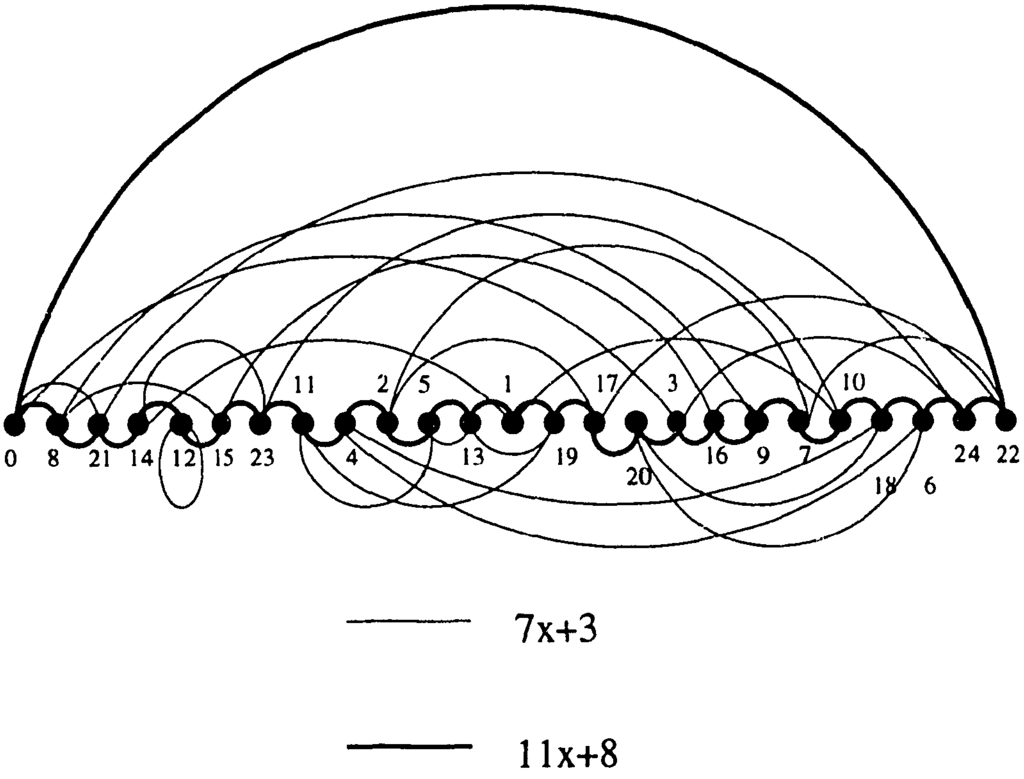


Figure 5.3: $G(\{11x+8, 7x+3\}, 25)$

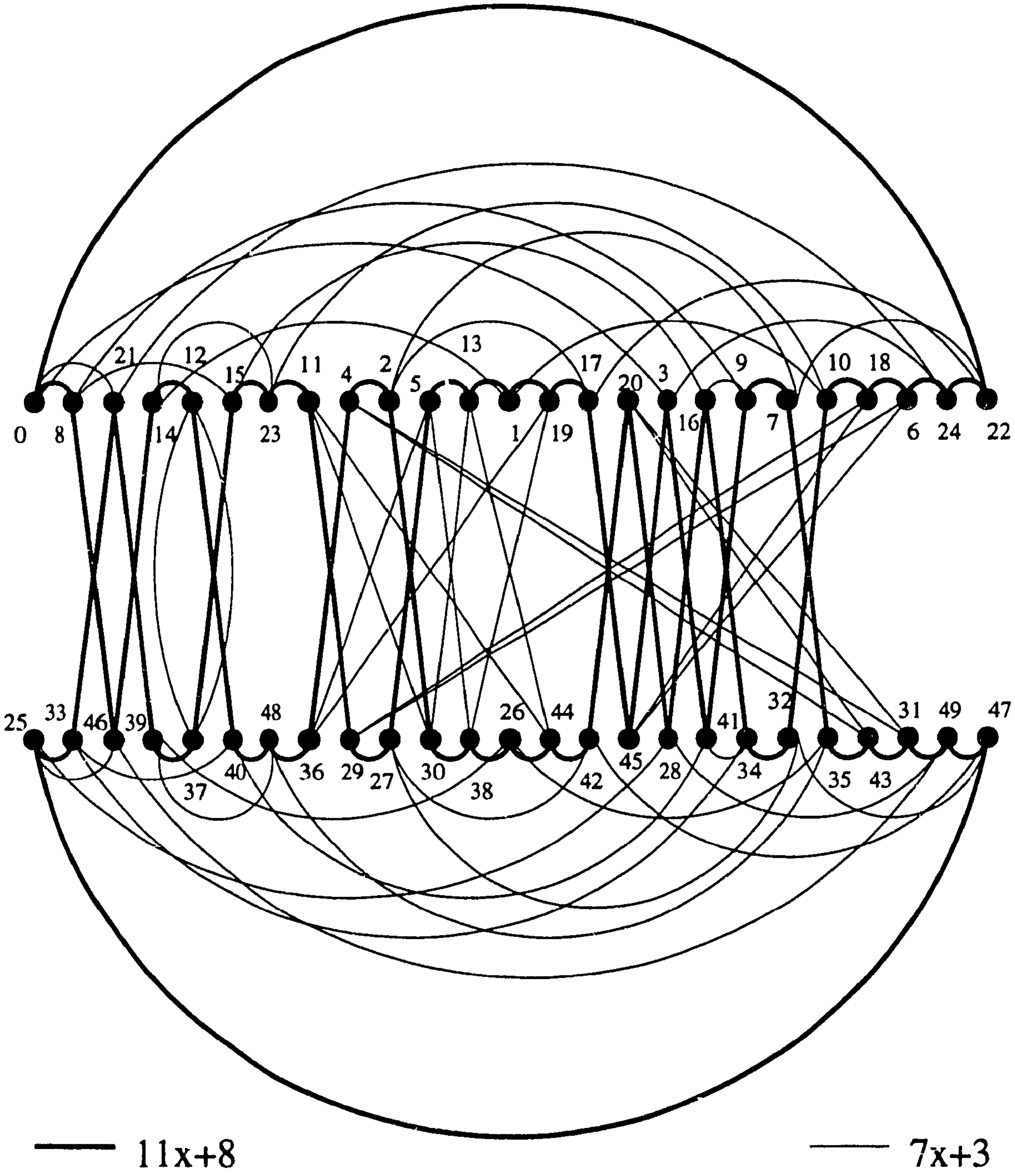


Figure 5.4: $G(\{11x+8, 7x+3\}, 50)$

Bibliography

[1] R. Beivide, V. Viñals, and C. Rodriguez. Optimal topologies with four bidirectional links and its applications. In *Proc. IAESTED Int. Symp. AI87*, pages 66–69, Grindelwald, Switzerland, 1987.

[2] J. C. Bermond, F. Comellas, and D. F. Hsu. Distributed loop computer networks: A survey. *Journal of Parallel and Distributed Computing*, 24:2–10, 1995.

[3] J. C. Bermond, G. Illiades, and C. Peyrat. An optimization problem in distributed loop computer networks. In *Third International Conference on Combinatorial Math.*, New York, USA, June 1985. Ann. New York Acad. Sci. **555**(1989), 45–55.

[4] J.-C. Bermond and C. Peyrat. The de bruijn and kautz networks, a competition for the hypercube and distributed computers. In *Proc. First European Workshop on Hypercubes*, pages 279–293, Amsterdam, October 1989. Elsevier/North Holland.

[5] F. Boesch and R. Tindell. Circulants and their connectivity. *J. Graph Theory*, 8:487–499, 1984.

[6] F. T. Boesch and J. K. Wang. Reliable circulant networks with minimum transmission delay. *IEEE Trans. Circuits Syst.*, CAS32:1286–1291, 1985.

[7] J. A. Bondy and U. S. R. Murty. *Graph Theory with Applications*. The Macmillan Press Ltd., 1976.

