EXTREMAL CAYLEY GRAPHS

THESIS

Presented to the Graduate Council of
Texas State University-San Marcos
in Partial Fulfillment
of the Requirements

for the Degree

Master of SCIENCE

by

Joni J. Schneider, B.S.

San Marcos, Texas
August 2012

FAIR USE AND AUTHOR'S PERMISSION STATEMENT

Fair Use

Duplication Permission

ACKNOWLEDGEMENTS

Many people have helped in the development of this thesis. I would like to thank the committee members for reading through the thesis and giving me many helpful comments, suggestions, and corrections. A special thanks goes to Abby Gail Mask for her support, encouragement, and time spent helping with calculations. And most importantly, I would like to thank Dr. Xingde Jia. Without his assistance and support, this thesis would not have been possible. Over the years, he has been a great teacher and advisor, and now he is someone I would call a great friend.

This manuscript was submitted on 15 April 2012.

TABLE OF CONTENTS

LIST OF TABLES

TABLE **Page**

LIST OF FIGURES

ABSTRACT

EXTREMAL CAYLEY GRAPHS

by

Joni J. Schneider, M.S.

Texas State University-San Marcos

August 2012

SUPERVISING PROFESOR: XINGDE JIA

Let Γ be a finite group with m elements. Let A be a nonempty subset of Γ. The *Cayley digraph* of Γ generated by A, denoted by $\mathrm{Cay}(\Gamma, A)$, is the digraph with vertex set Γ and arc set $\{uv \mid u^{-1}v \in A\}$. A simple example of a Cayley digraph is the n-Cube.

A Cayley digraph can be considered as a graphical representation of a finite group by its generating set. Cayley digraphs of finite abelian groups are often used to model communication networks. Because of their complex algebraic structure and their applications in network theory, Cayley digraphs have been studied extensively in recent years. In this thesis, we focus on some optimization problems about Cayley digraphs. In particular, we study how large the number of vertices a Cayley digraph can have for a

given diameter and degree. This is one of the central problems in the study of extremal Cayley digraphs.

Let $\mathbb{Z}_m$ denote the cyclic group of residue classes of integers modulo m with addition. Given any two positive integers d and k, define $m(d,k)$ as the largest positive integer m such that there exists a set A of k integers with $\mathrm{diam}(\mathrm{Cay}(\mathbb{Z}_m, A)) \leq d$, where $\mathrm{diam}(G)$ denotes that diameter of a graph G. In other words,

$$m(d,k) = \max_{\substack{A \\ |A|=k}} \{m \mid \mathrm{diam}(\mathrm{Cay}(\mathbb{Z}_m, A)) \leq d\}.$$

We will study this extremal function. In particular, we will prove a lower bound for $m(d,k)$.

We will introduce a geometric representation of $\mathbb{Z}_m$ with respect to a generating set A. This representation was first introduced by C. K. Wong and Don Coppersmith in 1974. This geometric representation of $\mathbb{Z}_m$ is very useful in establishing upper bounds for $m(d,k)$. We will discuss some properties of the A-representation of $\mathbb{Z}_m$ in two and three dimensional cases. We will also use this method to prove upper bounds for $m(d,2)$. Some other related extremal functions will also be studied in this thesis.

Chapter 1

INTRODUCTION

1.1 Information Networks

A network is traditionally referred to as a computer network which is a collection of hardware components and computers interconnected by communication channels that allow sharing of resources and information. However, a network can consist of a variety of entities (or nodes) such as computers, cellphones, televisons, fire alarms, and refrigerators. It can also consist of people, organizations, companies, and nations. A network has emerged as a necessary mechanism to exchange information between various sources. As such, network takes a new name, which is modern and meaningful: *information networks*.

Information networks have played a crucial role in the function of the information society. There are two types of information networks: one is called *natural networks* and the other is *designed networks*. These networks have to be robust, efficient, reliable, and cost effective. Therefore, the design of such information networks is extremely important.

Graphs are often used to model information networks. In fact, a network is a graph where the nodes of the network are represented by the vertices and the network links by the edges of the graph.

A major concern in the design of networks is the balance between some key parameters of the network, namely:

n—the size of the network,

d—the transmission delay, and

k—the number of links each node can have.

With a fixed number of nodes to connect, the transmission delay can be decreased by adding more links to the network. However, more links might result in lower performance because of physical restraints. Therefore, designs to optimize these parameters are extremely desirable in the construction of networks. Extensive research has been done in this area by both computer scientists and mathematicians (see, e.g. Bermond, Comellas and Hsu (1995) and Du and Hsu (1996)).

1.2 Cayley Graphs

Another key issue in designing communication networks is reducing the complexity of massively parallel processing systems. Symmetric graphs can be used to model networks so that the same routing algorithms apply to all the vertices. A good example would be the hypercube, a popular communication network design noted for its symmetry and expandability. However, recent studies have shown that optimal *Cayley digraphs* constructed by using groups can outperform hypercubes and other popular network topologies in terms of capacity and efficiency of the network.

Definition 1. Let Γ be a finite group with m elements. Let A be a nonempty subset of Γ. The *Cayley digraph* of Γ generated by A, denoted by $\mathrm{Cay}(\Gamma, A)$, is the digraph with vertex set Γ and arc set $\{uv \mid u^{-1}v \in A\}$.

For any given positive integer m, let $\mathbb{Z}_m$ denote the set of residue classes modulo m. We also use $\mathbb{Z}_m$ to denote the cyclic group of residue classes modulo m under addition. As shown in Figure 1.1, a 3-cube has 8 vertices with degree 3 and diameter 3, while the Cayley digraph of $\mathbb{Z}_{12}$ generated by $A = \{\pm 1, \pm 6\}$, as an undirected graph,

has 12 vertices, degree 3 and diameter 3. It is also easy to verify that Cayley digraph of $\mathbb{Z}_{41}$ generated by $\{\pm 11, \pm 17\}$ has degree 4 and diameter 4. Note that the Cayley graph has 41 vertices while a 4-cube has only 16 vertices with the same degree 4 and same diameter 4.

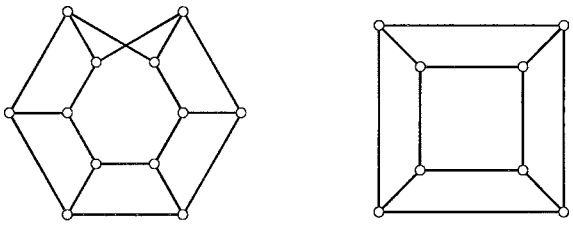


Figure 1.1: Two 3-regular graphs have the same diameter 3.

Let $\mathbb{Z}_m$ denote the cyclic group of residue classes modulo m with addition. Given any two positive integers d and k, define $m(d,k)$ as the largest positive integer m such that there exists a set A of k integers with $\mathrm{diam}(\mathrm{Cay}(\mathbb{Z}_m, A)) \leq d$, where $\mathrm{diam}(G)$ denotes that diameter of a graph G. In other words,

$$m(d,k) = \max_{\substack{A \\ |A|=k}} \{m \mid \mathrm{diam}(\mathrm{Cay}(\mathbb{Z}_m, A)) \leq d\}.$$

In this thesis, we focus on some optimization problems for Cayley digraphs, including $m(d,k)$. In particular, we study how large the number of vertices a Cayley digraph could have for a given diameter and degree. This is one of the central problems in the study of extremal Cayley digraphs.

1.3 Organization of the thesis

As mentioned earlier, this thesis focuses on some important optimization problems about Cayley digraphs. This is still an on-going research area in mathematics and

computer science. In order to effectively describe our new results and expose research topics, we include in Chapter 2 some basic concepts and results in graph theory.

In Chapter 3, we first introduce Cayley digraphs. We discuss the connectivity of Cayley digraphs of the finite abelian group $\mathbb{Z}_m^r$. In Section 3.3 we define various extremal functions related to Cayley digraphs, including $m(d,k)$, which is our main focus of this thesis.

In Chapter 4, we limit our focus to Cayley digraphs of finite cyclic groups. Our main concern is the extremal function $m(d,k)$. Because of a recursive inequality, one is able to use lower bounds for $m(d,k)$ with k being small to establish lower bounds for $m(d,k)$ with k large. Therefore, we first establish lower bounds for $m(d,k)$ when k= 2, 3.

In Chapter 5, we study the geometry of finite cyclic groups. The elements of a finite cyclic group can be represented by a k-dimensional solid with respect to a k-element generating set. This geometric representation can be regarded as a representation of the Cayley digraph of a finite cyclic group, which was first introduced by Wong and Coppersmith in the 1970's. This geometric representation is an essential tool in establishing upper bounds for $m(d,k)$ (see, e.g. Mask, Schneider and Jia, 2011).

In Chapter 6, we first summarize the key results in this thesis. Then we list some new and old open problems in related areas. In addition, we include remarks about some of the open problems.

Chapter 2

GRAPHS AND DIGRAPHS

In this chapter, some basic concepts and results in graph theory that are used in this thesis will be introduced. This is not intended to be an introduction to graph theory by any means. For more on graphs, the reader should see a very good book by Douglas B. West (West, 1996) titled *Introduction to Graph Theory*.

2.1 Definitions and Examples

Definition 2. A *simple graph* $G = (V, E)$ consists of a nonempty set V of objects called *vertices* and a set E of 2-element subsets of V called *edges*.

In a graph G, the two vertices on an edge are called *end vertices* of the edge, and the edge is said to be *incident* to its end vertices. Two vertices are said to be *adjacent* if they are the end vertices of an edge. If u and v are adjacent vertices in a graph, it is often more convenient to represent the edge $\{u, v\}$ by uv (or vu). A simple graph $G = (V, E)$ defined by $V = \{u, v, w, x, y, z\}$ and $E = \{uv, uw, ux, vy, wx\}$ can be represented by a graph as shown in Figure 2.1. This drawing of G is often referred to as the graph G. Note that the graphical representation of the graph is not unique.

The following are a few examples of graphs.

Path P_n: A *path* P_n of length n is a graph with $n+1$ vertices $v_1, \ldots, v_{n+1}$ and edges $v_i v_{i+1}$ $(i = 1, 2, \ldots, n)$, where v_1 and v_{n+1} are called the *end vertices* of the path.

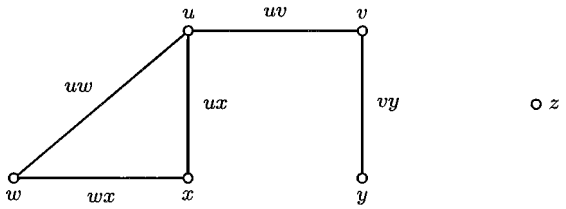


Figure 2.1: A simple graph G with 6 vertices.

Cycle C_n: A *cycle* C_n of length n is a path of length n with the end vertices being the same vertex.

Complete Graph K_n: A *complete graph* with n vertices, denoted as K_n, is a simple graph with all possible edges.

n-Cube Q_n: An *n-cube*, denoted by Q_n, is a simple graph with vertices that can be labeled with the 2^n bit strings[1] of length n so that two vertices are adjacent if and only if the corresponding bit strings differ in exactly one bit.

Bipartite Graphs: A simple graph $G = (V, E)$ is said to be a *bipartite graph* if the vertex set V can be colored with two colors so that every edge connects vertices with different colors.

Multigraphs, Pseudographs, and Digraphs: A *multigraph* $G = (V, E)$ consists of a set V of vertices and a multiset E of edges with distinct end vertices. A *pseudograph* $G = (V, E)$ consists of a set V of vertices and a multiset E of unordered pairs (edges) of not necessarily distinct vertices in V. An edge with the same end vertex is called a

[1]For convenience we sometimes use n-tuples of 0's and 1's instead of bit strings to label the vertices.

loop or a *self loop*. A *digraph* is a graph where the edges have a direction associated with them.

2.2 Connectivity

Graph connectivity is a central property of graphs. There are many problems related to the connectivity of graphs. Connectivity of a special kind of graphs, called Cayley digraphs, is one of the main focuses in this paper. In this section, some basic definitions shall be introduced along with Menger's Theorem.

Definition 3. Let k be a positive integer.

(i) A *walk* is a list of vertices and edges

$$v_0, e_1, v_1, e_2, v_2, \ldots, e_k, v_k$$

such that e_i has endpoints v_{i-1} and v_i.

(ii) A *trail* is a walk with distinct edges.

(iii) A *tour* or a *circuit* is a walk with the ending vertex being the same as the starting vertex.

(iv) A *path* is a walk without repeated vertices.

(v) A *cycle* is a closed path with the same starting and ending vertex. In other words, a cycle is a tour without repeated vertices.

(vi) The *length* of a walk, a path, or a cycle is the number of its edges.

Definition 4. An undirected graph is said to be *connected* if there exists a path between every pair of vertices. A directed graph is said to be *strongly connected* if there is a

directed path between every pair of vertices of the graph. A directed graph is said to be *weekly connected* if the underlining undirected graph is connected. A disconnected graph is the union of connected subgraphs, called *connected components*.

Definition 5. Let $G = (V, E)$ be a graph.

(i) A vertex $v \in V$ is called a *cut vertex* if G becomes disconnected after the removal of v and edges incident to v.

(ii) A set of vertices $W \subseteq V$ is called a *cut vertex set* if G becomes disconnected after the removal of W and edges incident to the vertices in W.

(iii) A *minimal* cut vertex set is a cut vertex set such that none of its proper subset is again a cut vertex set.

Definition 6. Let G be a graph. The size of a minimal cut vertex set is called the *connectivity* of G, and denoted by $\kappa(G)$. A graph G is k-connected if $\kappa(G) \geq k$. The *edge-connectivity* $\lambda(G)$ of a nontrivial graph G is the minimum number of edges whose removal from G results in a nonconnected graph.

Obviously, if W is a minimal cut vertex set of G, then G contains two vertices u, v such that every path between u and v contains a vertex in S.

It is easy to see that $\kappa(C_n) = 2$ and $\kappa(K_n) = n - 1$. If $\delta(G)$ is used to denote the minimum degree of G, then

$$\kappa(G) \leq \lambda(G) \leq \delta(G).$$

Theorem 1 (H. Whitney, 1932). *A graph G with order $n \geq 3$ is 2-connected if and only if any two vertices of G are joined by at least two internally-disjoint paths.*

Definition 7. Let G be a graph. An *independent edge set* is a subset of edges of G such that no two edges share a common vertex. An independent edge set is also called a *matching*. The maximum number of edges in an independent edge set is called the *edge independence number*, denoted by $\beta_1(G)$.

Definition 8. Let G be a graph. A *vertex cover* of G is a subset W of vertices of G such that each edge of G is incident to at least one vertex in W. The minimum number of vertices in a vertex cover is called the *vertex covering number*, denoted by $\alpha(G)$.

