CONNECTIVITIES AND DIAMETERS OF CIRCULANT GRAPHS

by

Paul Theo Meijer
B.Sc. (Honors), Simon Fraser University, 1987

THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE (MATHEMATICS)
in the Department
of
Mathematics and Statistics

SIMON FRASER UNIVERSITY
December 1991

Approval

Name: Paul Theo Meijer

Degree: Master of Science (Mathematics)

Title of Thesis: Connectivities and Diameters of Circulant Graphs

Examining Committee:

Chairman: Dr. Alistair Lachlan

____
Dr. Brian Alspach, Professor
Senior Supervisor

____
Dr. Luis Goddyn, Assistant Professor

____
Dr. Joseph Peters, Associate Professor

____
Dr. Tom Brown, Professor
External Examiner

Date Approved: December 4, 1991

PARTIAL COPYRIGHT LICENSE

Title of Thesis/Project/Extended Essay

CONNECTIVITIES AND DIAMETERS

OF CIRCULANT GRAPHS

Author: ______________________

(signature)

PAUL THEO MEIJER

(name)

NOV. 29, 1991

(date)

Abstract

Let $S = \{a_1, a_2, \ldots, a_k\}$ be a set of integers such that $0 < a_1 < \cdots < a_k < (n+1)/2$ and let the vertices of an n-vertex graph be labelled $0, 1, 2, \ldots, n-1$. Then the *circulant graph* $C(n, S)$ has $i \pm a_1, i \pm a_2, \ldots, i \pm a_k \pmod{n}$ adjacent to each vertex i.

In the design of networks, connectivity of the underlying graphs is of interest as a measure of network reliability and vulnerability, while diameter is a measure of transmission delay. We examine the connectivity properties of circulant graphs, and present some results on the diameter of these graphs.

Dedication

To my family, and Landa. In particular, my parents, Theo and Marjan, for always providing me with support and opportunities.

Acknowledgements

I wish to give thanks to the following:

- My supervisor, Dr. Brian Alspach, for introducing me to the topic of this thesis and for his guidance;
- Dr. F. Boesch and Dr. D.F. Hsu for providing me with relevant information; and
- My wife, Gina, for her patience, understanding, and support during the past two years.

Contents

List of Figures

Chapter 1

Introduction

In this thesis, we will examine the connectivity and diameter properties of *circulant graphs*. Definitions of graph theoretic terms and concepts not defined in this thesis can be found in Harary [20]. Our main interest in circulant graphs lies in the role they play in the design of networks. In this context, connectivity is of interest as a measure of reliability, while diameter is a measure of transmission delay. Hence, given certain parameters for a circulant graph, we will be interested in maximizing connectivity and minimizing diameter. As well, from an expense and practicality point of view, we will want to keep the number of links of the network to a minimum.

Let $S = \{a_1, a_2, \ldots, a_k\}$ be a set of integers such that $0 < a_1 < \cdots < a_k < (n+1)/2$ and let the vertices of an n-vertex graph be labelled $0, 1, 2, \ldots, n-1$. Then the *circulant graph* $C(n, S)$ has $i \pm a_1, i \pm a_2, \ldots, i \pm a_k \pmod{n}$ adjacent to each vertex i. The set S is called the *symbol* of $C(n, S)$.

In the literature on circulant graphs, the following definition and notation are also commonly used. Let the vertices of a graph be labelled $0, 1, 2, \ldots, p-1$. Then the *circulant graph* $C_p(n_1, n_2, \ldots, n_k)$ or briefly $C_p(n_i)$ where $0 < n_1 < \cdots < n_k < (p+1)/2$ has $i \pm n_1, i \pm n_2, \ldots, i \pm n_k$ (mod p) adjacent to each vertex i. In this latter definition, the sequence (n_i) is called the *jump sequence* and the n_i are called *jumps.*

If $a_k \neq n/2$ then $C(n, S)$ is regular of degree $2k$. For n even, we allow $a_k = n/2$, which gives *diagonal jumps.* When $a_k = n/2$, $C(n, S)$ is regular of degree $2k - 1$.

A *circulant matrix* is obtained by taking an arbitrary first row, and shifting it cyclically one position to the right in order to obtain successive rows. Formally, if the first row of an n-by-n circulant matrix is $a_0, a_1, \ldots, a_{n-1}$, then the $(i, j)^{th}$ element is a_{j-i}, where subscripts are taken modulo n. The term circulant graph arises from the fact that the adjacency matrix for such a graph is a circulant matrix.

For example, Figure 1.1 shows the circulant graphs $C(9, \{1, 2, 3\})$ and $C(12, \{2, 3\})$, while Figure 1.2 shows the adjacency matrix for $C(9, \{1, 2, 3\})$, which is clearly a circulant matrix. Note that in this thesis, when we say "circulant" we shall mean the graph as opposed to the matrix.

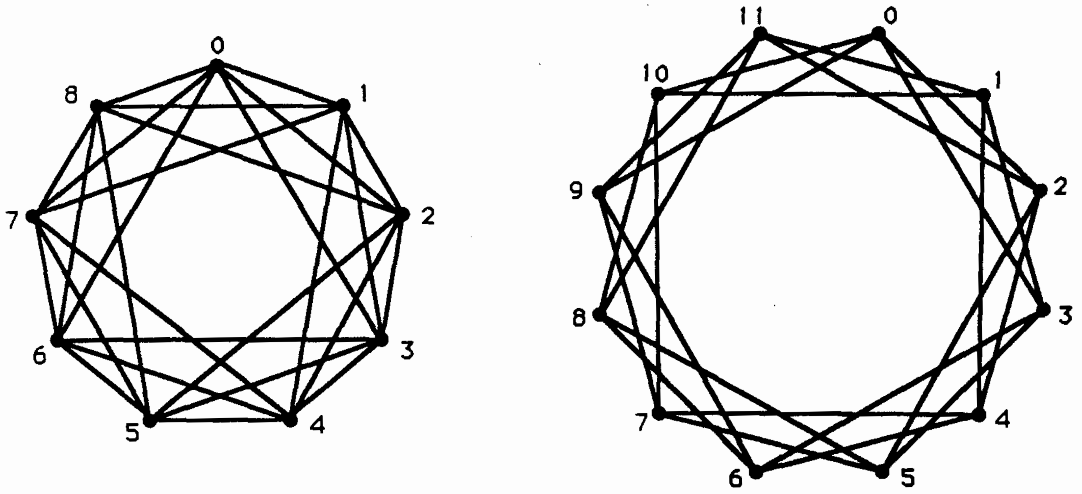

Figure 1.1: The circulants $C(9, \{1, 2, 3\})$ and $C(12, \{2, 3\})$

	v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8
v_0	0	1	1	1	0	0	1	1	1
v_1	1	0	1	1	1	0	0	1	1
v_2	1	1	0	1	1	1	0	0	1
v_3	1	1	1	0	1	1	1	0	0
v_4	0	1	1	1	0	1	1	1	0
v_5	0	0	1	1	1	0	1	1	1
v_6	1	0	0	1	1	1	0	1	1
v_7	1	1	0	0	1	1	1	0	1
v_8	1	1	1	0	0	1	1	1	0

Figure 1.2: The adjacency matrix for $C(9, \{1, 2, 3\})$

Chapter 2

Some Properties of Circulant Graphs

In this chapter, we describe some of the properties of circulant graphs. Since the properties of connectivity and diameter are the main areas of interest in this thesis, they appear in chapters of their own, and are examined in greater depth. This chapter is, basically, a list of various properties. We will do little more than define or describe each property, and provide some general comments.

Two vertices u and v of a graph G are said to be *similar* if there exists an automorphism α of G that maps one of the vertices onto the other; that is, $\alpha(u) = v$. Similarly, two edges $e_1 = u_1v_1$ and $e_2 = u_2v_2$ are called *similar* if there exists an automorphism α of G that maps one of the edges onto the other; that is, $\alpha(\{u_1, v_1\}) = \{u_2, v_2\}$. A graph is *vertex-transitive* if every pair of vertices is similar, and it is *edge-*

transitive if every pair of edges is similar. For circulants, the mapping f_j which rotates vertex i into vertex $i+j$ (mod n) is an automorphism; hence, *every circulant is vertex-transitive.* As an aside, we note that very few circulants are edge-transitive. For example, the circulant $C(9,\{1,2,3\})$ shown in Figure 1.1 is not edge-transitive since the endvertices of each edge corresponding to $a_1 = 1$ together are adjacent to 6 other vertices, while the endvertices of each edge corresponding to $a_2 = 2$ together are adjacent to 7 other vertices. Necessary and sufficient conditions for a circulant to be edge-transitive are not known; although the case where the number of vertices is prime has been solved (see Chao [15] and Berggren [2]).