[8] F. R. K. Chung. Diameters of graphs: Old problems and new results. *Congressus Numcrantium*, 60:295-317, 1987.

[9] P. Erdős and D. F. Hsu. Distributed loop networks with minimum transmission delay. *Theoretical Computer Science*, 100:223-241, 1992.

[10] M. A. Fiol, J. L. Yebra, I. Alegre, and M. Valero. A discrete optimization problem in local networks and data alignment. *IEEE Trans. Comput.*, C36:702-713, 1987.

[11] A. Gioia. *The Theory of Numbers, An Introduction.* Markham Publishing Company, Chicago, 1970.

[12] A. Grnarov, L. Kleinrock, and M. Gerla. A highly reliable distributed loop network architecture. In *1980 Int. Symp. Fault-Tolerance Comput.*, pages 319-324, Kyoto, Japan, 1980.

[13] M. C. Heydemann, J. Opatrny, and S. D. Embeddings of hypercubes and grids into de bruijn graphs. *Journal of Parallel and Distributed Computing*, 23:104-111, 1994.

[14] D. F. Hsu and J. Shapiro. Bounds for the minimal number of transmission delays in double loop networks. *J. Combin. Inform. System Sci.*, 16:55-62, 1991.

[15] T. W. Hungerford. *Algebra (Graduate Texts in Mathematics).* Springer-Verlag, New York, 1974.

[16] F. K. Hwang and Y. H. Xu. Double loop networks with minimum delay. *Discrete Mathematics*, 66:109-118, 1987.

[17] M. Imase and M. Itoh. Design to minimize diameter on building-block network. *IEEE Trans. Comput.*, C30:439-442, 1981.

[18] D. E. Knuth. *The Art of Computer Programming, Seminumerical Algorithms*, volume II. Addison-Wesley, 1972.

[19] F. T. Leighton. *Introduction to Parallel Algorithms and Architectures: Arrays, Trees, Hypercubes.* Morgan Kaufmann Publishers, San Mateo, California, 1992.

[20] Marsaglia. The structure of linear congruential sequences. In Z. Zurenba, editor, *Application of Number Theory to Numerical Analysis*, pages 249–285, New York, 1972. Academic Press.

[21] J. Opatrny and D. Sotteau. Linear congruential graphs. *Graph Theory, Combinatorics, Algorithms and Applications, SIAM Proceedings Series*, pages 404–426, 1991.

[22] J. Opatrny, D. Sotteau, N. Srinivasan, and K. Thulasiraman. DCC linear congruential graphs: A new class of interconnection networks. *IEEE Trans. on Computers*, (to appear).

[23] C. Raghavendra, M. Gerla, and A. Avizienis. Reliable loop topologies for large local computer networks. *IEEE Trans. Comput.*, C(34):46 55, 1985.

[24] C. S. Raghavendra and M. Gerla. Optimal loop topologies for distributed systems. In *7th Data Communication Symposium*, pages 218-223, Mexico City, 1981.

[25] C. S. Raghavendra, M. Gerla, and D. S. Parker. Multi-connected loop topologies for local computer networks. In *Conf. INFOCOM 82*, 1982.

[26] S. M. Reddy, D. K. Pradham, and J. Kuhl. Directed graphs with minimal diameter and maximal connectivity. Technical report, School of Engineering, Oakland University, 1980.

[27] J. Wolf and M. T. Liu. A distributed double-loop computer network. In *7th Texas Conf. Comput. Systems*, pages 6.29-6.34, 1978.

[28] J. Wolf, B. Weide, and M. T. Liu. Analysis and simulation of the distributed double loop network. Ir *Comput. Networking Symp. NBS*, pages 82-89, 1979.

[29] C. K. Wong and D. Coppersmith. A combinatorial problem related to multimode memory organizations. *J. Assoc. Comput. Mach.*, 21:392–402, 1974.

[30] J. L. A. Yebra, M. A. Fiol, and P. Morillo. The diameter of undirected graphs associated to plane tessellations. *Ars. Combin.*, 20B:159–171, 1985.