Let u and v be nonadjacent vertices in a graph G. A (u,v)-*cut* is a set $X \subseteq V(G) - \{u,v\}$ whose removal from G leaves u and v in different components. Let $\kappa(u,v)$ denote the minimum number of vertices in a (u,v)-cut, and $\lambda(u,v)$ the maximum number of internally-disjoint u-v paths. The following is the Menger's Theorem.

Theorem 2 (K. Menger, 1927). *Let u and v be nonadjacent vertices in a graph G. Then $\kappa(u,v) = \lambda(u,v)$.*

2.3 Distance and Diameter

Distance between vertices in a graph is an important parameter of the graph. In this section, we study the diameter and the average distance of graphs.

2.3.1 Eccentricity

Recall that the distance between two vertices in a graph is the number of edges in a shortest path connecting them. We use $d_G(u,v)$ to denote the distance between vertices u and v in G.

Definition 9. Let G be an undirected graph.

(*i*) The *eccentricity* $e(v)$ of a vertex v is the greatest distance between v and any other vertex in the graph.

(*ii*) The *radius* of G, denoted as $r(G)$, is the minimum eccentricity of any vertex.

(*iii*) The *diameter* of G, denoted as $\mathrm{diam}(G)$, is the maximum eccentricity of any vertex in the graph. In other words, the diameter is the greatest distance between any pair of vertices.

(*iv*) The *girth* of G is the length of the shortest closed path of the graph.

(*v*) A *central vertex* in a graph of radius r is one that is distance r from some other vertex.

(*vi*) A *peripheral vertex* in a graph of diameter d is one that is distance d from some other vertex.

Example 1. The graph shown in Figure 2.2 is connected. It is easy to see that the radius is 2 and the diameter is 3. The central vertices are the filled vertices while the rest of the vertices are the peripheral vertices of the graph.

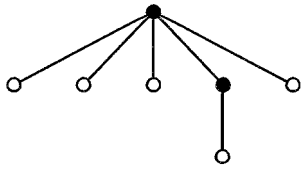


Figure 2.2: Filled vertices are central vertices. $r(G) = 2$ and $\mathrm{diam}(G) = 3$.

Example 2. Because the n-cube Q_n is distance symmetric, every vertex has the same eccentricity n. Therefore, $r(Q_n) = \mathrm{diam}(Q_n) = n$. Hence, every vertex is a central vertex and a peripheral vertex.

2.3.2 Average Distance

Definition 10. Let $G = (V, E)$ be a connected simple graph with $n \geq 2$ vertices. The *average distance* $\bar{d}(G)$ of G is defined as

$$\bar{d}(G) = \frac{1}{\binom{n}{2}} \sum_{u,v \in V} d(u, v).$$

Let G be a graph. Since $d(u, v) \leq d(G)$ for any two vertices u and v, we see that $\bar{d}(G) \leq d(G)$.

Proposition 1. *Let G be a connected graph. Then $\bar{d}(G) = d(G)$ if and only if G is a complete graph.*

Proof. Let G be a graph with n vertices. If G is a complete graph, it is obvious that $\bar{d}(G) = d(G) = 1$.

Now assume that $\bar{d}(G) = d(G)$. We only need to prove that $d(G) = 1$. If not, assume that

$$u = u_0, u_1, \ldots, u_d = v$$

is a shortest path of length $d = d(G) > 1$ in G. Then $d - 1 > 0$ and

$$\begin{aligned}
\bar{d}(G) &= \frac{1}{\binom{n}{2}} \sum_{u,v \in V} d(u, v) \\
&= \frac{2}{n(n-1)} \left(d(u_0, u_1) + \sum_{\{x,y\} \neq \{u_0,u_1\}} d(x, y) \right) \\
&\leq \frac{2}{n(n-1)} \left(1 + d \cdot \left(\frac{1}{2} n(n-1) - 1 \right) \right) \\
&= d - \frac{2(d-1)}{n(n-1)} \\
&< d = d(G).
\end{aligned}$$

□

Proposition 2. *The average distance of the n-cube Q_n is* $\dfrac{n}{2} + \dfrac{n}{2^{n+1}-2}$.

Proof. By the definition of Q_n, its 2^n vertices can be represented by the bit strings of length n so that two vertices are adjacent if their labels differ in exactly one bit. Because of the symmetry of Q_n, the average distance of Q_n is

$$\bar{d}(Q_n) = \frac{1}{2^n - 1} \sum_{\mathbf{0} \neq \ell(v) \in \mathscr{B}_n} d(\mathbf{0}, v),$$

where $\mathscr{B}_n$ is the set of bit strings of length n, and $\ell(v)$ is the bit string labeling of v. The vertices that have distance k to the vertex with label $\mathbf{0}$ are the vertices with labels that have exactly k 1's. Since there are $\binom{n}{k}$ distinct bit strings with exactly k 1's and $n-k$ 0's, we see that

$$\bar{d}(Q_n) = \frac{1}{2^n - 1} \sum_{k=1}^{n} \binom{n}{k} k = \frac{1}{2^n - 1} n 2^{n-1} = \frac{n}{2} + \frac{n}{2^{n+1} - 2}. \qquad \square$$

In particular, $\bar{d}(Q_2) = \dfrac{4}{3}$ and $\bar{d}(Q_3) = \dfrac{12}{7}$.

Proposition 3. *Let $\mathbf{C}_m$ be the directed cycle of length m. Then* $\bar{d}(\mathbf{C}_m) = \dfrac{1}{2}m$.

Proof. It follows from the fact

$$d(i, j) + d(j, i) = m \qquad \text{for any } 1 \leq i < j \leq m$$

that

$$\begin{aligned} \bar{d}(\mathbf{C}_m) &= \frac{1}{m(m-1)} \sum_{1 \leq i < j \leq m} (d(i, j) + d(j, i)) \\ &= \frac{1}{m(m-1)} \binom{m}{2} m \\ &= \frac{1}{2} m. \end{aligned}$$

$\square$

It is easy to verify the following proposition.

Proposition 4. *Let C_n be the cycle of length n, then*

$$\bar{d}(C_n) = \begin{cases} \dfrac{k^2+1}{2k-1}, & \text{if } n = 2k \\ \dfrac{k+1}{2}, & \text{if } n = 2k+1 \end{cases}.$$

Compared with the diameter of a graph, the average distance of the graph reflects more accurate information about the distance between vertices in the graph. The following example shows an extreme situation. For any given integer $d \geq 2$, let G be the graph obtained by attaching one of the end node of a path P_d to any vertex of a complete graph K_m as showed in Figure 2.3. Then $d(G) = d$. Noting that the dis-

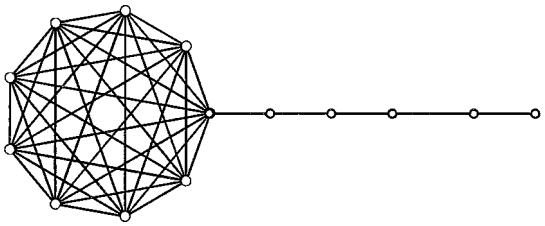


Figure 2.3: A graph that shows $\bar{d}(G) \to 1$ for any given $d = d(G)$.

tance between a vertex on P_d and any other vertex in G is at most d while the distance between any two vertices in K_m is one, we see that

$$\begin{aligned} 1 \leq \bar{d}(G) &\leq \frac{1}{\binom{m+d-1}{2}} \left((d-1)(m+d-2) + \binom{m}{2} \right) \\ &\leq \frac{2d(m+d)+m^2}{(m+d-1)(m+d-2)}. \end{aligned}$$

This shows that the average distance $\bar{d}(G)$ of this graph G has a limit 1 as $m \to \infty$. Given any positive integer d, define

$$\overline{D}(d) = \sup_{\substack{G \\ d(G)=d}} \bar{d}(G).$$

Then $\overline{D}(1) = 1$ as shown by the complete graph K_m. Let G_m denote the star graph with $m+1$ vertices. It is easy to verify that

$$\bar{d}(G_m) = \frac{2m}{m+1} \to 2 \qquad \text{as} \quad m \to \infty,$$

i.e., $\overline{D}(2) = 2$.

Let $T(m)$ denote the following graph: a star graph with m leaves each of which is the center vertex of a star graph with m leaves. Figure 2.4 shows the construction of $T(6)$. Then $T(m)$ has m^2+m+1 vertices and m^2+m edges. Easy to see that

$$\begin{aligned}\bar{d}(T(m)) &= \frac{1}{\binom{m^2+m+1}{2}} \sum_{uv \in E(T(m))} d(u,v) \\ &= \frac{4m^2(m^2-2)}{(m^2+m+1)(m^2+m)} \to 4 \qquad \text{as} \quad m \to \infty.\end{aligned}$$

Therefore, $\overline{D}(4) = 4$.

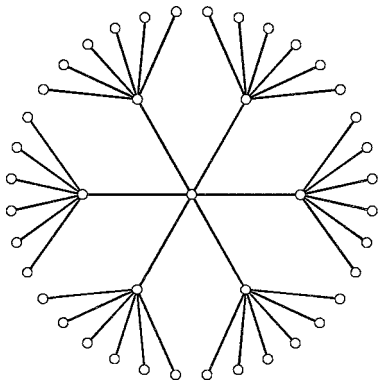


Figure 2.4: $T(6)$ is a graph that shows that $\overline{D}(4) = 4$.

2.4 Degree-Diameter Problem

The Degree-Diameter Problem is to determine the largest graphs with given maximum degree k and diameter d. In this section we address an upper bound, known as the Moore bound.

Let k and d be positive integers. A (k,d)-*graph* is a graph with maximum degree k and diameter at most d. Let $f(k,d)$ denote the maximum number of vertices that a (k,d)-graph can have.

Theorem 3. $f(k,d) \leq 1 + \frac{k}{k-2}\left((k-1)^d - 1\right)$.

Proof. Let $G = (V,E)$ be a (k,d)-graph with $m = |V|$. We only need to prove that $m \leq 1 + \frac{k}{k-2}\left((k-1)^d - 1\right)$. Pick any vertex $u \in V$. For each integer $i : 1 \leq i \leq d$, define

$$V_i = \{v \in V \mid d(u,v) = i\}.$$

Since the diameter of G is d, we see that

$$m = |V| = 1 + \sum_{i=1}^{d} |V_i|.$$

Because the maximum degree of G is k, we have that

$$|V_1| \leq k,$$

and

$$|V_i| \leq k(k-1)^{i-1} \qquad \text{for all} \quad i.$$

Therefore,

$$\begin{aligned} m &= 1 + \sum_{i=1}^{d} |V_i| \leq 1 + \sum_{i=1}^{d} k(k-1)^{i-1} \\ &= 1 + \frac{k}{k-2}\left((k-1)^d - 1\right). \end{aligned}$$

□

Now consider a graph G with minimum degree k and girth g.

Theorem 4. *Let G be a graph with minimum degree k and girth g. If $d = \left\lfloor \frac{g-1}{2} \right\rfloor$, then*

$$|V(G)| \geq 1 + \frac{k}{k-2}\left((k-1)^d - 1\right).$$

Proof. This proof follows a similar argument as the previous theorem. Let G be a graph with m vertices, with minimum degree k and girth g. Pick any vertex u. For each integer $i : 1 \leq i \leq d$, define

$$V_i = \{v \in V \mid d(u, v) = i\}.$$

Since the diameter of G is at least $d = \left\lfloor \frac{g-1}{2} \right\rfloor$, we see that

$$m = |V(G)| \geq 1 + \sum_{i=1}^{d} |V_i|.$$

Furthermore, it follows from the fact that the minimum degree of G is k that

$$|V_1| \geq k,$$

and

$$|V_i| \geq k(k-1)^{i-1} \qquad \text{for all} \quad i : 1 \leq i \leq d.$$

Therefore, we have

$$\begin{aligned} m &= 1 + \sum_{i=1}^{d} |V_i| \geq 1 + \sum_{i=1}^{d} k(k-1)^{i-1} \\ &= 1 + \frac{k}{k-2}\left((k-1)^d - 1\right). \end{aligned}$$

□

The upper bound in Theorem 3 is sometimes called the *Moore bound.* A regular graph with degree k and diameter d that has $1 + \frac{k}{k-2}\left((k-1)^d - 1\right)$ vertices is called a *Moore graph.* Equivalently, a Moore graph is a k-regular graph with diameter d that has girth $2d + 1$. The following is another equivalent definition.

Definition 11. A graph G is called a *Moore graph* if the following conditions hold:

(*i*) G is connected with maximum degree k and diameter d,

(*ii*) G has minimum degree k and girth $g = 2d + 1$,

(*iii*) G has $1 + \frac{k}{k-2}\left((k-1)^d - 1\right)$ vertices.

The following Table 2.1 shows the order of some large known (k, d)-graphs. The sizes in bold face in the table indicate the optimal value $f(k, d)$. For more information on (k, d)-graphs, please visit http://www-mat.upc.es/grup_de_grafs/table_g.html.

Table 2.1: The size of large (k, d)-graphs

$k \setminus d$	2	3	4	5	6	7	8	9	10
3	**10**	**20**	**38**	70	132	192	330	576	1250
4	**15**	41	96	364	740	1 320	3 243	7 575	17 703
5	**24**	72	210	624	2 772	5 516	17 030	53 352	164 720
6	32	110	390	1 404	7 917	19 282	75 157	295 025	1 212 117
7	**50**	168	672	2 756	11 988	52 768	233 700	1 124 990	5 311 572
8	57	253	1 100	5 060	39 672	130 017	714 010	4 039 704	17 823 532
9	74	585	1 550	8 200	75 893	270 192	1 485 498	10 423 212	31 466 244
10	91	650	2 223	13 140	134 690	561 957	4 019 736	17 304 400	104 058 822
11	104	715	3 200	18 700	156 864	971 028	5 941 864	62 932 488	250 108 668
12	133	786	4 680	29 470	359 772	1 900 464	10 423 212	104 058 822	600 105 100
13	162	851	6 560	39 576	531 440	2 901 404	17 823 532	180 002 472	1 050 104 118
14	183	916	8 200	56 790	816 294	6 200 460	41 894 424	450 103 771	2 050 103 984
15	186	1 215	11 712	74 298	1 417 248	8 079 298	90 001 236	900 207 542	4 149 702 144
16	198	1 600	14 640	132 496	1 771 560	14 882 658	104 518 518	1 400 103 920	7 394 669 856

Bold face numbers indicate the optimal values.