Proposition 2.1 *If G is a circulant, then its complement $\overline{G}$ is also a circulant.*

PROOF. Let $C(n,S)$ be an arbitrary circulant with edge set E, and let $\overline{E}$ denote the edge set of $\overline{C(n,S)}$, the complement of $C(n,S)$. If $(i,i+a_j) \notin E$ then by definition, $(i,i+a_j) \in \overline{E}$. Now note by the definition of circulant, if $(i,i+a_j) \notin E$ then $(i \pm k,(i+a_j) \pm k) \notin E$, where the addition is done modulo n. But this means that $(i,i+a_j) \in \overline{E}$ implies $(i \pm k,(i+a_j) \pm k) \in \overline{E}$, and thus $\overline{C(n,S)}$ is a circulant. □

Proposition 2.2 *An arbitrary graph G on n vertices is a circulant if and only if the automorphism group $\Gamma(G)$ of G contains a cycle of length n.*

PROOF. Note that if G is a circulant, then $\Gamma(G)$ contains an n-cycle. In fact, $\Gamma(G)$ contains the dihedral group D_n, the group of symmetries of the regular n-gon.

Conversely, suppose for an arbitrary n-vertex graph G, $\Gamma(G)$ contains an n-cycle σ, where $\sigma = (v_0 \; v_1 \; \cdots \; v_{n-1})$. Let vertex v_i be labelled with i, $0 \leq i \leq n-1$. By definition, an automorphism preserves adjacency, thus $(0,i) \in E$ implies $(\sigma(0), \sigma(i)) \in E$ for all vertices i adjacent to vertex 0. In particular, we have that $(0,i) \in E$ implies $(1, 1+i) \in E$, $(2, 2+i) \in E$, and so on. In other words, G is a circulant. □

The following result is due to Turner [31].

Theorem 2.1 *Every vertex-transitive graph of prime order is a circulant.*

Proposition 2.3 *The 3-cube (see* Figure 2.1*) is the smallest vertex-transitive graph that is not a circulant.*

PROOF. In Appendix 1 of [20], Harary provides a tabulation of all graphs on 6 or fewer vertices. A check of this tabulation shows that all vertex-transitive graphs of order 6 or less are circulants. By Theorem 2.1, any vertex-transitive graph on 7 vertices is a circulant.

Finally, it is not difficult to check that the automorphism group of the 3-cube does not contain a cycle of length 8; hence, by Proposition 2.2, the 3-cube is not a circulant. □

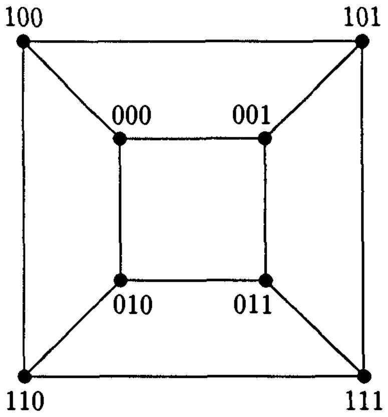

Figure 2.1: The 3-cube

We note that the statement of Proposition 2.3 also appears in [4], in which Boesch and Tindell make use of the fact that the 3-cube is bipartite to show that it is not a circulant.

As pointed out by Bermond, Favaron and Maheo [3], it is known that any connected Cayley graph (see Chapter 3 for a definition) on an abelian group is hamiltonian. Based on this fact we get the following.

Proposition 2.4 *All connected circulants are hamiltonian.*

Chapter 3

Circulants In Other Classes of Graphs

In this chapter we will give definitions and/or descriptions of various classes of graphs, and examine how they relate to circulant graphs. In particular, we will show some different areas of graph theory in which circulant graphs occur. In some cases, a defined class of graphs will be a proper subset of circulant graphs (or vice versa), while in other cases there will simply be an overlap between circulants and the other class of graphs.

If G is a group and $S \subset G$ satisfies:

(i) $e \notin S$, and

(ii) $s \in S$ implies $s^{-1} \in S$,

then the *Cayley graph* $\text{Cay}(G; S)$ has the elements of G as its vertices and edges joining g and gs for all $g \in G$ and all $s \in S$. As with circulant graphs, S is called the *symbol.*

If we consider the case where the group G is the additive group Z_n of residue classes modulo n for some positive integer n, then the Cayley graph $\text{Cay}(Z_n; S')$ such that $S' = \{\pm a_1, \pm a_2, \ldots, \pm a_k\}$, where $-a_i = n - a_i$, is equivalent to the circulant graph $C(n, S)$, for $S = \{a_1, \ldots, a_k\}$. Thus the class of Cayley graphs properly contains the class of circulants.

Another area of graph theory in which circulant graphs occur is *Ramsey Theory.* Let $G = (V, E)$ be an arbitrary simple graph with vertex set V and edge set E. A subset S of V is called an *independent set* of G if no two vertices of S are adjacent in G. A *clique* of G is a subset S of V such that the subgraph of G induced by S is complete. Ramsey's Theorem states that given positive integers k and l, there exists a smallest integer $r(k, l)$ such that every graph on $r(k, l)$ vertices contains either a clique of k vertices or an independent set of l vertices. A *(k, l)-Ramsey graph* is a graph on $r(k, l) - 1$ vertices that contains neither a clique of k vertices nor an independent set of l vertices. It turns out that several such graphs are circulants (see Section 7.2 on page 103 of Bondy and Murty [14]). In Figure 3.1, we show some examples of (k, l)-Ramsey graphs. In particular, Figure 3.1a shows a $(3, 3)$-Ramsey graph, which is equivalent to $C(5, \{1\})$. In Figure 3.1b we have a $(3, 4)$-Ramsey graph, which is equivalent to $C(8, \{1, 4\})$, and in Figure 3.1c we have a $(4, 4)$-Ramsey graph, which is equivalent to $C(17, \{1, 2, 4, 8\})$.

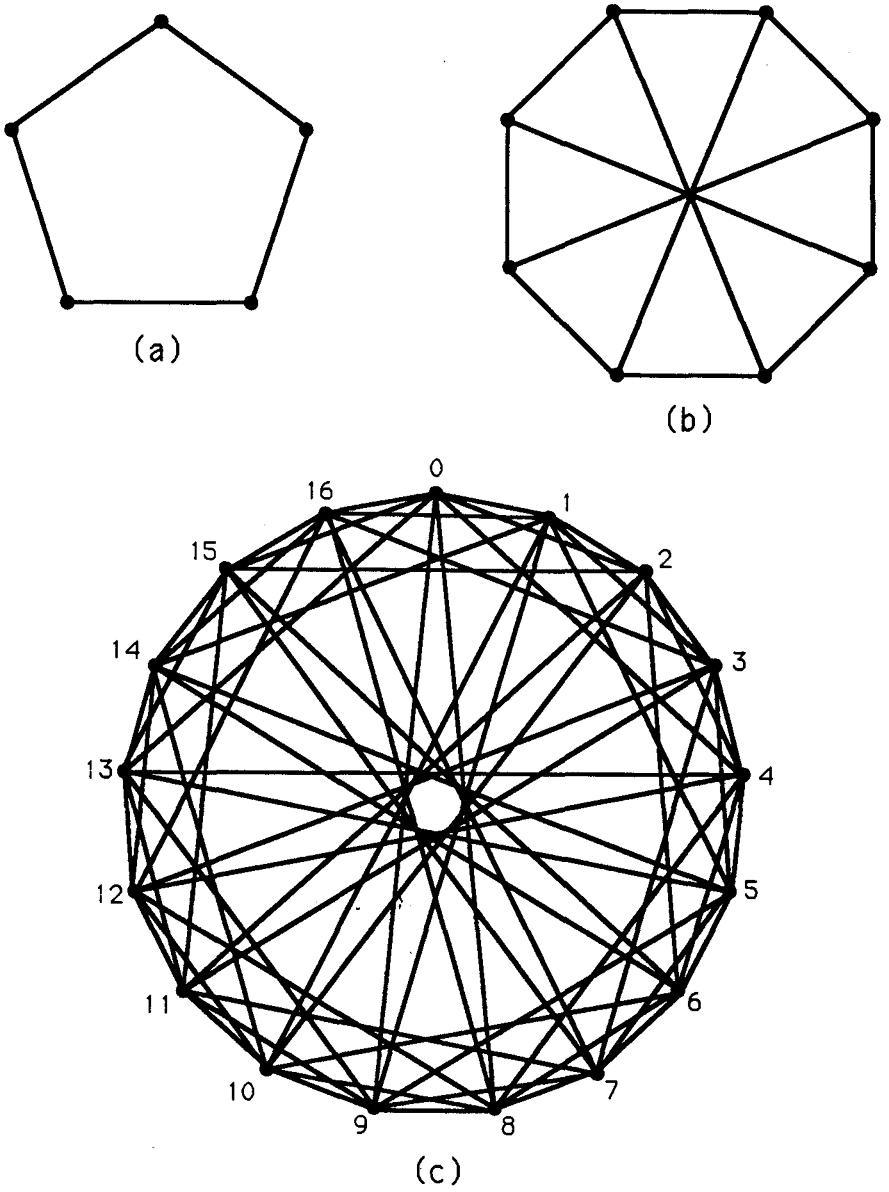

Figure 3.1: Examples of (k, l)-Ramsey graphs

Let n and d be positive integers with $d < n$. Consider a graph G whose vertices are labelled with the integers modulo n, and such that two vertices are adjacent if and only if the difference between their labels (mod n) is less than or equal to d. Then G is the *d'th power of a cycle on n vertices*, which we denote $C_n^{(d)}$. Note that we can assume $d < (n+1)/2$, and furthermore, we observe that such graphs are equivalent to the circulant graphs $C(n, \{1, 2, \ldots, d\})$. We note that these graphs are also equivalent to *Harary graphs*, which we define in Chapter 4. Thus the set of circulant graphs properly contains the set of powers of cycles. We shall see in a later chapter that such graphs have the property of *super edge-connectivity.* Based on this definition, we see that the circulant $C(9, \{1, 2, 3\})$ shown in Figure 1.1 is also a power of a cycle, and hence can be denoted $C_9^{(3)}$.