Chapter 3

EXTREMAL CAYLEY DIGRAPHS

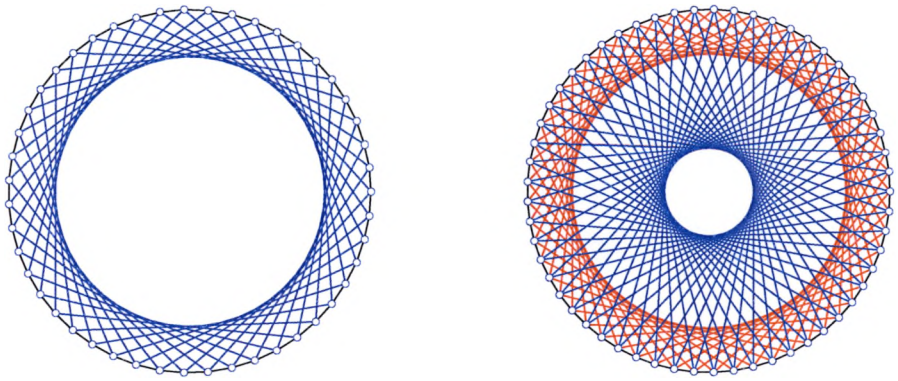
3.1 Cayley Digraphs

Recall that we have the following definition in Section 1.2.

Definition 1. *Let Γ be a finite group with m elements. Let A be a nonempty subset of Γ. The* Cayley digraph *of Γ generated by A, denoted by $\mathrm{Cay}(\Gamma, A)$, is the digraph with vertex set Γ and arc set $\{uv \mid u^{-1}v \in A\}$.*

Example 3. A directed cycle $\mathbf{C}_m$ is a Cayley digraph of $\mathbb{Z}_m$ with a single generating element 1, or, as a matter of fact, any $a \in \mathbb{Z}_m$ that is relatively prime to m.

Example 4. Cayley digraphs $\mathrm{Cay}(\mathbb{Z}_{47}, \{1, 11\})$ and $\mathrm{Cay}(\mathbb{Z}_{57}, \{1, 13, 33\})$:



$\mathrm{Cay}(\mathbb{Z}_{57}, \{1, 13, 33\})$ $\mathrm{Cay}(\mathbb{Z}_{47}, \{1, 11\})$

Figure 3.1: Two Cayley digraphs.

The edges in the graphs are supposed to be directed. The graphs are symmetric.

Clearly, Cayley digraph $\mathrm{Cay}(\Gamma, A)$ is connected if and only if A can generate the whole group Γ.

Definition 12. A subset A of a group Γ is said to be *symmetric* if $a^{-1} \in A$ for all $a \in A$.

Note that Cayley digraphs are directed graphs. However, if the generating set A is symmetric, the Cayley digraph $\mathrm{Cay}(\Gamma, A)$ can be considered as an undirected graph.

Example 5. The hypercube Q_n is actually a Cayley digraph of $\mathbb{Z}_2^n$ with generating set $\{e_i \mid i = 1, 2, \ldots, n\}$, where $e_i = (0, \ldots, 0, \underbrace{1}_{i}, 0, \ldots, 0)$ is the ith basis vector in $\mathbb{Z}_2^n$.

Cayley digraphs of finite abelian groups are often used to model information networks. Because of their applications, extremal Cayley digraphs have been studied extensively in recent years.

3.2 Connectivity of Cayley Digraphs

In this section, we discuss the connectivity of the Cayley digraph $\mathrm{Cay}(\Gamma, A)$ of a finite abelian group Γ generated by an r-element subset A, where $r = \mathrm{rank}(\Gamma)$ is the rank of Γ, is discussed.

Theorem 5. *Let* $\Gamma = \mathbb{Z}_m^r$. *Let* $A = \{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_r\}$ *be a subset of* Γ. *Assume that*

$$\mathbf{a}_i = (a_{i1}, a_{i2}, \ldots, a_{ir}) \qquad \textit{for} \quad i = 1, 2, \ldots, r.$$

Define $M_A = [a_{ij}]_{r \times r}$. *Then the Cayley digraph* $\mathrm{Cay}(\Gamma, A)$ *is connected if and only if* M_A *is an invertible matrix.*

Proof. ($\Rightarrow$) Assume that the Cayley digraph $\mathrm{Cay}(\Gamma, A)$ is connected. Then $A = \{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_r\}$ is a generating set of the finite abelian group Γ. Therefore, for each $i : 1 \leq i \leq r$, there exists an r-tuple $\xi_i = (x_{i1}, x_{i2}, \ldots, x_{ir})$ with

$$0 \leq x_{ij} \leq m - 1 \qquad \text{for} \quad j = 1, 2 \ldots, r$$

such that

$$\xi_i M_A = \mathbf{e}_i,$$

where $\mathbf{e}_i = (0, \ldots, 0, \underbrace{1}_{i}, 0, \ldots, 0)$ is the ith unit vector in Γ. Let B be the $r \times r$ matrix consisting $\xi_1, \xi_2, \ldots, \xi_r$ as its row vectors, i.e.,

$$B = [x_{ij}]_{r \times r}$$

Then $BM_A = I_r$, the $r \times r$ identity matrix.

Define a function $\sigma : \Gamma \to \Gamma$ defined by

$$\sigma : \mathbf{x} \mapsto \mathbf{x}M_A = \sum_{i=1}^{r} x_i \mathbf{a}_i$$

for every $\mathbf{x} = (x_1, x_2, \ldots, x_r) \in \Gamma$. Since A is a generating set of Γ, we see that σ is an onto function. Noting that Γ is finite, we know that σ is also one-to-one. Therefore, $\mathbf{x}M_A = \mathbf{0}$ has a unique solution.

It follows from $BM_A = I_r$ that

$$M_A B M_A = M_A I_r = M_A.$$

Then

$$0 = M_A B M_A - M_A = (M_A B - I_r) M_A.$$

Hence, $M_A B - I_r = 0$, i.e., $M_A B = I_r$. Therefore, B is the inverse matrix of M_A.

($\Leftarrow$) Assume that M_A is invertible. Let $\mathbf{x} \in \Gamma$ be any element. Define

$$\mathbf{c} = (c_1, c_2, \ldots, c_r) = \mathbf{x}M_A^{-1} \in \Gamma,$$

where

$$0 \leq c_i \leq m - 1 \qquad \text{for} \quad i = 1, 2, \ldots, r.$$

Then

$$\mathbf{x} = \mathbf{c}M_A = \sum_{i=1}^{r} c_i \mathbf{a}_i.$$

This implies that A is a generating set of Γ. Hence, the Cayley digraph $\mathrm{Cay}(\Gamma, A)$ of Γ generated by A is connected. □

Theorem 6. *Let $\Gamma = \mathbb{Z}_m^r$ be the direct product of r copies of $\mathbb{Z}_m$. Let $A = \{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_r\}$ be a generating set of Γ. Then $\mathrm{Cay}(\Gamma, A)$ is connected and*

$$\mathrm{diam}(\mathrm{Cay}(\Gamma, A)) = rm - r.$$

Proof. Because of the symmetry of $\mathrm{Cay}(\Gamma, A)$, we may assume that

$$d = \mathrm{diam}(\mathrm{Cay}(\Gamma, A) = d(\mathbf{0}, \mathbf{u}) = \sum_{i=1}^{r} u_i,$$

for some $\mathbf{u} = \sum_{i=1}^{r} u_i \mathbf{a}_i$. Since

$$0 \leq u_i \leq m - 1 \qquad \text{for} \quad i = 1, 2, \ldots, r.$$

Therefore,

$$d = \sum_{i=1}^{r} u_i \leq rm - r.$$

It is now proven that there exists an element $\mathbf{u} \in \Gamma$ such that

$$d(\mathbf{0}, \mathbf{u}) = rm - r.$$

Define

$$\mathbf{u} = \sum_{i=1}^{r} (m-1)\mathbf{a}_i.$$

If $d(\mathbf{0}, \mathbf{u}) < rm - r$, then $\mathbf{u}$ can be written as

$$\mathbf{u} = \sum_{i=1}^{r} c_i \mathbf{a}_i,$$

where

$$0 \leq c_i \leq m-1 \qquad \text{for} \quad i = 1, 2, \ldots, r$$

such that

$$\sum_{i=1}^{r} c_i < d.$$

Then

$$\mathbf{v} = (m-1, m-1, \ldots, m-1) - (c_1, c_2, \ldots, c_r) \neq \mathbf{0}.$$

This implies that

$$((m-1, \ldots, m-1) - (c_1, \ldots, c_r))M_A = \mathbf{u} - \mathbf{u} = \mathbf{0},$$

contradicting the fact that M_A is invertible. Hence, $d(\mathbf{0}, \mathbf{u}) = rm - r$. Therefore, the diameter of $\mathrm{Cay}(\Gamma, A)$ is $rm - r$. The proof of Theorem 6 is complete. □

3.3 Extremal Functions Related to Cayley Digraphs

In this section, we shall define a few extremal functions related to Cayley digraphs of $\mathbb{Z}_m$, the finite cyclic group of order m. A subset A of $\mathbb{Z}_m$ is called a d-basis for $\mathbb{Z}_m$ if $\mathrm{diam}(\mathrm{Cay}(\mathbb{Z}_m, A)) \leq d$.

3.3.1 $m(d, k)$

Definition 13. Given any two positive integers d and k, define $m(d, k)$ as the largest positive integer m such that there exists a d-basis A of k integers for $\mathbb{Z}_m$, i.e.,

$$\mathrm{diam}(\mathrm{Cay}(\mathbb{Z}_m, A)) \leq d,$$

where $\mathrm{diam}(G)$ denotes the diameter of a graph G. In other words,

$$m(d, k) = \max_{\substack{A \\ |A|=k}} \{m \mid \mathrm{diam}(\mathrm{Cay}(\mathbb{Z}_m, A)) \leq d\}.$$

Theorem 7. *For any given positive integer d,*

$$m(d,1) = d+1.$$

Proof. On one hand, we assume $G = \mathrm{Cay}(\mathbb{Z}_m, \{a\})$ has diameter at most d. Since every vertex of G can be written as xa where x is a nonnegative integer that is less than or equal to d. This implies that $m = |V(G)| \leq d+1$. Hence, $m(d,1) \leq d+1$.

On the other hand, we let $A = \{1\}$ and $m = d+1$. It is clear that

$$\mathrm{diam}(\mathrm{Cay}(\mathbb{Z}_m, A)) = d.$$

This means that we have $d+1 \leq m(d,1)$ Therefore, we proved the required identity in the theorem. □

Theorem 8. *For any given positive integer k,*

$$m(1,k) = k+1.$$

Proof. First, let $A = \{a_1, a_2, \ldots, a_k\}$ be a set of k elements so that $G = \mathrm{Cay}(\mathbb{Z}_m, A)$ has diameter 1. Then every vertex of G is an immediate neighbor of $0 \in \mathbb{Z}_m$. Since the neighbors of 0 are the elements in A:

$$a_1,\ a_2,\ \ldots,\ a_k,$$

Therefore, $m(1,k) \leq k+1$.

Now Let $A = \{1, 2, \ldots, k\}$. Then it is easy to see that $\mathrm{diam}(\mathrm{Cay}(\mathbb{Z}_{k+1}, A)) = 1$. This means that $m(1,k) \geq k+1$. Therefore, we have $m(1,k) = k+1$. □

Theorem 9 (Wong-Coppersmith, 1974)**.** *For any given positive integers d and k, we have*

$$\left\lfloor \frac{d}{k} + 1 \right\rfloor^k \leq m(d,k) \leq \binom{k+d}{k}.$$

Proof. We first prove the upper-bound. If A is a k element set with $\mathrm{diam}(\mathrm{Cay}(\mathbb{Z}_m, A)) \leq d$, then every element in $\mathbb{Z}_m$ is a sum of at most d elements from A. Noting that the addition of integers is commutative, we see that

$$m \leq \binom{k+1+d-1}{d} = \binom{k+d}{k},$$

which shows the upper bound of the required inequality.

Now we prove the lower-bound. Let

$$t = \left\lfloor \frac{d}{k} \right\rfloor + 1$$

and

$$A = \{1, t, t^2, \ldots, t^{k-1}\}.$$

For any $x \in [0, t^k - 1]$, then

$$x = \sum_{i=0}^{k-1} c_i t^i \qquad \text{with} \quad 0 \leq c_i \leq t-1.$$

Since

$$\sum c_i \leq k(t-1) = k\lfloor d/k \rfloor \leq d,$$

we see that $d(0, x) \leq d$. Therefore, the diameter of $\mathrm{Cay}(\mathbb{Z}_{t^k}, A)$ is at most d, which implies

$$m(d,k) \geq t^k = \left\lfloor \frac{d}{k} + 1 \right\rfloor^k. \qquad \square$$

Corollary 1. *For any given positive integer k, as $d \to \infty$,*

$$\left(\frac{d}{k}\right)^k + O(d^{k-1}) \leq m(d,k) \leq \frac{d^k}{k!} + O(d^{k-1}).$$

Proof. This follows immediately from Theorem 9. $\square$

Hsu and Jia (1994) proved that, for any integer $d \geq 2$,

$$m(d,2) = \left\lfloor \frac{d(d+4)}{3} \right\rfloor + 1. \tag{3.1}$$

We will prove this exact formula in Chapters 4 and 5.

Table 3.1 contains the exact values of $m(d,3)$ for $2 \leq d \leq 20$ together with the corresponding generating sets. We do not list the so called "isomorphic" generating sets. For instance, $A = \{1,3,4\}$ is a generating set for $\mathrm{Cay}(\mathbb{Z}_9, A)$ which gives diameter 2. The inverse element of 4 in $\mathbb{Z}_9$ is 7. Since

$$1 \cdot 7 = 7, \quad 3 \cdot 7 = 3, \quad \text{and} \quad 4 \cdot 7 = 1 \pmod 9,$$

we see that $\{1,3,7\}$ is an isomorphic generating set of $\{1,3,4\}$. So the generating set $\{1,3,7\}$ is not listed in the table.