In [24], Leighton defines an extension of the notion of a circulant to a broader class of vertex-transitive graphs, which he calls *multidimensional circulants.* In particular, let

$$S^n = \{(a_1^1, a_2^1, \ldots, a_k^1), (a_1^2, a_2^2, \ldots, a_k^2), \ldots, (a_1^n, a_2^n, \ldots, a_k^n)\}$$

be a set of k-tuples of integers and let the vertices of an $n_1 n_2 \cdots n_k$-vertex graph be labelled $(i_1, i_2, \ldots, i_k)$ where $0 \leq i_l < n_l$ for $1 \leq l \leq k$. Then the *k-dimensional circulant graph* $C((n_1, \ldots, n_k), S^n)$ has $(i_1 \pm a_1^m \pmod{n_1}, i_2 \pm a_2^m \pmod{n_2}, \ldots, i_k \pm a_k^m \pmod{n_k})$, for $1 \leq m \leq n$, adjacent to each vertex $(i_1, \ldots, i_k)$. Under this definition, what we have defined as a circulant becomes a *1-dimensional circulant.*

In [16], Deo and Krishnamoorthy propose a class of graphs called

Toeplitz networks, which they derive from Toeplitz matrices. Such graphs satisfy several properties that are desirable for the design of computer networks, and it turns out that they are equivalent to circulants of the form $C(n, \{1, w+1, 2w+1, \ldots\})$. Note that the symbol is an arithmetic progression with common difference w, where w is a parameter of the Toeplitz network.

Let $\mathrm{QR}(q)$ be the set of quadratic residues for a prime power $q \equiv 1 \pmod 4$. Then the *Paley graph* $G(q)$ has F_q as vertex set, and two vertices are adjacent whenever their difference is in $\mathrm{QR}(q)$. If q is a prime, then such a graph is equivalent to the circulant $C(q, \mathrm{QR}(q))$.

The *Möbius ladder* M_s is equivalent to the circulant $C(2s, \{1, s\})$. The complement of the regular, complete, n-partite graph $K_{m,m,\ldots,m}$ is equivalent to the circulant $C(nm, \{n, 2n, 3n, \ldots, \lfloor m/2 \rfloor n\})$, hence by Proposition 2.1, $K_{m,m,\ldots,m}$ itself is a circulant. The graphs resulting from the Cartesian products $K_2 \times K_n$ and $K_2 \times C_n$ are sometimes called *prisms.* For n odd, $K_2 \times K_n$ is equivalent to the circulant $C(2n, \{2, 4, \ldots, n-1, n\})$, while $K_2 \times C_n$ is equivalent to the circulant $C(2n, \{2, n\})$. For n even, neither $K_2 \times K_n$ nor $K_2 \times C_n$ is a circulant.

Chapter 4

Connectivity

In the design of networks, the connectivity of the underlying graph G of a network is related to the reliability and vulnerability of the network. We note that there is a distinction between reliability and vulnerability.

Network reliability is concerned with the model in which each link (or node) of the network is assigned a probability of failure. Usually, one supposes each link has the same probability ρ of failure, and that the links fail independently. This area of research is further divided into analysis versus synthesis.

Letting N_k denote the number of edge-disconnecting sets of cardinality k in a graph G, the analysis problem is to find the network reliability $P(G, \rho)$ given G and ρ, where

$$P(G,\rho) = \sum_{k=\lambda}^{q} N_k \rho^k (1-\rho)^{q-k}.$$

The synthesis problem is to find an n-vertex, e-edge graph G that minimizes $P(G, \rho)$ over the class of all graphs having e edges and n vertices.

For this thesis, we have chosen not to examine network reliability. For information and results on this problem, we refer the reader to two papers by Boesch [6, 7] in the case of synthesis, and to a paper by Wilkov [37] for the analysis problem.

Network vulnerability is concerned with a network's susceptibility to attack by adversaries; that is, the effect of removing links or nodes. Thus, in the vulnerability model, we do not work with probabilities. The connectivity of the underlying graph of the network is a measure of the network's vulnerability and is the topic of this chapter. We will be interested in determining the number of links or nodes that must fail for the network to become disconnected; that is, so that one set of remaining nodes can no longer communicate with another set.

We first define several terms related to graphs. Let $G = G(V, E)$ be an arbitrary simple graph with vertex set V and edge set E. The *degree* of a vertex $v \in V$ is the number of edges incident with v, and the *minimum* degree among all vertices in V is denoted by δ. A graph G is *connected* if every pair of vertices $u, v \in V$ is joined by a path; otherwise, G is *disconnected.* A *cut-edge* of G is an edge $e \in E$ such that removing e increases the number of components of G. Similarly, a *cut-vertex* of G is a vertex $v \in V$ such that removing v increases the number of components of G. In particular, a connected graph containing a cut-edge (cut-vertex) becomes disconnected upon removal of a cut-edge (cut-vertex). The *connectivity* κ of a graph G is the minimum number of vertices whose removal results in a disconnected or trivial graph. This is also called *vertex-connectivity.* The *edge-connectivity* λ of a graph G is the minimum number of edges whose removal results in a disconnected or trivial graph.

We are now ready for the statement and proof of the following which, except for the first inequality, is due to Whitney [36].

Theorem 4.1 *For an arbitrary graph $G(V, E)$,*

$$2|E|/|V| \geq \delta \geq \lambda \geq \kappa. \tag{4.1}$$

PROOF. We first show that $2|E|/|V| \geq \delta$. Since each edge contributes 2 to the sum, the sum of all the degrees of the vertices in V is equal to twice the number of edges, that is, $2|E|$. Thus, $2|E|/|V|$ represents the *average* of the degrees of the vertices in V, and since δ is the *minimum* degree, we have the result.

If G is trivial or disconnected, we have $\lambda = \kappa = 0$, and thus $\delta \geq \lambda \geq \kappa$. Otherwise, let $v \in V$ be a vertex of minimum degree δ. If we remove all of the δ edges incident with v, then v will be isolated and thus G will be disconnected. Hence, $\delta \geq \lambda$.

We now show the last inequality. If G is trivial or disconnected, we have $\lambda = \kappa = 0$, so that $\lambda \geq \kappa$ in this case. If G contains a cut-edge e, then removing e disconnects the graph so that $\lambda = 1$. Note that at least one of the endvertices of e, say v, will be a cut-vertex unless $G = K_2$. In either case, the graph obtained by removing v is either disconnected or trivial so that $\kappa = 1$, and we have $\lambda \geq \kappa$. Lastly, suppose G has no cut-edge, and let L be a minimum edge disconnecting set (so $|L| = \lambda$). Now, removing $\lambda - 1$ edges of L from G will leave a cut-edge e with endvertices u and v, and at least one of u or v, say v, will be a cut-vertex. For each of these $\lambda - 1$ edges, choose an endvertex different from u or v. Removing this set of chosen vertices from G will remove the $\lambda - 1$ edges of $L - \{e\}$ and may in fact result in a disconnected graph, in which case we have $\lambda > \kappa$. If the graph obtained by removing the chosen vertices from G is connected, removing the cut-vertex v will disconnect it, and we will have $\lambda \geq \kappa$. In all cases, we get $\lambda \geq \kappa$. □

Equation (4.1) gives δ as an upper bound for the connectivity of a graph, and Harary [19] was the first to define the following class of graphs, for which $\kappa = \delta$, and hence shows that this maximum connectivity can be achieved. Given two positive integers n and k with $k \leq n$, begin by drawing an n-gon and label its points $0, 1, 2, \ldots, n-1$. Join two points i and j if and only if $|i-j| \equiv m \pmod{n}$, where $1 \leq m \leq k$. The resulting graph has been called an *Harary graph*, and we denote it $H_n(k)$. As noted in Chapter 3, the Harary graph $H_n(k)$ is equivalent to the circulant $C(n, \{1, 2, \ldots, k\})$. Thus the circulant $C(9, \{1, 2, 3\})$ shown in Figure 1.1 is the Harary graph $H_9(3)$, and hence has maximum connectivity $\kappa = \delta = 6$.

Notice that if we show a graph G has maximum connectivity $\kappa = \delta$, then by Equation (4.1) we will have that $\lambda = \delta$ as well. Furthermore, it has been shown by Mader [28] that $\lambda = \delta$ for connected vertex-transitive graphs (this fact also appears in the statement of upcoming Theorem 4.8). So for circulant graphs the question of edge-connectivity is simply answered, and it is just the characterization of vertex-connectivity that is of interest.

From the viewpoint of network design, we are interested in determining what other circulant graphs, if any, have maximum connectivity $\kappa = \delta$. As stated in the proof of Theorem 4.1, $\kappa = 0$ when a graph is disconnected, so we would first like to determine which circulants are connected.

We first observe that, for a circulant $C(n, S)$, if an element a_i of S is relatively prime to n, then the edges corresponding to a_i form a Hamilton cycle, and thus the circulant is connected. However, the existence of such an element isn't necessary for a circulant to be connected. For example, neither of the jumps in $C(12, \{2, 3\})$ (see Figure 1.1) is relatively prime to the number of vertices, yet this circulant has a Hamilton cycle, given by the following sequence of vertices: $0, 2, 5, 3, 1, 4, 6, 8, 11, 9, 7, 10, 0$. In general, we can show that a circulant is connected by identifying the existence of a path from 0 to i for each vertex i. That is, we need a combination of elements of S that sum to i: $\sum_{j=1}^{k} \alpha_j a_j \equiv i$ (modulo n). This leads to the following theorem.

Theorem 4.2 *The circulant $C(n, S)$, where $S = \{a_1, \ldots, a_k\}$, is connected if and only if* $\gcd(a_1, a_2, \ldots, a_k, n) = 1$.

PROOF. Suppose $C(n, \{a_1, \ldots, a_k\})$ is connected. Then there exists a path from 0 to i for each vertex i $(1 \leq i \leq n-1)$. That is, there exist integers α_j $(1 \leq j \leq k)$ such that $\sum_{j=1}^{k} a_j \alpha_j \equiv i \pmod{n}$ for each $i \in Z_n$. In particular, we have

$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_k\alpha_k \equiv 1 \pmod{n}$ for some integers α_j $(1 \leq j \leq k)$.

This implies

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_k\alpha_k = mn + 1 \text{ for some } m \in Z.$$

Thus

$$n(-m) + a_1\alpha_1 + a_2\alpha_2 + \cdots + a_k\alpha_k = 1$$

which implies $\gcd(a_1, \ldots, a_k, n) = 1$.

Conversely, if $\gcd(a_1, \ldots, a_k, n) = 1$ then

$$nx_0 + a_1x_1 + \cdots + a_kx_k = 1 \text{ for some integers } x_j \ (0 \leq j \leq k)$$

from which it follows that the equation

$$n\alpha_0 + a_1\alpha_1 + \cdots + a_k\alpha_k = i$$

is solvable for all i, $0 \leq i \leq n-1$. Thus there exist integers α_j such that $a_1\alpha_1 + \cdots + a_k\alpha_k \equiv i$ (modulo n) for each i, $0 \leq i \leq n-1$. Hence $C(n, S)$ is connected. □

Having established the conditions under which a circulant is connected, we now consider the problem of determining which circulants achieve maximum connectivity. It turns out that there are some simple sufficient conditions for a circulant to have $\kappa = \delta$. Although none of these conditions is necessary, we state them here as they provide for several ways to easily construct a circulant having maximum connectivity.

The following is a variation of a result due to Watkins (see [34], Corollary 3B).

Theorem 4.3 *If $G = C(n,S)$ is a connected circulant of degree 4 or 6, then $\kappa = \delta$.*

The next result is due to Wang [32].

Theorem 4.4 *The circulant $C(n, \{a, 1+a, 2+a, \ldots, k+a\})$ has $\kappa = \delta$.*

The following result is a consequence of some of Watkins' work in [35], the details of which we provide later in this chapter.

Theorem 4.5 *Let G be a circulant with symbol $S = \{a_1, \ldots, a_k\}$. If a_j is relatively prime to n whenever $a_j \geq 4$, then $\kappa = \delta$.*

A property of sequences that has been used to obtain results on maximum connectivity for circulant graphs is that of convexity. In particular, the sequence $(a_1, a_2, \ldots, a_k)$ is *convex* if $a_{i+1} - a_i \leq a_{i+2} - a_{i+1}$ for $1 \leq i \leq k-2$. The following result makes use of this property, and is due to Boesch and Felzer [8].

Theorem 4.6 *The circulant $C(n, \{a_1, \ldots, a_k\})$ has $\kappa = \delta$ if $a_1 = 1$ and $(a_1, \ldots, a_k)$ is convex.*

The following improvement of the above result is due to Wang [32].

Theorem 4.7 *The connected circulant $C(n, \{a_1, \ldots, a_k\})$ has $\kappa = \delta$ if the sequence $(0, a_1, a_2, \ldots, a_k)$ is convex.*

Note that the above theorem is an improvement of Theorem 4.6 as it allows $a_1 \geq 1$. We have already seen that $C(9, \{1, 2, 3\})$ has maximum connectivity, since it is an Harary graph, but another way to demonstrate this fact is to observe that the sequence $(0, 1, 2, 3)$ is convex.

A structural property of graphs used in some connectivity results is that of atomic part and atomic number. An *atomic part* (also called an *atom*) of a graph G is a smallest order component (with respect to number of vertices) of $G - T$ over all vertex-disconnecting sets T of cardinality κ. The *atomic number* $\alpha(G)$ of a graph G is the number of vertices in an atomic part.

In [5], Boesch and Tindell give the following theorem, which is a combination of results due to Watkins [33, 34] and, independently, Mader [25, 26, 27, 28].

Theorem 4.8

(A) *For a connected vertex-transitive graph G with n vertices:*

1. $\kappa = \delta$ *if and only if* $\alpha(G) = 1$,
2. $\alpha(G)$ *divides* n,
3. $\delta = \lambda \geq \kappa > 2\delta/3$, *and*
4. *if* G *doesn't contain* K_4, *then* $\kappa = \delta$.

(B) *For connected edge-transitive graphs,* $\kappa = \delta$.

We have seen that the circulant $C(9, \{1, 2, 3\})$ has $\kappa = \delta$, but note that it contains K_4 (for example, the subgraph induced on the vertices

$0, 1, 2, 3$), and furthermore we have shown that $C(9, \{1, 2, 3\})$ is not edge-symmetric. Thus, points **(A)***(4)* and **(B)** of Theorem 4.8 are not necessary to have $\kappa = \delta$ in circulants.

The preceding has given us several classes of circulants that achieve maximum connectivity. We now consider the problem of determining the connectivity of an arbitrary circulant. We first provide some pertinent definitions.

Let $G = G(V, E)$ be an arbitrary graph and let $F \subseteq V(G)$. Then the *neighborhood* of F is defined as

$$N(F) = \{v \in V(G) \backslash F : v \text{ is adjacent to an element of } F\}.$$

The *complement* of F, denoted $\overline{F}$, is $V(G) \backslash (F \cup N(F))$. For a finite regular graph G of degree δ, if $\kappa < \delta$ then G is called *hypoconnected.*

Since the results for determining the connectivity of an arbitrary circulant make use of several results concerning atomic parts, we give some of the basic properties of atomic parts, as derived by Tindell [30] and Watkins [34]. (Recall that Theorem 4.8 also contains results on atomic parts.)

Theorem 4.9 *Let G be an n-vertex connected circulant with atomic number α and $n = m\alpha$. If A is an atomic part of G, then $i \in A$ implies $(i + m) \in A$, where the addition is done modulo n.*

Note that Theorem 4.9 tells us that if A is the atomic part containing 0, then A will be made up of multiples of m. That is, $A = \{0, m, 2m, \ldots, n - m\}$.

Lemma 4.1 *In a connected graph, distinct atomic parts are disjoint.*

Lemma 4.2 *If F is the vertex set of a union of atomic parts, then each of $N(F)$ and $\overline{F}$ is also the vertex set of a union of atomic parts.*

Lemma 4.3 *If G is vertex-transitive, then $V(G)$ admits a partition into vertex sets of atomic parts, and all of these parts are pairwise isomorphic.*

Boesch and Tindell [4] obtained the following result, which gives necessary and sufficient conditions for a circulant to be hypoconnected. The discussion and example following the theorem show how an algorithm for determining the connectivity of a circulant comes out of this result.

Theorem 4.10 *The circulant $C(n, S)$, where $S = \{a_1, \ldots, a_k\}$, satisfies $\kappa < \delta$ if and only if for some proper divisor m of n, the number r_m of distinct positive residues (modulo m) of the numbers $a_1, \ldots, a_k, n - a_k, \ldots, n - a_1$ is less than the minimum of $m - 1$ and $\delta m/n$.*

Rather than giving the proof for Theorem 4.10, we provide the following discussion given by Boesch and Tindell in [5].