3.3.2 $\overline{m}(\lambda, k)$

Definition 14. Given any positive integer k and any real number λ, define $\overline{m}(\lambda, k)$ as the largest positive integer m such that there exists a set A of k integers with

$$\bar{d}(\mathrm{Cay}(\mathbb{Z}_m, A)) \leq \lambda,$$

where $\bar{d}(G)$ denotes the average distance of a graph G. In other words,

$$\overline{m}(\lambda, k) = \max_{\substack{A \\ |A|=k}} \{m \mid \bar{d}(\mathrm{Cay}(\mathbb{Z}_m, A)) \leq \lambda\}.$$

Theorem 10. *For any given positive integer k,*

$$\overline{m}(1,k) = k+1.$$

Proof. First, we prove that $\overline{m}(1,k) \leq k+1$. Let $A = \{a_1, a_2, \ldots, a_k\}$ be a generating set of $\mathbb{Z}_m$ so that $\bar{d}(\mathrm{Cay}(\mathbb{Z}_m, A)) \leq 1$. However, the average distance of any

Table 3.1: $m(d,3)$ for $2 \leq d \leq 20$ with corresponding extremal generating sets.

d	$m(d,3)$	Corresponding extremal generating sets
2	9	$\{1,3,4\}, \{1,4,6\}$
3	16	$\{1,4,5\}, \{1,5,12\}$
4	27	$\{1,4,17\}, \{1,5,12\}, \{1,6,8\}, \{1,16,23\}$
5	40	$\{1,6,15\}, \{1,6,25\}, \{1,16,35\}, \{1,26,35\}$
6	57	$\{1,13,33\}, \{1,16,36\}$
7	78	$\{1,6,49\}, \{1,7,48\}, \{1,12,61\}, \{1,30,73\}$
8	111	$\{1,31,69\}$
9	138	$\{1,11,78\}, \{1,17,96\}, \{1,19,26\}, \{1,43,122\}$
10	176	$\{1,17,56\}, \{1,24,33\}, \{1,32,153\}, \{1,41,64\}, \{1,81,104\}, \{1,121,160\}$
11	217	$\{1,13,119\}, \{1,18,46\}, \{1,34,161\}, \{1,51,92\}$
12	273	$\{1,14,153\}, \{1,49,104\}, \{1,53,186\}, \{1,88,221\}$
13	340	$\{1,90,191\}$
14	395	$\{1,35,271\}, \{1,125,361\}$
15	462	$\{1,29,97\}, \{1,33,254\}, \{1,44,56\}, \{1,44,408\}, \{1,55,419\}, \{1,89,121\}, \{1,110,254\}, \{1,122,165\}, \{1,165,188\}, \{1,209,430\}, \{1,224,380\}, \{1,275,298\}, \{1,282,296\}, \{1,298,341\}, \{1,342,374\}, \{1,366,434\}$
16	560	$\{1,215,326\}, \{1,235,346\}$
17	648	$\{1,76,237\}, \{1,412,573\}$
18	748	$\{1,41,147\}, \{1,174,362\}, \{1,490,676\}, \{1,602,708\}$
19	861	$\{1,27,463\}, \{1,84,298\}, \{1,84,319\}, \{1,543,778\}$
20	979	$\{1,22,351\}, \{1,138,787\}, \{1,193,842\}, \{1,374,637\}$

graph is always at least one. Thus, $\bar{d}(\mathrm{Cay}(\mathbb{Z}_m, A)) = 1$. Therefore, the Cayley graph $\mathrm{Cay}(\mathbb{Z}_m, A)$ is a complete digraph. Since $0 \in \mathbb{Z}_m$ has out-degree k (because each element of A contributes at most one to the out-degree of 0), we see that $m \leq k+1$.

Now we prove that $\overline{m}(1,k) \geq k+1$. Define

$$A = \{1, 2, \ldots, k\}.$$

Then $\mathrm{diam}(\mathrm{Cay}(\mathbb{Z}_{k+1}, A)) = 1$, which implies that $\bar{d}(\mathrm{Cay}(\mathbb{Z}_{k+1}, A)) = 1$. Therefore, $\overline{m}(1,k) \geq k+1$. The proof is complete. □

Theorem 11. *For any given positive real number λ,*

$$\overline{m}(\lambda, 1) = \lfloor 2\lambda \rfloor.$$

Proof. First we prove that $\overline{m}(\lambda,1) \leq \lfloor 2\lambda \rfloor$. Let $A = \{a\}$ be a generating set of $\mathbb{Z}_m$ so that the average distance of $G = \mathrm{Cay}(\mathbb{Z}_m, A)$ is no more than λ. Since $A = \{a\}$ is a generating set of $\mathbb{Z}_m$, $G = \mathbf{C}_m$ is a directed cycle. It follows from Example 3 that

$$\bar{d}(G) = \bar{d}(\mathbf{C}_m) = \frac{1}{2}m.$$

Therefore, $\frac{1}{2}m \leq \lambda$, i.e., $m \leq 2\lambda$. Thus, $m \leq \lfloor 2\lambda \rfloor$. This shows that $\overline{m}(\lambda,1) \leq \lfloor 2\lambda \rfloor$.

We now prove that $\overline{m}(\lambda,1) \geq \lfloor 2\lambda \rfloor$. Let $A = \{1\}$, and let $m = \lfloor 2\lambda \rfloor$. It follows from Example 3 that the average distance of $\mathrm{Cay}(\mathbb{Z}_m, A) = \mathbf{C}_m$ is

$$\frac{1}{2}m = \frac{1}{2}\lfloor 2\lambda \rfloor \leq \frac{1}{2} \cdot 2\lambda = \lambda$$

Therefore, by definition, $\overline{m}(\lambda,1) \geq m = \lfloor 2\lambda \rfloor$. The proof is complete. □

3.3.3 Undirected Cases

Recall that when the generating set is symmetric, the Cayley digraph can be regarded as an undirected graph. In this subsection, we discuss two extremal functions that are related to undirected Cayley graphs. They are actually the undirected analogue of $m(d,k)$ and $\overline{m}(\lambda,k)$. These have been studied by several authors and many results have been discovered. However, the focus of the thesis is on the extremal function $m(d,k)$. Here we only introduce the definitions. For more information on the undirected cases, see Chen and Jia (1993) and Lee, Sheu and Jia (2008).

Definition 15. Given any two positive integers d and k, define $M(d,k)$ as the largest positive integer m such that there exists a symmetric set $A = \{\pm a_1, \pm a_2, \ldots, \pm a_k\}$ with

$$\mathrm{diam}(\mathrm{Cay}(\mathbb{Z}_m, A)) \leq d,$$

In other words,

$$M(d,k) = \max_{A=\{\pm a_1, \pm a_2, \ , \pm a_k\}} \{m \mid \mathrm{diam}(\mathrm{Cay}(\mathbb{Z}_m, A)) \leq d\}.$$

Definition 16. Given any positive integer k and any real number λ, define $\overline{M}(\lambda,k)$ as the largest positive integer m such that there exists a symmetric set

$$A = \{\pm a_1, \pm a_2, \ldots, \pm a_k\}$$

with

$$\bar{d}(\mathrm{Cay}(\mathbb{Z}_m, A)) \leq \lambda,$$

where $\bar{d}(G)$ denotes the average distance of a graph G. In other words,

$$\overline{M}(d,k) = \max_{A=\{\pm a_1, \pm a_2, \ , \pm a_k\}} \{m \mid \bar{d}(\mathrm{Cay}(\mathbb{Z}_m, A)) \leq \lambda\}.$$

Chapter 4

LOWER BOUNDS OF $m(d,k)$

4.1 Introduction

In order to establish lower bounds for $m(d,k)$, one only needs to construct a "good" generating set A so that the diameter of $\mathrm{Cay}(\mathbb{Z}_m, A)$ is less than or equal to d. In this chapter, some lower bounds for $m(d,2)$ and $m(d,3)$ will be discussed. A recursive theorem will be used to establish a lower bound for the general case.

4.2 Case $k = 2$

We prove the following lower bound for $m(d,2)$.

Theorem 12. *Let $d \geq 2$ be an integer. Then*

$$m(d,2) \geq \left\lfloor \frac{d(d+4)}{3} \right\rfloor + 1. \tag{4.1}$$

Proof. Let $m_0 = \lfloor d(d+4)/3 \rfloor + 1$.

Part One: We show that $m(d,2) \geq m_0$, i.e., we need to find a set $A = \{a, b\}$ so that A is a d-basis for $\mathbb{Z}_m$. Let $A_0 = \{0, a, b\}$. We divide this part of the proof into three cases according to d modulo 3.

CASE I. Suppose $d = 3t$ for some positive integer t. Then

$$m_0 = \left\lfloor \frac{3t(3t+4)}{3} \right\rfloor + 1 = 3t^2 + 4t + 1.$$

Let $a = 1$ and $b = 3t + 3$. Let $n \in [0, m_0)$. If $n \geq tb = 3t^2 + 3t$, then $n - tb \geq 0$ and

$$(n - tb) + t \leq m_0 - 1 - tb + t = 3t^2 + 4t + 1 - 1 - 3t^2 - 3t + t = 2t < d.$$

Therefore,

$$n = (n - tb) \cdot 1 + t \cdot b \in dA_0.$$

Now assume that $(u-1)b \leq n < ub$ for some $u : 1 \leq u \leq t$. Noting that

$$(u+t)b - m_0 = ub - t - 1,$$

we see that

$$(u-1)b < (u+t)b - m_0 < bu - 1.$$

Thus, we can further divide this case into two subcases.

SUBCASE IA. If $(u-1)b \leq n < (u+t)b - m_0$, then

$$\begin{aligned} n - (u-1)b &\leq (u+t)b - m_0 - 1 - (u-1)b \\ &= (t+1)(3t+3) - (3t^2 + 4t + 1) - 1 \\ &= 2t + 1. \end{aligned}$$

Therefore, $n = (n - (u-1)b) \cdot 1 + (u-1) \cdot b \in dA_0$ because

$$(n - (u-1)b) + (u-1) \leq (2t+1) + (t-1) = 3t = d.$$

SUBCASE IB. $(u+t)b - m_0 \leq n < ub$. Then

$$\begin{aligned} 0 \leq n - ((u+t)b - m_0) &\leq ub - 1 - (u+t)b + m_0 = m_0 - tb - 1 \\ &= (3t^2 + 4t + 1) - t(3t+3) - 1 = t. \end{aligned}$$

Hence,

$$n \equiv (n - ((u+t)b - m_0)) \cdot 1 + (u+t) \cdot b \pmod{m_0}.$$

Since

$$(n - (u+t)b - m_0) + (u+t) \leq t + u + t \leq 3t = d.$$

Therefore, $n \in dA_0$.

CASE II. Suppose that $d = 3t + 1$ for some positive integer t. Then

$$m_0 = \left\lfloor \frac{(3t+1)(3t+5)}{3} \right\rfloor + 1 = 3t^2 + 6t + 2.$$

Let $a = 1$ and $b = 3t + 2$. Let $n \in [0, m_0)$. If $(t+1)b \leq n < m_0$, then

$$\begin{aligned} 0 \leq n - (t+1)b &\leq m_0 - 1 - (t+1)b \\ &= (3t^2 + 6t + 2) - 1 - (t+1)(3t+2) = t - 1. \end{aligned}$$

It therefore follows from

$$(n - (t+1)b) + (t+1) \leq (t-1) + (t+1) = 2t < d$$

that

$$n = (n - (t+1)b) \cdot 1 + (t+1) \cdot b \in dA_0.$$

Next, we assume that $ub \leq n < (u+1)b$ for some integer u with $0 \leq u \leq t$. Noting that

$$(u + t + 2)b - m_0 = ub + 2t + 2 = (u+1)b - t,$$

we see that

$$ub < (u + t + 2)b - m_0 < (u+1)b.$$

As in CASE I, we further divide the argument into two subcases.

SUBCASE IIA. If $ub \leq n < (u + t + 2)b - m_0$, then

$$\begin{aligned} 0 \leq n - ub &\leq (u + t + 2)b - m_0 - 1 - ub = (t+2)b - m_0 - 1 \\ &= (t+2)(3t+2) - (3t^2 + 6t + 2) - 1 = 2t + 1. \end{aligned}$$

Therefore, $n = (n - ub) \cdot 1 + ub \in dA_0$ because

$$(n - ub) + u \leq t + 2t + 1 = 3t + 1 = d.$$

SUBCASE IIB. If $(u+t+2)b - m_0 \leq n < (u+1)b$, then

$$\begin{aligned} 0 \leq n - ((u+t+2)b - m_0) &\leq (u+1)b - 1 - ((u+t+2)b - m_0) \\ &= m_0 - 1 - (t+1)b \\ &= 3t^2 + 6t + 2 - (t+1)(3t+2) - 1 = t - 1. \end{aligned}$$

Noting that

$$(n - ((u+t+2)b - m_0)) + (u+t+2) \leq (t-1) + t + t + 2 = 3t + 1 = d,$$

we have

$$n \equiv n + m_0 = (n - (u+t+2)b - m_0)a + (u+t+2)b \in dA_0.$$

CASE III. Suppose that $d = 3t+2$ for some nonnegative integer t. Then

$$m_0 = \left\lfloor \frac{(3t+2)(3t+6)}{3} \right\rfloor + 1 = 3t^2 + 8t + 5.$$

Let $a = 1$ and $b = 3t+4$. Let $n \in [0, m_0)$. If $(t+1)b \leq n < m_0$, then

$$0 \leq n - (t+1)b \leq m_0 - 1 - (t+1)b = 3t^2 + 8t + 5 - 1 - (t+1)(3t+4) = t.$$

Therefore,

$$(n - (t+1)b) + (t+1) \leq t + (t+1) = 2t + 1 < d,$$

which implies that $n = (n - (t+1)b) \cdot 1 + (t+1) \cdot b \in dA_0$.

Now assume that $ub \leq n < (u+1)b$ for some integer u with $0 \leq u \leq t$. It is clear that

$$ub < (u+t+2)b - m_0 < (u+1)b.$$

If $ub \leq n < (u+t+2)b - m_0$, then

$$\begin{aligned} n - ub &\leq ((u+t+2)b - m_0) - 1 - ub \\ &= (t+2)(3t+4) - (3t^2 + 8t + 5) - 1 = 2t + 2. \end{aligned}$$

Therefore, $(n-ub)+u \leq 2t+2+t = d$ implies that

$$n = (n-ub)\cdot 1 + u \cdot b \in dA_0.$$

If $(u+t+2)b - m_0 \leq n < (u+1)b$, then

$$\begin{aligned} n - ((u+t+2)b - m_0) &\leq (u+1)b - 1 - ((u+t+2)b - m_0) \\ &= m_0 - (t+1)b - 1 \\ &= (3t^2+8t+5) - (t+1)(3t+4) - 1 = t. \end{aligned}$$

Hence,

$$(n-((u+t+2)b-m_0)) + (u+t+2) \leq t + (t+t+2) = 3t+2 = d,$$

which implies that

$$n \equiv n + m_0 = (n-((u+t+2)b-m_0))\cdot 1 + (u+t+2)\cdot b \in dA_0.$$

Summarizing the above three cases, we conclude that

$$m(d,2) \geq m_0 = \left\lfloor \frac{d(d+4)}{3} \right\rfloor + 1 \qquad \text{for all } d \geq 2. \qquad \square$$

4.3 Case $k = 3$

It seems more complex to handle bases for $\mathbb{Z}_m$ when compared with bases for $[1,m]$. An exact formula for $m(d,3)$, is yet to be discovered. We now turn our attention to the estimates for $m(d,3)$. In this section, we prove a lower bound for $m(d,3)$ by constructing a good d-basis, which was first proved by Hsu and Jia (1994).

Theorem 13. *$m(d,3) \geq \frac{1}{16}d^3 + \frac{3}{8}d^2 + O(d)$ as $d \to \infty$.*

Proof. Let $d \geq 4$ be a positive integer. Define

$$r = \lfloor d/4 \rfloor, \qquad b = 3d - 8r + 5,$$
$$c = rb + d - 3r + 2, \qquad m_0 = rc + 2d - 6r + 3.$$

Define $A = \{1, b, c\}$, and denote $A_0 = \{0\} \cup A$. Then

$$m_0 = rc + 2d - 6r + 3 = r^2 b + rd - 3r^2 + 2r + 2d - 6r + 3$$
$$= r^2(3d - 8r + 2) + r(d - 4) + 2d + 3 = \frac{1}{16}d^3 + \frac{3}{8}d^2 + \gamma(d),$$

where $\gamma(d)$ is linear in d with coefficients depending only on d modulo 4. Therefore, we only need to show that A is a d-basis for $\mathbb{Z}_{m_0}$, i.e., $dA_0 = \mathbb{Z}_{m_0}$.

For any nonnegative integers v, w with $v + w < d$, define

$$I_{v,w} = [vb + wc,\ vb + wc + d - v - w].$$

Let $v,\ w \in [1, r]$. Then $v + w \leq 2r < d$. If $n \in I_{v,w}$, then n can be written as

$$n = (n - vb - wc) \cdot 1 + vb + wc.$$

Since $n - vb - wc \geq 0$ and

$$n - vb - wc + v + w \leq d - v - w + v + w = d,$$

we see that $n \in dA_0$. Hence, $I_{v,w} \subseteq dA_0$. Similarly, for any $v,\ w \in [1, r]$, we have

$$I_{r+v,w} \subseteq dA_0 \qquad \text{and} \qquad I_{v,r+w} \subseteq dA_0.$$

The basic idea in the proof is to arrange all these intervals modulo m_0 to cover an interval of length m_0.

It follows from $d - (v - 1) - w \leq d - 2r + 1 < d$ that $I_{v-1,w} \subseteq dA_0$. Since

$$b = 3d - 8r + 5 \qquad \text{and} \qquad m_0 = rc + 2d - 6r + 3,$$

we see

$$\begin{aligned} m_0 + (v-1)b + wc + d - (v-1) - w & \\ &\geq m_0 + vb - b + wc + d - 2r + 1 \\ &= (rc + 2d - 6r + 3) + vb - (3d - 8r + 5) + wc + d - 2t + 1 \\ &= vb + (r+w)c - 1. \end{aligned}$$

Hence,

$$[m_0 + (v-1)b + wc,\ vb + (r+w)c - 1] \subseteq dA_0. \tag{4.2}$$

Similarly, it follows from the definition of m_0, b, and c that

$$\begin{aligned} m_0 + (r+v)b + (w-1)c - 1 & \\ &= (rc + 2d - 6r + 3) + rb + vb + wc - (rb + d - 3r + 2) - 1 \\ &= vb + (r+w)c + d - 3r \\ &\leq vb + (r+w)c + d - v - (r+w). \end{aligned}$$

Since $v + (r+w) \leq 3r < d$, $I_{v,r+w} \subseteq dA_0$. Hence,

$$[vb + (r+w)c,\ m_0 + (r+v)b + (w-1)c - 1] \subseteq dA_0. \tag{4.3}$$

Noting that $c = rb + d - 3r + 2$, we see

$$\begin{aligned} m_0 + (r+v)b + (w-1)c + d - (r+v) - (w-1) & \\ &\geq m_0 + vb + wc - c + rb + d - 3r + 1 \\ &= m_0 + vb + wc - 1. \end{aligned}$$

Hence, $m_0 + I_{r+v,w-1} \subseteq dA_0$ implies that

$$[m_0 + (r+v)b + (w-1)c,\ m_0 + vb + wc - 1] \subseteq dA_0. \tag{4.4}$$

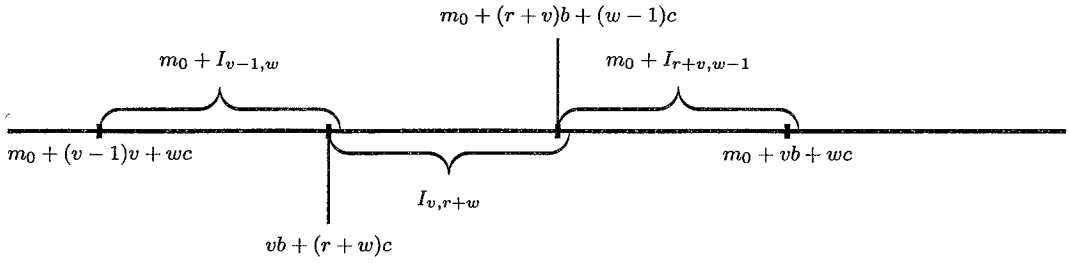


Figure 4.1: Coverage of $[m_0 + (v-1)b + wc,\ m_0 + vb + wc - 1]$

Therefore, it follows from (4.2), (4.3), and (4.4) that

$$[m_0 + (v-1)b + wc,\ m_0 + vb + wc - 1] \subseteq dA_0 \qquad \text{for all } v, w \in [1, r].$$

This implies that

$$[m_0 + wc,\ m_0 + rb + wc - 1] \subseteq dA_0 \qquad \text{for all } w \in [1, r]. \tag{4.5}$$

When $r \geq 1$, we have

$$\begin{aligned} rb + wc + d - r - w &\geq rb + wc + d - 2r \\ &= wc + (rb + d - 3r + 2) + r - 2 \\ &\geq (w+1)c - 1, \end{aligned}$$

which implies that

$$[m_0 + rb + wc,\ m_0 + (w+1)c - 1] \subseteq dA_0.$$

It then follows from (4.5) that

$$[m_0 + wc,\ m_0 + (w+1)c - 1] \subseteq dA_0 \qquad \text{for all} \quad 1 \leq w \leq r.$$

Therefore, we have

$$[m_0 + c,\ m_0 + (r+1)c - 1] \subseteq dA_0. \tag{4.6}$$

When $d \geq 12$, we have $r = \lfloor d/4 \rfloor \geq 3$. Then

$$\begin{aligned}(r+1)c + d - (r+1) &= m_0 + c - d + 5r - 4 \\ &\geq m_0 + c + r - 4 \\ &\geq m_0 + c - 1.\end{aligned}$$

Hence, the fact that $I_{0,r+1} \subseteq dA_0$ implies that $[m_0 + (r+1)c,\ 2m_0 + c - 1] \subseteq dA_0$ when $d \geq 12$. Then

$$[m_0 + c,\ 2m_0 + c - 1] \subseteq dA_0.$$

This proves that $dA_0 = \mathbb{Z}_{m_0}$, i.e., the diameter of $\mathrm{Cay}(\mathbb{Z}_{m_0}, A)$ is at most d. The proof of the theorem is complete. □

4.4 General Case

The following theorem can be used to construct large efficient generating sets A so that $m(d, A)$ is large by using small efficient generating sets.

Theorem 14. *Let $d_1 \geq 2$, $d_2 \geq 2$, $k_1 \geq 1$, and $k_2 \geq 1$ be integers. Then*

$$m(d_1 + d_2, k_1 + k_2) \geq m(d_1, k_1)m(d_2, k_2).$$

Proof. Let $A_s = \{0 < a_{s1} < a_{s2} < \cdots < a_{sk_s}\}$ be a set of integers with

$$m(d_s, A_s) = m(d_s, k_s) = m_s \qquad \text{for} \quad s = 1, 2.$$

We may assume, without loss of generality, that $a_{sk_s} < m_s$ for $s = 1, 2$. Define

$$A = A_1 \cup \{m_1 a_{2j} \mid j = 1, 2, \ldots, k_2\}.$$

Since $|A| = k_1 + k_2$, we only need to prove that A is a $(d_1 + d_2)$-basis for $\mathbb{Z}_{m_1 m_2}$.

Let n be any nonnegative integer. Since A_1 is an d_1-basis for $\mathbb{Z}_{m_1}$, we see that

$$n \equiv \sum_{i=1}^{k_1} x_i a_{1i} \pmod{m_1},$$

where x_i's are nonnegative integers with $\sum_{i=1}^{k_1} x_i \leq d_1$. Assume

$$n = \sum_{i=1}^{k_1} x_i a_{1i} + q m_1$$

for some integer q. It follows from the fact that A_2 is a d_2-basis for $\mathbb{Z}_{m_2}$ that

$$q = \sum_{j=1}^{k_2} y_j a_{2j} + p m_2,$$

where y_j's are nonnegative integers with $\sum_{j=1}^{k_2} y_j \leq d_2$, and p is an integer. Therefore,

$$n \equiv \sum_{i=1}^{k_1} x_i a_{1i} + \sum_{j=1}^{k_2} y_j m_1 a_{2j} \pmod{m_1 m_2},$$

where

$$\sum_{i=1}^{k_1} x_i + \sum_{j=1}^{k_2} y_j \leq d_1 + d_2.$$

This implies that $n \in (d_1 + d_2)A_0$, where $A_0 = A \cup \{0\}$. Hence, A is a $(d_1 + d_2)$-basis for $\mathbb{Z}_{m_1 m_2}$. Therefore,

$$m(d_1, k_1)m(d_2, k_2) = m_1 m_2 \leq m(d_1 + d_2, k_1 + k_2).$$

The proof is complete. □

Theorem 15. *Let d be a sufficiently large positive integer. Let $r = \lfloor d/5 \rfloor$ and define*

$$b = 4d - 15r + 7, \qquad c = ar + d - 4r + 2,$$

$$d = br + 2d - 4r + 4, \qquad m = cr + 3d - 12r + 5.$$

Then $A = \{1, b, c, d\}$ *is a* d*-basis for* $\mathbb{Z}_m$*. Therefore,*

$$m(d,4) \geq \frac{1}{125}d^4 + O(d^3) \qquad as \quad d \to \infty. \tag{4.7}$$

If interested, a proof can be found in (Jia, 1992). Now we are ready to prove the following lower bound for $m(d,k)$ for any fixed $k \geq 4$ as d approaches infinity.

Theorem 16. *For fixed* $k \geq 4$ *as* $d \to \infty$*,*

$$m(d,k) \geq \varepsilon_k \left(\frac{256}{125}\right)^{\lfloor k/4 \rfloor} \left(\frac{d}{k}\right)^k + O(d^{k-1}),$$

where

$$\varepsilon_k = \begin{cases} 1, & \text{if } k \equiv 0 \text{ or } 1 \pmod 4 \\ \frac{4}{3}, & \text{if } k \equiv 2 \pmod 4 \\ \frac{27}{16}, & \text{if } k \equiv 3 \pmod 4 \end{cases}.$$

Proof. Recall that

$$\begin{aligned} m(d,1) &= d+1, \\ m(d,2) &= \left\lfloor \frac{d(d+2)}{3} \right\rfloor + 1 = \frac{1}{3}d^2 + O(d), \\ m(d,3) &\geq \frac{1}{16}d^3 + O\left(d^2\right). \end{aligned}$$

Therefore, for $1 \leq r \leq 3$, we have

$$m(d,r) \geq \varepsilon_r \left(\frac{d}{r}\right)^r + O\left(d^{r-1}\right),$$

where ε_r is defined as in the theorem.

Now we assume that

$$d = ku + v \qquad \text{and} \qquad k = 4q + r$$

where $0 \le v < k$ and $0 \le r \le 3$. For convenience, let $m(0,0) = 1$. Then

$$\begin{aligned}
m(d,k) &= m(ku+v,k) \\
&\ge m(4qu+ru, 4q+r) \\
&\ge m(4qu,4q)\cdot m(ru,r) \\
&\ge m(4u,4)^q \cdot \left(\varepsilon_r u^r + O(u^{r-1})\right) \\
&\ge \left(\frac{256}{125}u^4 + O(u^3)\right)^q \left(\varepsilon_r u^r + O(u^{r-1})\right) \\
&= \varepsilon_r \left(\frac{256}{125}\right)^q u^{4q+r} + O\left(u^{4q+r-1}\right) \\
&= \varepsilon_r \left(\frac{256}{125}\right)^q \left(\frac{d-v}{k}\right)^k + O\left(\left(\frac{d-v}{k}\right)^{k-1}\right) \\
&= \varepsilon_r \left(\frac{256}{125}\right)^{\lfloor k/4 \rfloor} \left(\frac{d}{k}\right)^k + O\left(d^{k-1}\right).
\end{aligned}$$

This proves the theorem. □

4.5 Remarks

The lower bound of Wong and Coppersmith has been improved several times by various authors. The best known lower bound was proved by Su in early 1990's. Jia and Su (1997) proved

$$\begin{aligned}
m(d,k) &\ge \tau_k \left(\frac{5^5 \cdot 7^4}{17^5}\right)^{\lfloor k/5 \rfloor} \left(\frac{d}{k}\right)^k + O(d^{k-1}) \\
&\approx \tau_k (5.2844)^{\lfloor k/5 \rfloor} \left(\frac{d}{k}\right)^k + O(d^{k-1}),
\end{aligned}$$

where

$$\tau_k = \begin{cases} 1, & \text{if } k \equiv 0,1 \pmod 5 \\ \dfrac{4}{3}, & \text{if } k \equiv 2 \pmod 5 \\ \dfrac{4752}{2197} \approx 2.163, & \text{if } k \equiv 3 \pmod 5 \\ \dfrac{165888}{50625} = 3.2768, & \text{if } k \equiv 4 \pmod 5 \end{cases}.$$

Chapter 5

GEOMETRIC REPRESENTATION OF $\mathbb{Z}_m$

In this chapter, we will introduce a geometric representation of $\mathbb{Z}_m$, the cyclic group of residue classes modulo m. This method was introduced by Wong and Coppersmith (1974). In order to do so, we first introduce a special function called the A-norm, where A is a generating set of $\mathbb{Z}_m$.

5.1 A-norm and Minimal Representations

Let d, k, and m be positive integers. Let $A = \{a_1, a_2, \ldots, a_k\}$ be a d-basis for $\mathbb{Z}_m$. Then every element $s \in \mathbb{Z}_m$ can be written as a linear combination

$$\sum_{i=1}^{k} a_i x_i \equiv s \pmod{m},$$

where $x_1, \ldots, x_k$ are nonnegative integers with $\sum_{i=1}^{k} x_i \leq d$. For some elements in $\mathbb{Z}_m$, the number of elements in A needed in the above representations may be less than d. The *A-norm* of an element $s \in \mathbb{Z}_m$, denoted as $||s||_A$, is the smallest nonnegative integer ℓ such that s is a sum of ℓ not necessarily distinct elements in A. In other words,

$$||s||_A = \min\left\{ \ell \;\middle|\; s = \sum_{i=1}^{k} a_i x_i, \quad \sum_{i=1}^{k} x_i \leq \ell \quad \text{and } x_i \geq 0 \text{ integers} \right\}.$$

Example 6. Let $A = \{1, 3\}$. Then A is a generating set for $\mathbb{Z}_9$. It can be verified that

the following are the "shortest" representations by A:

$$0 = 1\cdot 0 + 3\cdot 0, \qquad 1 = 1\cdot 1 + 3\cdot 0, \qquad 2 = 1\cdot 2 + 3\cdot 0,$$
$$3 = 1\cdot 1 + 3\cdot 1, \qquad 4 = 1\cdot 1 + 3\cdot 1, \qquad 5 = 1\cdot 2 + 3\cdot 1,$$
$$6 = 1\cdot 0 + 3\cdot 2, \qquad 7 = 1\cdot 1 + 3\cdot 2, \qquad 8 = 1\cdot 2 + 3\cdot 2.$$

Hence,

s	0	1	2	3	4	5	6	7	8
$\|\|s\|\|_A$	0	1	2	1	2	3	2	3	4

Therefore, A is a 4-basis for $\mathbb{Z}_9$.