Let A be an atomic part of a graph G and consider the determination of $N(A)$, the neighborhood of A. By Theorem 4.9, $i \in A$ implies $(i + a_j) \in N(A)$, modulo n, if and only if $a_j \not\equiv 0 \pmod{m}$. Let J be a set of r_m jumps having distinct positive residues modulo m. Then each vertex $(i + a_j)$, modulo n, with $i \in A$ and $a_j \in J$ is in $N(A)$.

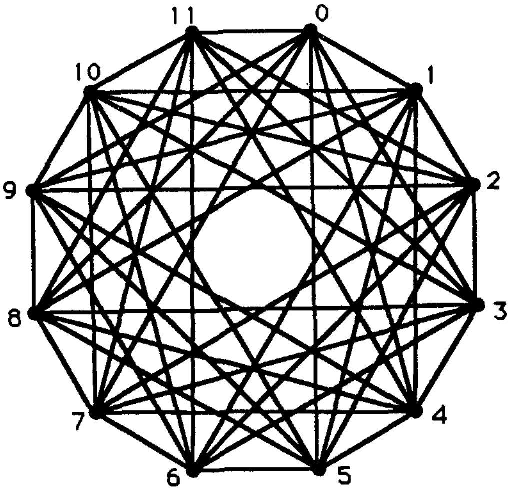

Figure 4.1: The circulant $C(12, \{1,3,4,5\})$

The sets of vertices in $N(A)$ obtained from vertices $i, j \in A$ by adding the jumps in J are pairwise-disjoint. Moreover, these sets cover $N(A)$. Hence $|N(A)| = |A| \cdot r_m$.

As mentioned after Theorem 4.9, in an n-vertex circulant, there exists an atomic part that will have as vertices all multiples of some divisor m of n. The above argument shows the neighborhood of any such set will have $r_m \cdot \alpha$ elements, where $\alpha = n/m$.

For any nonempty set A, $N(A)$ disconnects the graph if and only if there is at least one vertex not in $A \cup N(A)$. Moreover, we will have $\kappa < \delta$ if and only if for some such set $|N(A)| < \delta$.

These two conditions translate into the conditions of the theorem. By considering all the possible divisors of n, one obtains the actual connectivity.

We now give an example making use of Theorem 4.10. Consider the circulant $C(12, \{1,3,4,5\})$ shown in Figure 4.1 which has minimum degree $\delta = 8$. The proper divisors of 12 are $2,3,4$ and 6, and for this example, the numbers $(a_1, \ldots, a_k, n-a_k, \ldots, n-a_1)$ are $(1,3,4,5,7,8,9,11)$.

We first consider $m = 2$. The numbers $(1,3,4,5,7,8,9,11)$ become $(0,1)$ modulo 2, so $r_2 = 1$. Now, $\min\{m-1, \delta m/n\} = \min\{1, 8(2)/12\} = 1$, which is not greater than r_2 and thus does not satisfy the statement of the theorem.

Now consider $m = 3$. The numbers $(1,3,4,5,7,8,9,11)$ become $(0,1,2)$ modulo 3, so $r_3 = 2$, and $\min\{2, 8(3)/12\} = 2$, which is not greater than r_3 and thus does not satisfy the statement of the theorem.

For $m = 6$, the numbers $(1,3,4,5,7,8,9,11)$ become $(1,2,3,4,5)$ modulo 6, so $r_6 = 5$, and $\min\{5, 8(6)/12\} = 4$, which is less than r_6 and thus does not satisfy the statement of the theorem.

For $m = 4$, the numbers $(1,3,4,5,7,8,9,11)$ become $(0,1,3)$ modulo 4, so $r_4 = 2$. Now, $\min\{3, 8(4)/12\} = 8/3$, which is greater than r_4, so by the theorem, $\kappa < 8$. Continuing along the lines of the above discussion, if $\alpha(G) = n/m$ for $m = 4$, then by Theorem 4.9, an atomic part of $C(12, \{1,3,4,5\})$ would be defined by $A = \{0,4,8\}$. Now let $J = \{1,3\}$ be the set of jumps discussed above. Then $N(A) = \{0+1, 0+3\} \cup \{4+1, 4+3\} \cup \{8+1, 8+3\}$. Thus $\delta = 8, \kappa = 6$, and $\{1,3,5,7,9,11\}$ is a vertex-disconnecting set.

Boesch and Tindell [4] have shown that this circulant is the smallest example of $\kappa < \delta$ for δ even. For the case where δ is odd, the smallest circulant having $\kappa < \delta$ is $C(8, \{1,3,4\})$, which has $\delta = 5, \kappa = 4$, and $\{1,3,5,7\}$ as a vertex-disconnecting set.

We now give a pseudo-code version of an algorithm for computing the connectivity of a circulant, based on Theorem 4.10. Comments appearing within the algorithm are delimited by a pair of double slashes ("//"), and the notation "$|S|$" is used to denote the cardinality of the set S.

4.1 Boesch and Tindell's Algorithm for Computing Connectivity

```
STEP 1: Input circulant $C(n, S)$ where $S = \{a_1, a_2, \ldots, a_k\}$.
    Go to STEP 2.

STEP 2: Initialization.
    Let $S^{-1} = \{n - a_k, \ldots, n - a_1\}$;
    DELTA = $2k$ if $a_k \neq n/2$, otherwise DELTA = $2k - 1$;
    Let KAPPA = DELTA;
    Let NFACTORS be the set of proper divisors of $n$;
    $i = 0$.
    Go to STEP 3.

STEP 3: Let $i = i + 1$.
    If $i >$ |NFACTORS|, go to STEP 6.
    Let $m = i^{th}$ element of NFACTORS.
    Go to STEP 4.

STEP 4: Let $R_m = \{j \pmod{m} : j \in S \cup S^{-1}, j \not\equiv 0 \pmod{m}\}$;
    Let $M = \min\{m - 1,$ DELTA$\cdot(m/n)\}$;
    If $|R_m| \geq M$ return to STEP 3
    // i.e. $m$ is rejected //,
    otherwise go to STEP 5.

STEP 5: Let NU = $|R_m| \cdot (n/m)$
    // note that NU gives the size of the neighborhood of the atomic
    part $A = \{0, m, 2m, \ldots, n-m\}$ //
    If NU < KAPPA then let KAPPA = NU.
    // i.e. choose minimum NU //
    Return to STEP 3.
STEP 6: Terminate.
    KAPPA gives the connectivity of $C(n, S)$.
```

Independently from Boesch and Tindell, Watkins [35] developed an algorithm for computing the connectivity of a circulant from its symbol. We point out here that in his paper, Watkins' use of the term *symbol* includes n, the number of vertices. Also, Watkins obtains results for infinite circulants, but since we are interested in circulants as they apply to the design of networks, we choose not to include those results here.

Watkins makes use of the following definition due to Sabidussi [29]. The *lexicographic product* $H_1[H_2]$ of a graph H_1 by a graph H_2 has vertex set $V(H_1) \times V(H_2)$, and $[(x_1, x_2), (y_1, y_2)]$ is an edge of $H_1[H_2]$ if and only if either

(i) $[x_1, y_1] \in E(H_1)$, or

(ii) $x_1 = y_1$ and $[x_2, y_2] \in E(H_2)$.

The next definition, due to Watkins [35], defines a subgraph of the lexicographic product, and provides the basis for his algorithm for computing the connectivity of a circulant.

Let Θ and Λ be finite circulants having n_1 and n_2 vertices, respectively, and let G be a connected spanning subgraph of the lexicographic product $\Theta[\Lambda]$. For each $x \in V(\Theta)$, let Λ_x be the subgraph of G with vertex set $V(\Lambda_x) = \{(x, y) : y \in V(\Lambda)\}$. We call G a *circulant product*, or simply *c-product*, of Θ by Λ if the automorphism group of G contains an automorphism σ satisfying:

(a) the sets $V(\Lambda_x)$ for $x \in V(\Theta)$ are the orbits of σ^{n_1};

(b) the automorphism group of Θ contains an n_1-cycle τ such that $\sigma[\Lambda_x] = \Lambda_{\tau(x)}$.

The notation $G = \Theta c\Lambda$ means that G is a c-product of Θ by Λ. In developing his algorithm, Watkins makes use of the following properties of the c-product.

Lemma 4.4 *Let Θ and Λ be circulants. If $G = \Theta c\Lambda$, then G is a circulant.*

Lemma 4.5 *Let G be a circulant and let Λ be an atomic part of G. Then there exists a unique circulant Θ (up to isomorphism) such that $G = \Theta c\Lambda$.*

Lemma 4.6 *Let G be a graph and let Λ be an atomic part of G. Then G is a circulant if and only if $G = \Theta c\Lambda$ for some circulant Θ.*

Watkins also uses the following adaptation of a result by Hamidoune [18].