Example 7. Let $A = \{1, 7\}$. Then A is a 5-basis for $\mathbb{Z}_{10}$. Note that $||6||_A = 4$ because $6 \equiv 1\cdot 2 + 7\cdot 2 \pmod{10}$.

Example 8. Let $A = \{1, 11\}$. Then it can be verified that A is a 10-basis for $\mathbb{Z}_{47}$. It can be verified (see Figure 5.3) that

$$||0||_A = 0, \quad ||13||_A = 3, \quad ||28||_A = 8, \quad ||43||_A = 10, \quad \text{and} \quad ||44||_A = 4.$$

If $A = \{1, 11, 78\}$, then the A-norm of 113 in $\mathbb{Z}_{138}$ is 6.

Proposition 5. *Let $s, t \in \mathbb{Z}_m$, and let A be a subset of $\mathbb{Z}_m$. Then*

(*i*) $||s + t||_A \leq ||s||_A + ||t||_A$;

(*ii*) $||\alpha s||_A \leq \alpha ||s||_A$ *for any nonnegative integer* α.

Proposition 6. *Let $A = \{a_1, a_2, \ldots, a_k\}$ be a subset of $\mathbb{Z}_m$, and $s \in \mathbb{Z}_m$. Assume that*

$$s + a_{i_0} = \sum_{i=1}^{k} x_i a_i, \qquad \textit{where} \qquad ||s + a_{i_0}||_A = \sum_{i=1}^{k} x_i.$$

If $||s + a_{i_0}||_A \leq ||s||_A$, then $x_{i_0} = 0$.

Proof. Suppose that $x_{i_0} \geq 1$. Then

$$s = (s + a_{i_0}) - a_{i_0} = \sum_{i=1}^{k} x_i a_i - a_{i_0} = \sum_{i \neq i_0} x_i a_i + (x_{i_0} - 1)a_{i_0}$$

is a valid representation of s by A, which implies that

$$||s||_A \leq \sum_{i \neq i_0} x_i + (x_{i_0} - 1) = \sum_{i=1}^{k} x_i - 1 = ||s + a_{i_0}||_A - 1 \leq ||s||_A - 1,$$

which is a contradiction. □

Proposition 7. *Let $A = \{a_1, a_2, \ldots, a_k\}$ be a subset of $\mathbb{Z}_m$, and $s \in \mathbb{Z}_m$. If*

$$||s - a_i||_A \geq ||s||_A \qquad \textit{for all} \quad i = 1, 2, \ldots, k,$$

then $s = 0$.

Proof. If $s \neq 0$, then s can be written as

$$s = \sum_{i=1}^{k} x_i a_i \qquad \text{and} \qquad ||s||_A = \sum_{i=1}^{k} x_i,$$

where at least one x_i is positive, say, $x_1 \geq 1$. Then

$$s - a_1 = (x_1 - 1)a_1 + x_2 a_2 + \cdots + x_k a_k,$$

which implies that

$$||s - a_1||_A \leq (x_1 - 1) + x_2 + \cdots + x_k = ||s||_A - 1,$$

which is a contradiction. □

5.2 Ordering of 2-Dimensional Lattice Points

Before describing the geometric representation of $\mathbb{Z}_m$, an ordering of the lattice points in the first quadrant of $\mathbb{R}^2$ is introduced. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$

be two lattice points in the first quadrant, i.e., x_1, x_2, y_1, and y_2 are all nonnegative integers. We say that $P \preccurlyeq Q$ if

$$x_1 + y_1 < x_2 + y_2$$

or

$$y_1 \leq y_2 \qquad \text{when} \qquad x_1 + y_1 = x_2 + y_2.$$

If $P \preccurlyeq Q$ and $P \neq Q$, we write $P \prec Q$. It is easy to see that $\prec$ is a total ordering of the set of all lattice points in the first quadrant of $\mathbb{R}^2$ as shown in Figure 5.1.

$$\begin{aligned}(0,0) &\prec (1,0) \prec (0,1)\\ &\prec (2,0) \prec (1,1) \prec (0,2)\\ &\prec (3,0) \prec (2,1) \prec (1,2) \prec (0,3)\\ &\prec (4,0) \prec (3,1) \prec (2,2) \prec (1,3) \prec (0,4)\\ &\prec (5,0) \prec (5,1) \prec (5,2) \prec (5,3) \prec (5,4) \prec (5,5)\\ &\prec \cdots\cdots\end{aligned}$$

Figure 5.1: Total ordering of lattice points in the first quadrant of $\mathbb{R}^2$.

Definition 17. Let d and m be positive integers. Assume that $A = \{a, b\}$ is a d-basis for $\mathbb{Z}_m$. The following representation of $s \in \mathbb{Z}_m$ as a linear combination of the elements in A

$$s \equiv ax + by \pmod{m} \qquad (x \text{ and } y \text{ are nonnegative integers})$$

is said to be *minimal* if

$$s \equiv ax' + by' \pmod{m} \qquad \text{implies} \qquad (x, y) \preccurlyeq (x', y'),$$

where x' and y' are nonnegative integers.

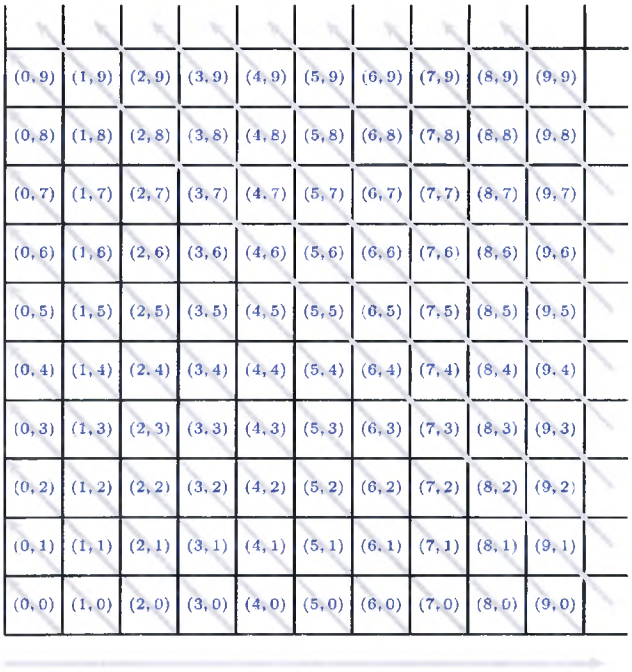


Figure 5.2: Ordering of the lattice points in $\mathbb{R}^2$.

It follows immediately from the definition that every element in $\mathbb{Z}_m$ has a unique minimal representation by a d-basis $A = \{a, b\}$. It is also easy to see that $||s||_A = x+y$ if $s = ax + by$ is a minimal representation of $s \in \mathbb{Z}_m$. However, the converse is not true. For instance, $A = \{1, 11\}$ is a 10-basis for $\mathbb{Z}_{20}$. Then both representations

$$13 \equiv 1 \cdot 0 + 11 \cdot 3 \equiv 1 \cdot 2 + 11 \cdot 1 \pmod{20}$$

give $||13||_A = 3$. But only one is a minimal representation of 13 by A in $\mathbb{Z}_{20}$.

5.3 Geometric Representation of $\mathbb{Z}_m$

Definition 18. Let $A = \{a, b\}$ be a d-basis for $\mathbb{Z}_m$. The *A-representation* of $\mathbb{Z}_m$, denoted as $\mathscr{G}(A, m)$, is the set of all the lattice points (x, y) in the first quadrant such that $\xi(x, y) = ax + by$ is the minimal representation in $\mathbb{Z}_m$.

Let $A = \{a, b\}$ be a d-basis for $\mathbb{Z}_m$. Because each element $s \in \mathbb{Z}_m$ has a unique minimal representation by using $A = \{a, b\}$, ξ is a one-to-one and onto function from $\mathscr{G}(A, m)$ to $\mathbb{Z}_m$. This function ξ may be regarded as a function from $\mathbb{Z}^2 \to \mathbb{Z}_m$ with $\xi(x, y) = ax + by$, where $\mathbb{Z}^2$ is the set of all integer lattice points in $\mathbb{R}^2$.

This geometric representation of $\mathbb{Z}_m$ by a generating set A was first introduced by Wong and Coppersmith (1974). This representation can be generalized to arbitrary k generators which will be discussed later in this chapter.

The A-representation of $\mathbb{Z}_m$ is often displayed by using a chart of lattice points (x, y) arranged at their relative locations and filled with its labeling $\xi(x, y) = ax + by \in \mathbb{Z}_m$. With this arrangement, the A-norm $||s||_A$ of an element is equal to the L^1-norm in $\mathbb{Z}^2$. In other words,

$$||s||_A = ||(x, y)||_{L^1} = x + y,$$

where $s = \xi(x, y) = ax + by \in \mathbb{Z}_m$ is the minimal representation of s.

For example, Figure 5.3 shows the A-representation of $\mathbb{Z}_{65}$, where $A = \{5, 21\}$, followed by two more examples of geometric representations.

59	64	4	9	14			
38	43	48	53	58			
17	22	27	32	37			
61	1	6	11	16			
40	45	50	55	60			
19	24	29	34	39	44	49	54
63	3	8	13	18	23	28	33
42	47	52	57	62	2	7	12
21	26	31	36	41	46	51	56
0	5	10	15	20	25	30	35

Figure 5.3: $\mathscr{G}(A, 65)$, the A-representation of $\mathbb{Z}_{65}$ with $A = \{5, 21\}$.

60	67	4	11	18	25	32	39	46	53
50	57	64	1	8	15	22	29	36	43
40	47	54	61	68	5	12	19	26	33
30	37	44	51	58	65	2	9	16	23
20	27	34	41	48	55	62	69	6	13
10	17	24	31	38	45	52	59	66	3
0	7	14	21	28	35	42	49	56	63

41	42	43					
30	31	32					
19	20	21					
8	9	10					
44	45	46					
33	34	35	36	37	38	39	40
22	23	24	25	26	27	28	29
11	12	13	14	15	16	17	18
0	1	2	3	4	5	6	7

Figure 5.4: A-representation of $\mathbb{Z}_{70}$ with $A = \{7, 10\}$ (left) and A-representation of $\mathbb{Z}_{47}$ with $A = \{1, 11\}$ (right).

Let A be a set of integers. Let $d(A, \mathbb{Z}_m)$ denote the smallest positive integer d such that A is a d-basis for $\mathbb{Z}_m$.

Theorem 17 (Wong and Coppersmith, 1974). *Let $A = \{a, b\}$ be a set of integers with $\gcd(a, b) = 1$. If m is a positive integer, then $\mathcal{G}(A, m)$ is of the form as shown in Figure 5.5, where $u \geq 0$, $v \geq 0$, $p > 0$ and $q > 0$. Therefore,*

$$d(A, \mathbb{Z}_m) = u + q + \max\{v, p\} - 2.$$

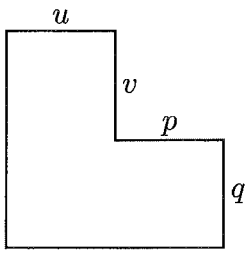


Figure 5.5: $\mathcal{G}(A, m)$, the geometric representation of $\mathbb{Z}_m$ by $A = \{a, b\}$.

In order to prove this theorem, the following lemma is needed.

Lemma 1. *Let $A = \{a, b\}$ with $\gcd(a, b) = 1$. If $(x_0, y_0) \notin \mathcal{G}(A, m)$, then $(x, y) \notin \mathcal{G}(A, m)$ for all lattice points (x, y) with*

$$x \geq x_0 \qquad \text{and} \qquad y \geq y_0.$$

Proof. If not, then there exists $(x_1, y_1) \in \mathscr{G}(A, m)$ with $(x_0, y_0) \prec (x_1, y_1)$. Assume without loss of generality, that (x_1, y_1) is such a lattice point that is closest to (x_0, y_0) and $x_1 > x_0$ and $y_1 \geq y_0$. Since $(x_1 - 1, y_1) \notin \mathscr{G}(A, m)$, it follows from the construction of $\mathscr{G}(A, m)$ that there exists a lattice $(x_2, y_2) \in \mathscr{G}(A, m)$ with $(x_2, y_2) \prec (x_1 - 1, y_1)$ such that

$$ax_2 + by_2 \equiv a(x_1 - 1) + by_1 \pmod{m}.$$

Therefore,

$$a(x_2 + 1) + by_2 \equiv ax_1 + by_1 \pmod{m}.$$

Since $(x_2 + 1, y_2) \prec (x_1, y_1)$, we see $(x_1, y_1) \notin \mathscr{G}(A, m)$, which is a contradiction. □

Proof of Theorem 17. For convenience, let $R = \mathscr{G}(A, m)$. It follows from Lemma 1 that R shapes as shown in Figure 5.6.

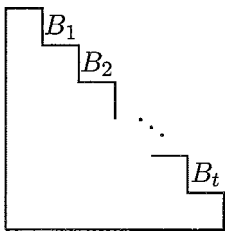


Figure 5.6: In $\mathscr{G}(A, m)$, the number of B_i corners must be at most one.

It only needs to be shown that R contains at most one corner like B_i as shown in the above figure.

First, for each $i : 1 \leq i \leq t$, assume that $(x_i, y_i) \in B_i$ with

$$(x_i - 1, y_i) \in R \qquad \text{and} \qquad (x_i, y_i - 1) \in R.$$

Since $(x_i, y_i) \notin R$, there is a lattice point $(x_i', y_i') \in R$ such that

$$ax_i + by_i \equiv ax_i' + by_i' \pmod{m}.$$

We claim that $(x_i', y_i') = (0,0)$. Otherwise, then either $(x_i'-1, y_i') \in R$ or $(x_i', y_i'-1) \in R$ or both, say, $(x_i'-1, y_i') \in R$. Since

$$a(x_i-1)+by_i = ax_i+by_i-a \equiv ax_i'+by_i'-a = a(x_i'-1)+by_i' \pmod m,$$

we see that $(x_i'-1, y_i') \in R$ implies $(x_i-1, y_i) \notin R$, a contradiction. Therefore,

$$ax_i+by_i \equiv a\cdot 0+b\cdot 0 \equiv 0 \pmod m.$$

Assume that $t > 1$. Since

$$ax_i+by_i \equiv 0 \pmod m, \qquad \text{for} \quad i = 1,2,\ldots,t,$$

we see that, in particular,

$$a(x_1-1)+by_1 \equiv a(x_2-1)+by_2 \pmod m.$$

This is a contradiction because both (x_1-1, y_1) and (x_2-1, y_2) are in R. Therefore $t = 1$, i.e., R has at most one corner that is strictly inside the first quadrant as shown in Figure 5.5. □

5.4 Tiling $\mathbb{Z}^2$

Let $A = \{a, b\}$ be a d-basis for $\mathbb{Z}_m$. Define

$$L_0 = \{(x_0, y_0) \in \mathbb{Z}^2 \mid ax_0+by_0 \equiv 0 \pmod m\}.$$

If $(x_0, y_0) \in L_0$, then

$$ax+by \equiv a(x_0+x)+b(y_0+y) \pmod m \qquad \text{for all } (x,y) \in \mathscr{G}(A,m).$$

Hence, $\xi(x,y) = \xi(x_0+x, y_0+y)$ for all $(x,y) \in \mathscr{G}(A,m)$. This means that $\mathscr{G}(A,m)$ and its translation by (x_0, y_0)

$$(x_0, y_0)+\mathscr{G}(A,m) = \{(x_0+x, y_0+y) \mid (x,y) \in \mathscr{G}(A,m)\}$$

have the same labeling ξ. Note that the translation has the same shape as the original $\mathscr{G}(A, m)$.

On the other hand, if $(x, y) \in \mathbb{Z}^2$ is a lattice point, then $\xi(x, y) = \xi(x', y')$ for some $(x', y') \in \mathscr{G}(A, m)$. Then

$$\xi(x - x', y - y') = a(x - x') + b(y - y') = \xi(x, y) - \xi(x', y') \equiv 0 \pmod{m}.$$

Let $x_0 = x - x'$ and $y_0 = y - y'$. Then

$$(x, y) = (x_0, y_0) + (x', y'),$$

which implies that $(x, y) \in (x_0, y_0) + \mathscr{G}(A, m)$. Therefore, the following theorem is obtained.

Theorem 18. *Let $A = \{a, b\}$ be a d-basis for $\mathbb{Z}_m$ for some integer d. Then*

(a) $\mathbb{Z}^2 = \bigcup_{(x_0, y_0) \in L_0} ((x_0, y_0) + \mathscr{G}(A, m))$;

(b) $((x_0', y_0') + \mathscr{G}(A, m)) \cap ((x_0'', y_0'') + \mathscr{G}(A, m)) = \emptyset$ *for all* $(x_0', y_0') \in L_0$ *and* $(x_0'', y_0'') \in L_0$ *with* $(x_0', y_0') \neq (x_0'', y_0'')$.

In other words, $\mathbb{Z}^2$ can be tiled by $\mathscr{G}(A, m)$ as shown in Figure 5.7.

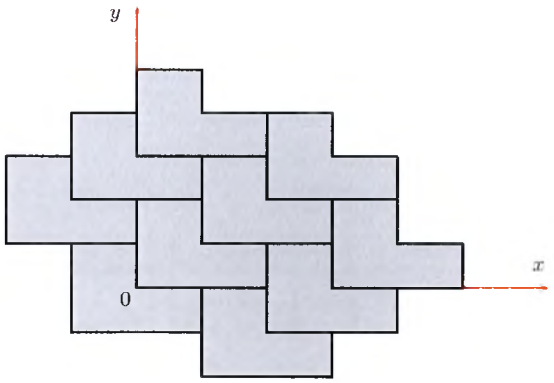


Figure 5.7: $\mathscr{G}(A, m)$ tiles $\mathbb{Z}^2$.

5.5 An Upper Bound for $m(d, 2)$

Theorem 19. *Let $d \geq 2$ be an integer. Then*

$$m(d,2) \leq \left\lfloor \frac{d(d+4)}{3} \right\rfloor + 1 \qquad \textit{for all} \quad d \geq 2. \tag{5.1}$$

Proof. First, we show that m_0 is indeed also an upper bound for $m = m(d, 2)$. Assume that $A = \{a, b\}$ is an optimal d-basis for $\mathbb{Z}_m$. Then Theorem 17 shows that the A-representation $\mathscr{G}(A, m)$ is an L-shaped block of m lattice points labelled with elements in $\mathbb{Z}_m$ as shown in Figure 5.5. We again divide this part of the proof into the following three cases.

CASE 1. Assume that $d = 3t$ for some positive integer t. It follows from Theorem 17 that

$$u + q + \max\{v, p\} - 2 \leq d = 3t.$$

The L-shaped A-representation $\mathscr{G}(A, m)$ of $\mathbb{Z}_m$ would contain the maximum number of lattice points when $u = q = t + 1$ and $v = p = t$, in which case we would have

$$m = (t+1)^2 + 2(t+1)t = 3t^2 + 4t + 1 = m_0.$$

CASE 2. Assume that $d = 3t + 1$ for some positive integer t. Then

$$u + q + \max(v, p) - 2 \leq d = 3t + 1, \tag{5.2}$$

where u, v, p and q are as defined in Theorem 17. It is easy to see that, when $u = v = p = q = t + 1$, the L-shaped $\mathscr{G}(A, m)$ would contain the maximum number of lattice points: $3(t+1)^2 = 3t^2 + 6t + 3 > m_0$. However, we prove that the A-representation $\mathscr{G}(A, m)$ of $\mathbb{Z}_m$ cannot have this shape with $u = v = p = q = t + 1$. Otherwise, then the number of lattice points in $\mathscr{G}(A, m)$ is $m = 3(t+1)^2$. The lattice point $(t+1, t+1)$ at the corner must represent 0 in $\mathbb{Z}_m$. Hence, as shown in Figure 5.8, we have

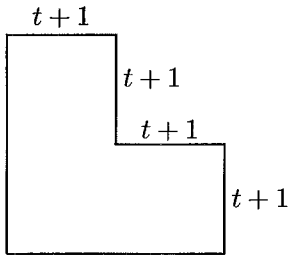


Figure 5.8: This cannot be an A-representation $\mathscr{G}(A,m)$ in any case.

$$(t+1)\cdot a+(t+1)\cdot b\equiv 0 \pmod{m},$$

which implies that

$$a+b\equiv 0 \pmod{3(t+1)}.$$

Then there exists an integer λ_0 such that

$$a+b-m=3(t+1)\lambda_0.$$

Noting that $m=3(t+1)^2$, we see that

$$a+b=m+3(t+1)\lambda_0=3(t+1)(t+1+\lambda_0)=3(t+1)\lambda,$$

where $\lambda=t+1+\lambda_0$. Since $1\le a<b<m=3(t+1)^2$, we see that $1\le\lambda<2(t+1)$. We claim that $\gcd(\lambda,t+1)=1$. Otherwise, we may write

$$\lambda=r\lambda' \quad\text{and}\quad t+1=rt' \qquad \text{for some integer } r \text{ with } \quad 2\le r\le t+1.$$

Then

$$\begin{aligned} t'\cdot a+t'\cdot b&=t'(a+b)=t'\cdot 3(t+1)\lambda\\ &=3(t+1)^2t'r\lambda'=3(t+1)^2\lambda'\equiv 0 \pmod{m}. \end{aligned}$$

Hence, the lattice point (t',t') also represents 0, i.e., $\xi(t',t')=0$. It is easy to see that $1\le t'<t+1$, which implies that $(t',t')\in\mathscr{G}(A,m)$. This is a contradiction

because there are at least two distinct lattice points, $(0,0)$ and (t',t'), both representing 0. Therefore, we must have $\gcd(\lambda, t+1) = 1$. This implies that the equation

$$\lambda x \equiv a \pmod{(t+1)}$$

has a solution $x_0 : \ t+2 \leq x_0 \leq 2t+1$. Then

$$\lambda x_0 = a + (t+1)\sigma \qquad \text{for some integer} \quad \sigma.$$

Therefore, we have

$$\begin{aligned} x_0 b &= x_0(a+b) - x_0 a \\ &= x_0 \cdot 3(t+1)\lambda - x_0 a \\ &= 3(t+1)(a+(t+1)\sigma) - x_0 a \\ &\equiv (3(t+1) - x_0)a \pmod{m}. \end{aligned}$$

This means

$$\begin{aligned} \xi(0, x_0) &= 0 \cdot a + x_0 \cdot b \\ &\equiv (3(t+1) - x_0) \cdot a + 0 \cdot b \\ &= \xi(3(t+1) - x_0, 0) \pmod{m}. \end{aligned}$$

However,

$$t+1 < x_0 \leq 2t+1 \qquad \text{and} \qquad t+1 \leq 3(t+1) - x_0 \leq 2t+1$$

imply that

$$(0, x_0) \in \mathscr{G}(A, m) \qquad \text{and} \qquad (3(t+1) - x_0, 0) \in \mathscr{G}(A, m).$$

Hence, we have two distinct lattice points $(0, x_0)$ and $(3(t+1) - x_0, 0)$ in $\mathscr{G}(A, m)$ representing the same value in $\mathbb{Z}_m$, which is a contradiction. This proves that, when

$d = 3t + 1$, the optimal L-shaped block with maximum number of lattice points cannot be a geometric representation by any generating set $A = \{a, b\}$. Therefore, the next best possible dimension for $\mathscr{G}(A, m)$ with maximum number of lattice points is

$$u = t + 1, \qquad q = t + 2, \qquad \text{and} \qquad p = v = t,$$

which gives

$$m = (t+1)(t+2) + t(t+1) + t(t+2) = 3t^2 + 6t + 2 = m_0.$$

CASE 3. Suppose that $d = 3t + 2$ for some nonnegative integer t. It is easy to see that the best possible dimension for $\mathscr{G}(A, m)$ is

$$u = v = p = t + 1 \qquad \text{and} \qquad q = t + 2.$$

Then

$$m = (t+1)(t+2) + (t+1)^2 + (t+1)(t+2) = 3t^2 + 8t + 5 = m_0.$$

Combining CASES 1, 2, and 3, we have that

$$m(d, 2) \leq m_0 = \left\lfloor \frac{d(d+4)}{3} \right\rfloor + 1 \qquad \text{for all} \quad d \geq 2.$$

This completes the proof of Theorem 12. □

Therefore, from the previous we have the following theorem.

Theorem 20 (Hsu and Jia (1994)). *Let $d \geq 2$ be an integer. Then*

$$m(d, 2) = \left\lfloor \frac{d(d+4)}{3} \right\rfloor + 1. \tag{5.3}$$

5.6 Ordering k-dimensional Lattice Points and Minimal A-Representations

In this section, the geometric representation of $\mathbb{Z}_m$ is extended by a generating A with k integers. This representation will be used in developing upper bound for $m(d, k)$ for arbitrary positive integers d and k. The A-representation of $\mathbb{Z}_m$ is k-dimensional if the generating set A contains k integers.

In order to describe the k-dimensional A-representation of $\mathbb{Z}_m$, the total ordering $\prec$ for the lattice points in the first quadrant of $\mathbb{R}^2$ defined earlier needs to be extended to one for the lattice points $\mathbb{N}^k$ where $\mathbb{N}$ is the set of all nonnegative integers.

Let $\mathbf{x} = (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k$. The *$L^1$-norm* of $\mathbf{x}$, denoted as $||\mathbf{x}||_{L^1}$, is defined by $||\mathbf{x}||_{L^1} = x_1 + x_2 + \cdots + x_k$.

The binary relation $\preccurlyeq$ for $\mathbb{N}^2$ is defined on page 45. Let k be a positive integer ≥ 3. Assume that a binary relation $\preccurlyeq$ on $\mathbb{N}^{k-1}$ is already defined. Now define a binary relation[1] $\preccurlyeq$ on $\mathbb{N}^k$ recursively as follows. Let $\mathbb{N}^k$ denote the set of all k-tuples of nonnegative integers. Let $\mathbf{x} = (x_1, \ldots, x_k) \in \mathbb{N}^k$ and $\mathbf{y} = (y_1, \ldots, y_k) \in \mathbb{N}^k$ be any two lattice points. We say that $\mathbf{x} \preccurlyeq \mathbf{y}$ if

(i) $||\mathbf{x}||_{L^1} < ||\mathbf{y}||_{L^1}$; or

(ii) $||\mathbf{x}||_{L^1} = ||\mathbf{y}||_{L^1}$ and $x_k < y_k$; or

(iii) $||\mathbf{x}||_{L^1} = ||\mathbf{y}||_{L^1}$ and $x_k = y_k$ and $(x_1, \ldots, x_{k-1}) \preccurlyeq (y_1, \ldots, y_{k-1})$ as elements in $\mathbb{N}^{k-1}$.

If $\mathbf{x} \preccurlyeq \mathbf{y}$ and $\mathbf{x} \neq \mathbf{y}$, we write $\mathbf{x} \prec \mathbf{y}$. In the 3-dimensional case, Figure 5.9 shows the ordering of lattice points in $\mathbb{N}^3$ arranged according to the ordering $\preccurlyeq$.

[1] Strictly speaking, different notations for the orderings $\preccurlyeq$ on $\mathbb{N}^k$ with different k's are needed.

$(0,0,0),\ (1,0,0),\ (0,1,0),\ (0,0,1),\ (2,0,0),\ (1,1,0),\ (0,2,0),\ (1,0,1),$
$(0,1,1),\ (0,0,2),\ (3,0,0),\ (2,1,0),\ (1,2,0),\ (0,3,0),\ (2,0,1),\ (1,1,1),$
$(0,2,1),\ (1,0,2),\ (0,1,2),\ (0,0,3),\ (4,0,0),\ (3,1,0),\ (2,2,0),\ (1,3,0),$
$(0,4,0),\ (3,0,1),\ (2,1,1),\ (1,2,1),\ (0,3,1),\ (2,0,2),\ (1,1,2),\ (0,2,2),$
$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$

Figure 5.9: Ordering of lattice points in $\mathbb{N}^3$

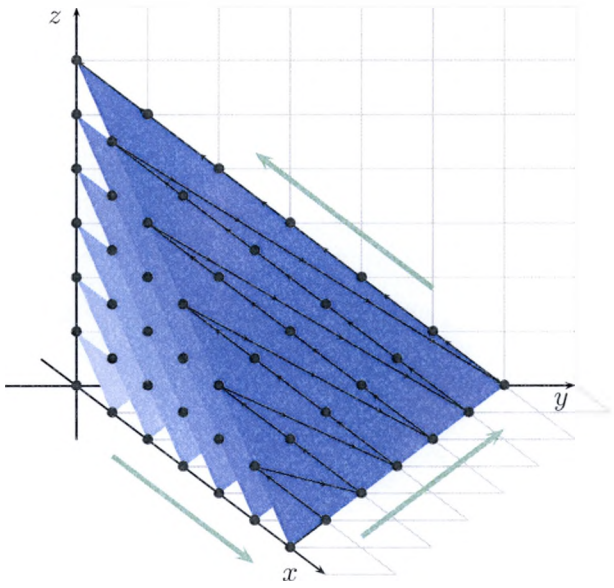


Figure 5.10: Ordering lattice points in $\mathbb{N}^3$.