Lemma 4.7 *Let G be a finite abelian group and let Λ be the atomic part of Cay($G; S$) containing the identity of G. Then $V(\Lambda)$ is the subgroup of G generated by $V(\Lambda) \cap S$. The vertex sets of the atomic parts of Cay($G; S$) are the cosets of G with respect to $V(\Lambda)$.*

If G is a vertex-transitive graph, let Θ be the graph whose vertex set is the set of atomic parts of G. For distinct atomic parts $A_1, A_2 \in V(\Theta)$, define $[A_1, A_2] \in E(\Theta)$ if and only if some vertex of A_1 is adjacent to some vertex of A_2. The resulting graph is called the *atomic graph* of G.

Note that if G is not complete, then its atomic graph will not be. By Lemma 4.2, if A_1 is an atomic part of G, then $N(A_1)$ is the union of those atomic parts of G which, as vertices of the atomic graph Θ, are all the neighbors of the vertex $A_1 \in V(\Theta)$. We also have by Lemma 4.2 that a minimum vertex-disconnecting set is always a union of atomic parts.

The connectivity of a circulant $G = \Theta c \Lambda$ is equal to the least degree of regularity of Θ times the number of vertices in Λ, where the minimum is taken over all c-products $G = \Theta c \Lambda$ wherein Θ is not complete. In other words, the connectivity of a circulant is given by the cardinality of the neighborhood of an atomic part; that is, $\kappa = |N(\Lambda)|$ for atomic part Λ.

The approach of Watkins' algorithm is to run through the c-products $G = \Theta c \Lambda$ of a given circulant G with symbol S, seeking a c-product in which Λ is isomorphic to an atomic part of G. For each proper divisor d of n (the number of vertices in G), Watkins considers the (n/d)-element subgroup

$$A(d) = \{0, d, 2d, \ldots, n-d\}$$

of $V(G) = Z_n$. The subgraph $\Lambda(d)$ induced by $A(d)$ is then a candidate to be an atomic part of G. We subject such a candidate to five tests. If no candidate passes all these tests, then G has only trivial atomic parts, and hence $\kappa = \delta$. The tests are the following:

TEST 1: $A(d) \cap S \neq \phi$.

TEST 2: The greatest common divisor of $(A(d) \cap S) \cup \{n\}$ is d.

TEST 3: $d \geq 4$.

TEST 4: $\delta(\Theta(d)) \leq d-2$.

TEST 5: $|N(\Lambda(d))| < \delta(G)$.

Note that the goal of these tests is to identify a nontrivial atomic part. The validity of Tests 1 and 2 follows from Lemma 4.7. That is, the conditions in Tests 1 and 2 will be satisfied if $\Lambda(d)$ is a nontrivial atomic part. In particular, if $\Lambda(d)$ is a trivial atomic part, then $A(d)$ will simply consist of the element 0, and by definition, $0 \notin S$, hence we get Test 1. If Test 1 is passed, Test 2 then checks if $A(d)$ is generated by $A(d) \cap S$. If the greatest common divisor of $(A(d) \cap S) \cup \{n\}$ is greater than d, then $A(d)$ could not be generated as we could not get, for example, the element d.

Let $\Theta(d)$ be the circulant such that $G = \Theta(d)\mathrm{c}\Lambda(d)$ (the existence of $\Theta(d)$ is guaranteed by Lemma 4.5). Note that $|V(\Theta(d))| = d$. By an earlier discussion, we have that $\Theta(d)$ must not be complete, from which we get the validity of Tests 3 and 4. Of those values d which survive all of the tests, we only consider those for which $|N(\Lambda(d))|$ is minimum. This minimum value gives us the connectivity of G (and hence Test 5 is valid by Theorem 4.1).

In his paper, Watkins includes an APL function based on his algorithm. The input to the function is the symbol for a circulant G. The output from the function is the connectivity of G and the atomic number of G, as well as the symbol for the atomic part Λ of G, and the symbol for Θ, the first factor of the c-product $G = \Theta\mathrm{c}\Lambda$.

We now give a pseudo-code version of Watkins' algorithm. As before, comments appearing within the algorithm are delimited by a pair of double slashes. Note that we only include that part of the algorithm which gives the connectivity, and we have left out the determination of the atomic parts and first factor of the c-product that make up the input circulant.

4.2 Watkins' Algorithm for Computing Connectivity

```
STEP 1: Input circulant $C(n, S)$ where $S = \{a_1, a_2, \ldots, a_k\}$.
    Go to STEP 2.

STEP 2: Initialization.
    Let $S^{-1} = \{n - a_k, \ldots, n - a_1\}$;
    DELTA $= 2k$ if $a_k \neq n/2$, otherwise DELTA $= 2k - 1$;
    Let KAPPA = DELTA;
    Let NFACTORS be the set of proper divisors of $n$;
    $i = 0$.
    Go to STEP 3.

STEP 3: Let $i = i + 1$.
    If $i >$ |NFACTORS|, go to STEP 10.
    Let $d = i^{th}$ element of NFACTORS.
    Go to STEP 4.

STEP 4: If $d < 4$ return to STEP 3
    // i.e. $d$ is rejected — Test 3 //,
    otherwise go to STEP 5.

STEP 5: Let $S_d = \{s \in S : s = md$ for some $m \in Z^+\}$.
    // i.e. $S_d$ is the subset of $S$ made up of those elements which are
    multiples of $d$. Note that $S_d = A(d) \cap S$ //
    If $S_d = \phi$ return to STEP 3
    // i.e. $d$ is rejected — Test 1 //,
    otherwise go to STEP 6.

STEP 6: If $\gcd\{S_d \cup \{n\}\} \neq d$ return to STEP 3
    // i.e. $d$ is rejected — Test 2 //,
    otherwise go to STEP 7.

STEP 7: // The candidate's neighborhood is the union of all nonzero
    congruence classes (modulo $d$) represented in $S$, together with
    their inverses (modulo $d$) //
    Let NBD $= \{s \pmod{d} : s \in S \cup S^{-1}, s \not\equiv 0 \pmod{d}\}$.
    // Reject candidate if it is adjacent to all other atomic parts
    because first factor of c-product must not be a complete graph //
    If $|\mathrm{NBD}| > d-2$ return to STEP 3
    // i.e. $d$ is rejected — Test 4 //,
    otherwise go to STEP 8.

STEP 8: Let NU $= |\mathrm{NBD}| \cdot (n/d)$
    // note that NU $= |N(\Lambda(d))|$ //
    If NU $\geq$ DELTA return to STEP 3
    // i.e. $d$ is rejected — Test 5 //,
    otherwise go to STEP 9.

STEP 9: If NU $<$ KAPPA then let KAPPA $=$ NU.
    // i.e. choose minimum NU //
    Return to STEP 3.
```

STEP 10: Terminate.

KAPPA gives the connectivity of $C(n, S)$.

We now discuss the computational complexity of the two algorithms we have presented. The measure of complexity we will use is that of estimating an upper bound on the number of operations each algorithm will perform. Clearly, the two algorithms are very similar. First of all, they each process the divisors of n, the number of vertices. For an arbitrary positive integer n, note that its divisors occur in pairs. That is, if d is a divisor, then so too is n/d. The product of such a pair is equal to n, thus one divisor in each pair $(d, n/d)$ must be less than or equal to $n^{1/2}$. Thus, an upper bound on the number of divisors of n is $2n^{1/2}$.

Therefore, in Boesch and Tindell's algorithm, the number of times the loop initiated by **STEP 3** will be executed is of order $n^{1/2}$. This is also true of the loop initiated by **STEP 3** in Watkins' algorithm. We now consider the steps contained within each of these loops.

In Boesch and Tindell's algorithm, **STEP 5** has a constant number of operations: the calculation of NU, comparing NU to KAPPA, and possibly assigning NU to KAPPA. In **STEP 4**, we have the calculation of M, which requires a constant number of operations, and the comparison of M to the cardinality of R_m. We also have the determination of the set R_m, which is a subset of $S \cup S^{-1}$. Thus the complexity of **STEP 4** depends on the cardinality of $S \cup S^{-1}$. In particular, for each element j in $S \cup S^{-1}$, we must check that $j \not\equiv 0 \pmod{m}$, and we must check whether or not $j \pmod{m}$ already appears in R_m. Note that by definition, we have $|S| < (n+1)/2$, or equivalently, $|S| \leq \lfloor n/2 \rfloor$, so it follows that $|S \cup S^{-1}| \leq n-1$. Hence, the complexity of **STEP 4** is of order n. Therefore, the number of operations in Boesch and Tindell's algorithm is of order $n^{3/2}$.

In Watkins' algorithm, **STEP 4** just has the single operation of comparing d to 4. In **STEP 5**, we have the comparison of S_d to the empty set, and the determination of the set S_d, for which the number of operations depends on the cardinality of S. That is, for each element $s \in S$, we must check if $s = md$ for some $m \in Z^+$. Since by definition $|S| \leq \lfloor n/2 \rfloor$, we have that the number of operations in **STEP 5** is of order n.

In **STEP 6**, we need to determine the greatest common divisor of $S_d \cup \{n\}$ and compare it to d. If we view the calculation of the greatest common divisor of two integers as a single operation, then the complexity of **STEP 6** depends on the cardinality of $S_d \cup \{n\}$. Since $|S_d| \leq \lfloor n/2d \rfloor$, we have that **STEP 6** is of order n.

Note that **STEP 7** is basically equivalent to **STEP 4** of Boesch and Tindell's algorithm, which we have shown is of order n, while **STEP 8** and **STEP 9** combined are basically equivalent to **STEP 5** of Boesch and Tindell's algorithm, which has a fixed number of operations. So in total, the number of operations performed in **STEP 4** through **STEP 9** is of order n, since each of them is of order no greater than n. Therefore, the number of operations in Watkins' algorithm is of order $n^{3/2}$.

From the point of view of simply computing the connectivity of a circulant, **STEP 4**, **STEP 5** and **STEP 6** in Watkins' algorithm aren't really necessary. They appear in the algorithm because more is being determined than just the connectivity. As explained earlier, Watkins' APL version of his algorithm also gives as output the symbols for Λ and Θ, the two circulants whose c-product is the input circulant to which the algorithm is being applied.

4.3 Superconnectivity

In this section, we examine a concept that can be thought of as a higher order measure of connectivity relevant to the design of reliable networks. As we have seen previously in this chapter (see Theorem 4.8), *all* circulants have maximum edge-connectivity. So given a circulant, we know that at least δ edges must be removed in order to disconnect it. Let $N_\lambda(G)$ denote the number of edge-disconnecting sets of cardinality λ in the graph G. Now, consider the two graphs G_1 and G_2 shown in Figure 4.2. Both G_1 and G_2 are circulants ($G_1 = C(6, \{2,3\})$ and $G_2 = C(6, \{1,3\})$) thus $\lambda = \delta = 3$ in both cases, by point **(A)***(3)* of Theorem 4.8. For these graphs, we have $N_\lambda(G_1) = 7$ and $N_\lambda(G_2) = 6$, so in a sense, we may consider G_2 to be less vulnerable than G_1.

In a regular graph G with $\lambda = \delta$, the set of edges incident to a vertex forms a minimum edge-disconnecting set. If these are the *only* minimum size edge-disconnecting sets for G, we refer to G as a *super-λ* graph. Note that since the incidence sets of the vertices of G are all distinct, $N_\lambda(G) \geq n$, and if G is super-λ, then $N_\lambda(G) = n$. Thus a regular graph with $\lambda = \delta$ is super-λ if each minimum size disconnecting set of edges isolates a vertex. Referring again to Figure 4.2, we see that G_2 is super-λ, but G_1 is *not* super-λ since removing the set of edges corresponding to $a_2 = 3$ disconnects the graph without isolating a vertex.

Our interest in super edge-connectivity lies in determining which circulants have this property. Bauer, Boesch, Suffel and Tindell [1]

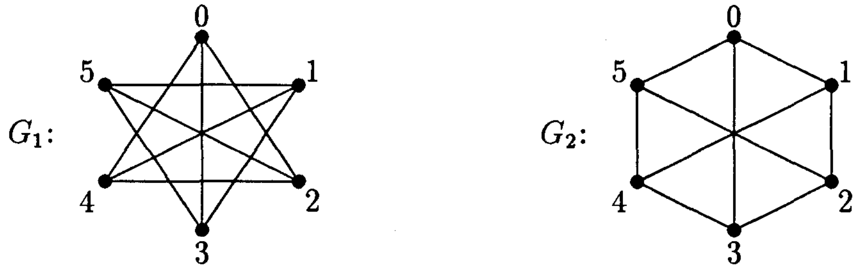

Figure 4.2: An example demonstrating the super-λ property

obtained the following result.

Theorem 4.11 *If $k \geq 2$, then $C(n, \{1, a_2, \ldots, a_k\})$ is super-λ.*

Boesch and Wang [12] improved on the above result by obtaining the following, which characterizes *all* super-λ circulants.

Theorem 4.12 *The only connected circulants which are not* super-λ *are the cycles $C(n, S)$ where $S = \{a_1\}$, and the graphs $C(2n, S)$ where $S = \{2, 4, \ldots, n-1, n\}$ with $n \geq 3$ an odd integer.*

One can define an analogous concept for vertices. We have seen in an earlier section of this chapter that certain classes of circulants attain maximum connectivity, so given such a circulant, we know that at least $\kappa = \delta$ vertices must be removed in order to disconnect it. In a regular graph G with $\kappa = \delta$, the neighborhood of each vertex will be a minimum size disconnecting set of vertices for G. If each minimum size vertex-disconnecting set isolates a vertex, then G is called *super-κ*.

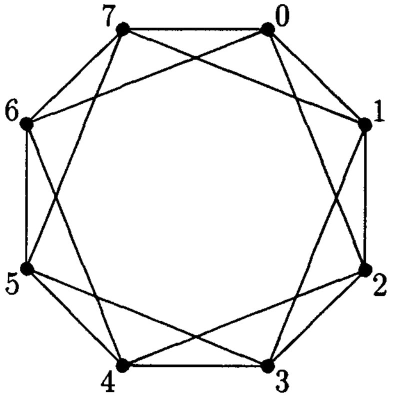

Figure 4.3: An example of a graph that is not super-κ

To help demonstrate this concept, we consider an example of a graph that does *not* have this superconnectivity property. Figure 4.3 shows the circulant $C(8, \{1, 2\})$, which has $\delta = 4$ and, since this graph is equivalent to the Harary graph $H_8(2)$, it has $\kappa = \delta = 4$. Now, removing the set of vertices $\{0, 3, 4, 7\}$ disconnects the graph without isolating a vertex; thus, the graph is not super-κ.

As pointed out by Boesch [6], this definition is just one of several possible choices. Note that a minimum vertex-disconnecting set could isolate several vertices, as for example in the case for complete bipartite graphs $K_{n,n}$. So one possible alternative definition could be to require that each minimum vertex-disconnecting set creates exactly two components, one of which is an isolated vertex. Boesch uses the term *hyper-κ* for this definition. Another alternative would be to let $M_\kappa(G)$ denote the total number of distinct vertex-disconnecting sets of cardinality κ in the graph G, and determine which graphs minimize $M_\kappa(G)$.

Unlike the case for super-λ, there are no results that fully characterize which circulants have the super-κ or hyper-κ properties, nor which circulants minimize $M_k(G)$. Some partial results can be found in Boesch and Thomas [10], Boesch and Felzer [9], Boesch and Tindell [4], and Boesch and Wang [11].

Chapter 5

Diameter

In designing reliable networks, several authors have noted that considering just the connectivity of the underlying graph is not sufficient. One should also take into account the transmission delays inherent in the design of the network. This corresponds to the diameter of the underlying graph. Bollobás [13] initiated work in the area of considering both connectivity and diameter as measures of reliability.

As we have seen in the preceding chapter, there are several classes of circulant graphs which have maximum connectivity; however, their diameters can vary greatly. Hence, we are interested in determining which circulants maximize connectivity while minimizing diameter. The graph theoretic terms relevant to this chapter are the following. The *length* of a path in a graph G is the number of edges the path contains. The *distance* $d(u, v)$ between two vertices u and v in a graph G is the length of a shortest path joining them. If no path joins u

and v, then we say $d(u, v) = \infty$. The *diameter* $d(G)$ of a graph G is the greatest distance between any pair of vertices. Due to symmetry, the diameter of a circulant graph can be determined by considering the greatest distance from 0 to any other vertex.

Several different approaches have been used to obtain diameter results for circulant graphs, and in this chapter we shall present some of them. One of the objectives of the diameter results we will discuss is to determine a lower bound for the diameter of a circulant. That is, given the parameters of a circulant (number of vertices, number of elements in the symbol) we would like to know what is the smallest diameter that can be obtained. Then, having established this bound, we examine results that determine some classes of circulants that achieve the lower bound. Before going into the details of the various results, we wish to comment on the distinctions between their two different types of backgrounds. In particular, there is the distinction between a graph theoretic approach and a computer science approach. In the area of computer networks, the standard topology is that of a ring network; that is, a cycle in graph theoretic terms. Cycles have relatively large diameter, and in an attempt to reduce the diameter by adding edges, we wish to retain certain properties. In particular, we would like to retain maximum connectivity and vertex-transitivity. As we have seen, certain circulants achieve this.

Most computer science work with circulants begins with a cycle, to which edges are added. Hence, most results in this area have $a_1 = 1$. In contrast, graph theoretic results tend not to have such a restriction on the first element of the symbol. We point out though that fixing $a_1 = 1$ is not a serious restriction, as the following proposition makes clear.