Let $A = \{a_1 < a_2 < \cdots < a_k\}$ be a d-basis for $\mathbb{Z}_m$. We use $\mathbf{a}$ to denote the k-tuple with elements in A as the components, namely

$$\mathbf{a} = (a_1, a_2, \ldots, a_k).$$

Define $\xi_{\mathbf{a}} : \mathbb{N}^k \to \mathbb{Z}_m$ by

$$\xi_{\mathbf{a}}(\mathbf{x}) = \mathbf{a} \cdot \mathbf{x} = \sum_{i=1}^{k} a_i x_i \pmod{m} \qquad \text{for all } \mathbf{x} \in \mathbb{N}^k.$$

Let $s \in \mathbb{Z}_m$. Then

$$s \equiv \mathbf{a} \cdot \mathbf{x} = \sum_{i=1}^{k} a_i x_i \pmod{m}$$

is called a *minimal* representation of s by A (or a *minimal* A-representation of s) if

$$s \equiv \mathbf{a} \cdot \mathbf{y} \pmod{m} \qquad \text{implies} \qquad \mathbf{x} \preccurlyeq \mathbf{y}.$$

Example 9. Let $A = \{1, 11, 78\}$, then A is a 10-basis for $\mathbb{Z}_{138}$. It is easy to verify that

$$43 \equiv 3 \cdot 1 + 2 \cdot 11 + 2 \cdot 78 \pmod{138}$$

is a minimal representation of 43.

Let A be a d-basis for $\mathbb{Z}_m$. Since $\prec$ is a total ordering, we see that every element in $\mathbb{Z}_m$ has a unique minimal representation by A.

5.7 k-dimensional Geometric Representation

Definition 19. Let k be a positive integer and let $A = \{a_1 < a_2 < \cdots < a_k\}$ be a generating set of $\mathbb{Z}_m$. The *A-representation* of $\mathbb{Z}_m$, denoted by $\mathcal{G}(A, m)$, is the set of all the lattice points $\mathbf{x} = (x_1, \ldots, x_k) \in \mathbb{N}^k$ such that $\xi(\mathbf{x}) = \sum_{i=1}^{k} a_i x_i$ is the minimal representation in $\mathbb{Z}_m$.

For any given d-basis $A = \{a_1, \ldots, a_k\}$, the construction of the A-representation of $\mathbb{Z}_m$ is similar to that in the 2-dimensional case. We proceed to fill each lattice point $\mathbf{x} = (x_1, \ldots, x_k) \in \mathbb{N}^k$ with an element $s \in \mathbb{Z}_m$ where

$$s \equiv \sum_{i=1}^{k} a_i x_i \pmod{m}.$$

Start with the origin $(0, \ldots, 0)$, and then follow the ordering $\prec$ for the elements in $\mathbb{N}^k$. At each point $\mathbf{x}$ if the value s has not appeared so far, fill $\mathbf{x}$ with s; otherwise the lattice

point x is left blank. The process ends when all values of $s \in \mathbb{Z}_m$ have been exhausted. It follows from definition that the set of lattice points that have elements filled is the A-representation $\mathscr{G}(A, m)$ of $\mathbb{Z}_m$. Figure 5.11 shows the A-representation of $\mathbb{Z}_{138}$ with $A = \{1, 11, 78\}$.

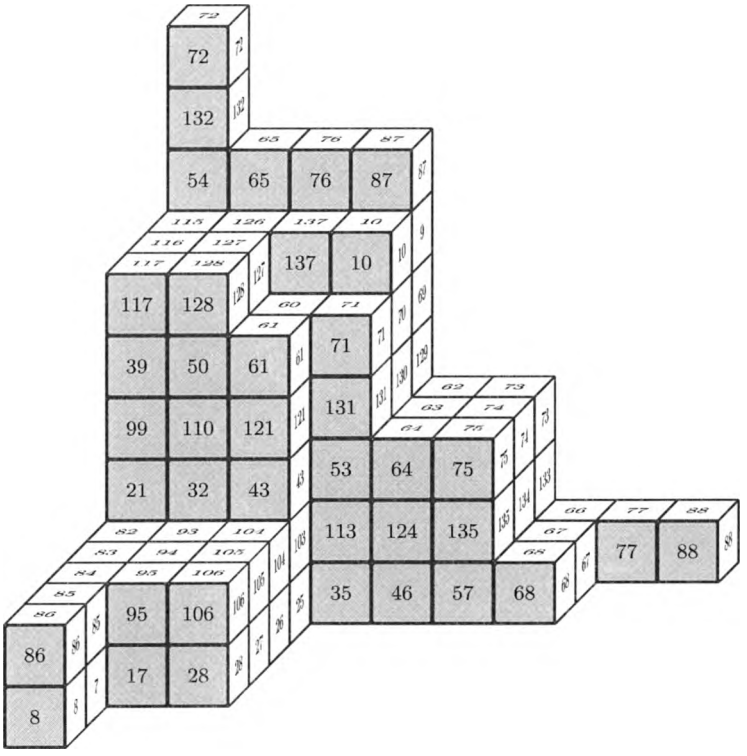


Figure 5.11: $\mathscr{G}(A, 138)$, the A-representation of $\mathbb{Z}_{138}$ with $A = \{1, 11, 78\}$.

Let m and k be two positive integers with $m > k$. Let $\mathbf{e}_i$ denote the lattice point $(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k$ such that $x_i = 1$ and $x_j = 0$ for all $j \neq i$. Let $A = \{a_1, a_2, \ldots, a_k\}$ be a k-element subset of $\mathbb{Z}_m$. Let $\mathscr{G}(A, m)$ denote the A-representation of $\mathbb{Z}_m$.

The following are a few examples.

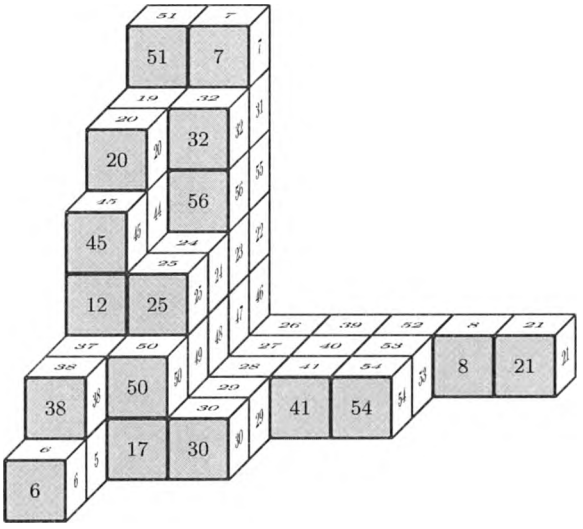


Figure 5.12: $\mathscr{G}(A, 57)$, the A-representation of $\mathbb{Z}_{57}$ with $A = \{1, 13, 33\}$.

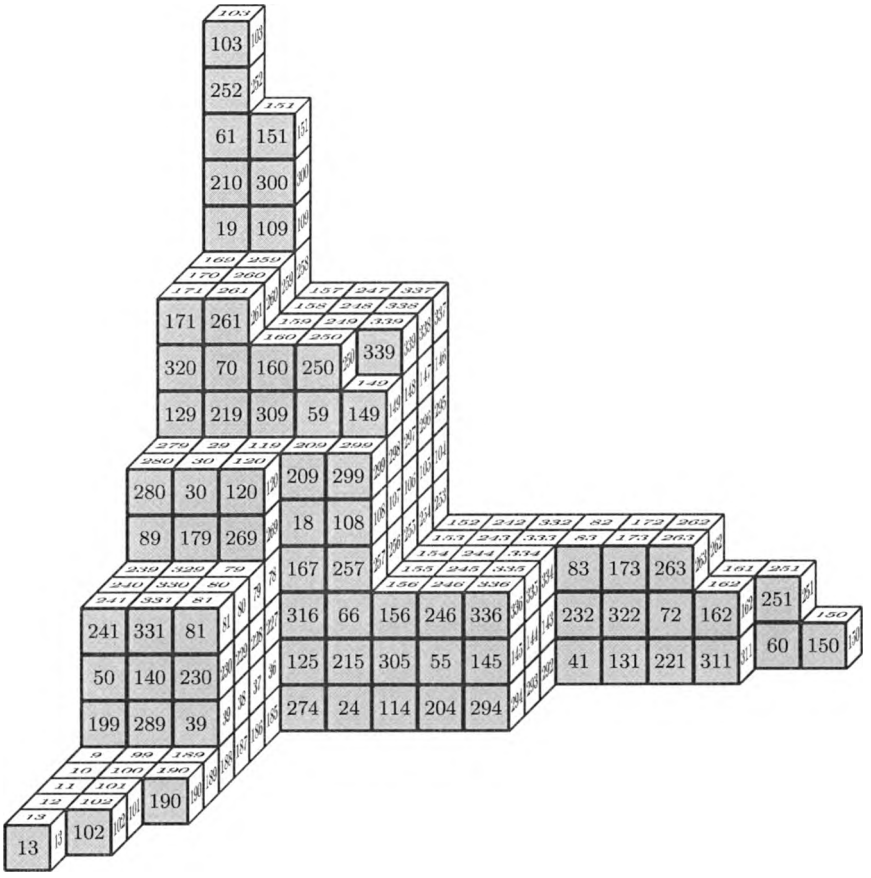


Figure 5.13: $\mathscr{G}(A, 340)$, the A-representation of $\mathbb{Z}_{340}$ with $A = \{1, 90, 191\}$.

Chapter 6

REMARKS AND OPEN PROBLEMS

Undirected Extremal Cayley Graphs. We only briefly mentioned the definitions for $M(d,k)$ and $\overline{M}(\lambda,k)$, the two extremal functions related to undirected Cayley graphs. They have been studied by various authors. In particular, Chen and Jia (1993) and Lee, Sheu and Jia (2008) proved that

$$M(d,2) = 2d^2 + 2d + 1,$$
$$\overline{M}(\lambda,2) = \frac{9}{2}\lambda^2 + O(\lambda).$$

It is still an open problem to compute these functions for $k \geq 3$.

An Extremal Problem on Multi-dimensional Tori: Minimum Diameter. Given positive integers k and m, let $d = d_m(k)$ be the least positive integer such that there exists a generating set $A = \{a_1, a_2, \ldots, a_{k+1}\} \subseteq \mathbb{Z}_m^k$ so that

$$\mathrm{diam}(\mathrm{Cay}(\mathbb{Z}_m^k, A)) \leq d.$$

If A is a d-basis for $\mathbb{Z}_m^k$, then

$$\binom{k+1+d}{k+1} = \binom{k+2+d-1}{d} \geq m^k.$$

This implies that, for any given fixed positive integer k,

$$d \geq \sqrt[k+1]{(k+1)!}(1+o(1))m^{\frac{k}{k+1}} \qquad \text{as} \quad m \to \infty.$$

One open question is to determine the correct leading coefficient. Note that, when $k = 1$, the problem has been studied extensively.

Another Extremal Problem on Multi-dimensional Tori: Maximum Size. Another aspect of the above problem is to determine the largest possible m with given d and k. Namely, for any given positive integers d and k, let $m = m_k(d)$ be the largest possible integer m such that there exists a generating set $A = \{a_1, a_2, ...a_{k+1}\}$ so that

$$\text{diam}(\text{Cay}(\mathbb{Z}_m^k, A)) \leq d.$$

It is easy to verify that

$$m = m_k(d) \leq \frac{1 + o(1)}{\sqrt[k]{(k+1)!}} d^{1+\frac{1}{k}}.$$

It can be proved that

$$m_k(d) \geq \frac{1}{(k+1)^{1+\frac{1}{k}}}(1 + o(1))d^{1+\frac{1}{k}}.$$

It is an open problem to determine $m_k(d)$. Note that

$$m_1(d) = m(d, 2) = \left\lfloor \frac{d(d+4)}{3} \right\rfloor + 1.$$

The Undirected and The Average Cases. The undirected and average versions of $d_k(m)$ and $m_k(d)$ have never been studied for $k \geq 2$. It is open to determine their values. In the case $k = 1$, these extremal functions have been studied, and approximate formulae or estimates have been proved. See the book *Combinatorial Networks* (under preparation) by Hsu and Jia for more information.

The Geometric Representation of Finite Cyclic Groups. The geometric representation of $\mathbb{Z}_m$ by a generating set can be used in establishing upper bounds for $m(d, k)$, $M(d, k)$, $\overline{m}(\lambda, k)$, and $\overline{M}(\lambda, k)$. It is a wide open problem to determine these extremal functions for $k \geq 3$.

BIBLIOGRAPHY

Bermond, J. C., Comellas, F. and Hsu, D. F.: Distributed loop computer networks: a survey. *Journal of Parallel and Distributive Computation*, 24 1995, 2–11

Chen, Sheng and Jia, Xingde: Undirected loop networks. *Networks*, 23 1993, Nr. 4, 257–260, ISSN 0028–3045

Du, Ding-Zhu and Hsu, D. Frank , editors: *Combinatorial Network Theory*. Volume 1, Applied Optimization. Dordrecht: Kluwer Academic Publishers, 1996, viii+212, ISBN 0–7923–3777–8

Hsu, D. Frank and Jia, Xingde: Extremal problems in the construction of distributed loop networks. *SIAM Journal of Discrete Mathematics*, 7 1994, Nr. 1, 57–71, ISSN 0895–4801

Jia, Xingde: Extremal bases for finite cyclic groups. *Journal of Number Theory*, 41 1992, Nr. 1, 116–127, ISSN 0022–314X

Jia, Xingde and Su, Weidong: Triple loop networks with minimal transmission delay. *International Journal of Foundations of Computer Science*, 8 1997, 305–328

Lee, J., Sheu, E. and Jia, X.: Extremal Cayley graphs of finite cyclic groups. *Journal of Interconnection Networks*, 9 2008, 73–82

Mask, Abby Gail, Schneider, Joni J. and Jia, Xingde: Extremal Cayley graphs of finite abelian groups. *Journal of Interconnection Networks*, 12 2011, Nr. 1&2, 125–135

West, Douglas B.: *Introduction to graph theory*. Upper Saddle River, NJ: Prentice Hall Inc., 1996, xvi+512, ISBN 0–13–227828–6

Wong, C. K. and Coppersmith, Don: A combinatorial problem related to multimodule memory organizations. *Journal of the Association for Computing Machinery*, 21 1974, 392–402, ISSN 0004–5411

VITA

Joni Schneider was born June 3, 1985 to Jane Schneider of Flatonia, Texas. She graduated as valedictorian of Flatonia High School in May 2003. She then attended Texas State University-San Marcos. There she received a Bachelor of Science in Applied Mathematics and Minor in Biology in December 2008. Joni enrolled in the Texas State University-San Marcos Graduate Program to pursue a Masters of Science in Pure Mathematics in January 2009.

Permanent address: 1018 North Knezek Road, Flatonia, Texas 78941

This thesis was typed by Joni J. Schneider.