Proposition 5.1 *If the circulant* $G_1 = C(n, \{a_1, \ldots, a_k\})$ *is such that for some* i, $1 \leq i \leq k$, $\gcd(n, a_i) = 1$, *then there exists a circulant* $G_2 = C(n, \{b_j\})$, $1 \leq j \leq k$ *isomorphic to* G_1, *with* $b_i = 1$.

PROOF. As $\gcd(n, a_i) = 1$, there exists an integer r, relatively prime to n, such that $ra_i \equiv 1 \pmod{n}$. Now, multiply each element in G_1's symbol by r, to get $rG_1 = C(n, \{ra_1, ra_2, \ldots, ra_i, \ldots, ra_k\})$. Letting $b_j = ra_j, 1 \leq j \leq k$, gives us $rG_1 = G_2 = C(n, \{b_j\})$, with $b_i = 1$. It remains to show that each b_j is distinct. Suppose $b_j = b_m$ for $j \neq m$. Then $ra_j = ra_m$, implying $a_j = a_m$, which is a contradiction. Thus G_1 and G_2 are isomorphic. □

5.1 Diameter Results by Wong and Coppersmith

Of the results we wish to discuss, those achieved by Wong and Coppersmith [38] were obtained first. Although some of their results were later improved upon, their method is quite accessible. As we shall see, it is only their final, most general result that applies to circulants.

Let the vertices of an n-vertex digraph be labelled $0, 1, \ldots, n-1$. Pick any integer s, $1 < s < n$, and draw an arc from vertex i to vertex

$i+1 \pmod{n}$, and from vertex i to vertex $i+s \pmod{n}$. This defines a circulant *digraph*, which we denote $\vec{C}\ (n, \{1, s\})$. Note that at this point we are only considering a symbol of cardinality 2, with $a_1 = 1$.

By the number of steps from a fixed vertex i to a fixed vertex j, we shall mean the smallest possible number of arcs in a directed path. Let $d_n(s)$ denote the maximum number of steps from any i to any j. By symmetry we can assume $i = 0$. We wish to find a value of s which minimizes the diameter $d_n(s)$ of $\vec{C}\ (n, \{1, s\})$.

Instead of computing the number of steps needed to travel from 0 to j, we will calculate the vertices which can be reached from 0 in a given number of steps. In the first quadrant ($x \geq 0, y \geq 0$) of the Euclidean plane, we fill the lattice points with the vertices reachable from 0 in 0 steps, 1 step, 2 steps, and so on. Note that to reach a vertex, only the total number of 1's and total number of s's are material, not their ordering. At lattice point (x, y) we fill in the value k determined by $x1 + ys \equiv k \pmod{n}$ meaning that in a total of $x + y$ steps, the vertex k can be reached. We proceed in the following manner:

Start from the origin $(0,0)$, then go along the line $(1,0)$, $(0,1)$, then the line $(2,0)$, $(1,1)$, $(0,2)$, and so on. At each point (x, y), if the value k has not appeared so far, we write it down; otherwise we leave a blank. We stop when all values of k ($k = 0, 1, \ldots, n-1$) are accounted for.

As an example of this procedure, consider the case $n = 16$ and $s = 7$, shown in Figure 5.1. Here, k is determined by $x1 + y7 \equiv k$ (mod 16).

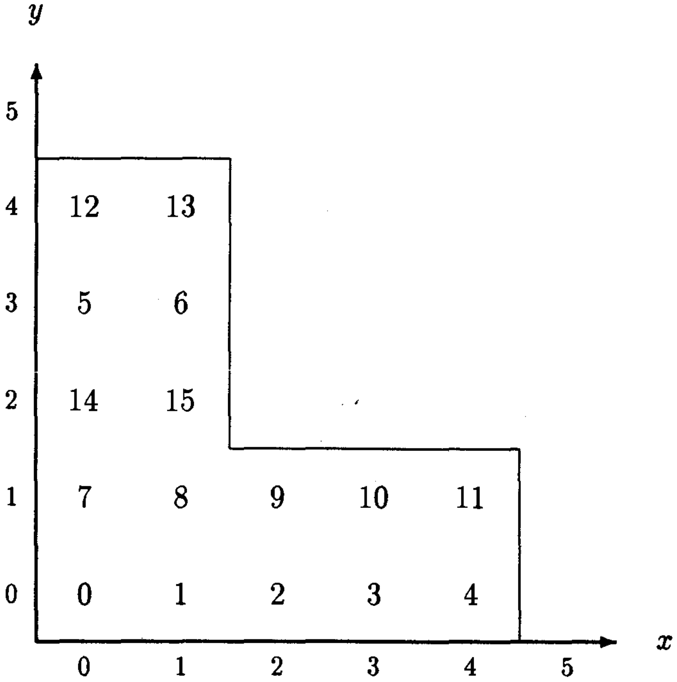

Figure 5.1: Sample pattern with $n = 16$ and $s = 7$

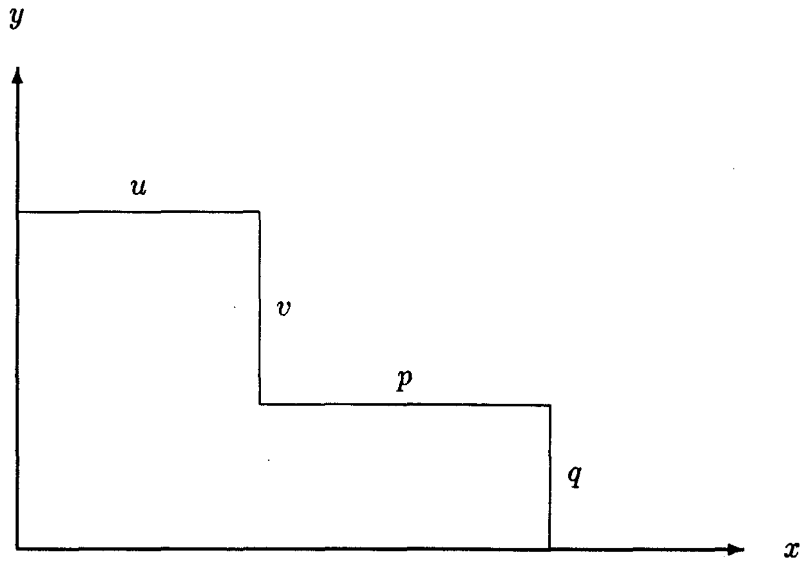

Figure 5.2: Filled pattern of Lemma 5.1

Lemma 5.1 *The filled pattern is always of the form shown in Figure 5.2, where $u \geq 0, v \geq 0, p > 0, and\ q > 0$.*

PROOF. Notice that if the point (x_0, y_0) is blank, then all lattice points $\{(x,y) : x \geq x_0, y \geq y_0\}$ will also be blank. For example, in Figure 5.1 the point $(2,2)$ is blank because it represents $(2)1 + (2)7 = 16 \equiv 0 \pmod{16}$, which is already represented by the point $(0,0)$. Now, the point $(2,3)$, which is one unit above $(2,2)$, will represent the same value as the point one unit above $(0,0)$; that is, the point $(0,1)$. So it follows that $(2,3)$ will be blank, and so on. Therefore, at the least, we will get the pattern shown in Figure 5.3.

Let $A = (0,a)$ be the first point on the y-axis to be blank. This implies the integer $0 \cdot 1 + a \cdot s \pmod{n}$ has already appeared previously. Thus, there exist integers $f \geq 0$ and $g \geq 0$ such that $f + g \leq a$ and $0 \cdot 1 + a \cdot s \equiv f \cdot 1 + g \cdot s \pmod{n}$. Now consider the point $(0, a-1)$, for which we have $0 \cdot 1 + (a-1) \cdot s \equiv f \cdot 1 + (g-1) \cdot s \pmod{n}$, and $f + (g-1) \leq a - 1$.

By the definition of f and g, we know the point (f, g) was visited before $(0, a)$, which implies $(f, g-1)$ must have been visited before $(0, a-1)$ if $(f, g-1)$ is in the first quadrant. But then $(0, a-1)$ would be blank, and hence $(f, g-1)$ cannot be in the first quadrant. Thus $g - 1 < 0$, implying $g = 0$. Therefore, the integer $0 \cdot 1 + a \cdot s \pmod{n}$ appears at a point on the x-axis.

A similar argument shows that the first blank point on the x axis corresponds to an integer that appears previously on the y-axis. Applying this argument to points like B, B' or B'', we find that these points represent an integer that appears in a previously visited point that lies on both axes; in other words, the origin. But this implies that the points immediately to the left of B, B' and B'' all represent the value $n - 1$, which is a contradiction. Thus there can be at most one point like B, B' or B'', and the result follows. □

Lemma 5.2 *Given n and s, if the resulting pattern has sides u, v, p, q as in* Lemma 5.1, *then $d_n(s) = u + q + \max\{v, p\} - 2$.*

PROOF. In $x + y$ steps, vertex k can be reached. The way we've drawn the pattern, where k appears gives us the fewest number of steps

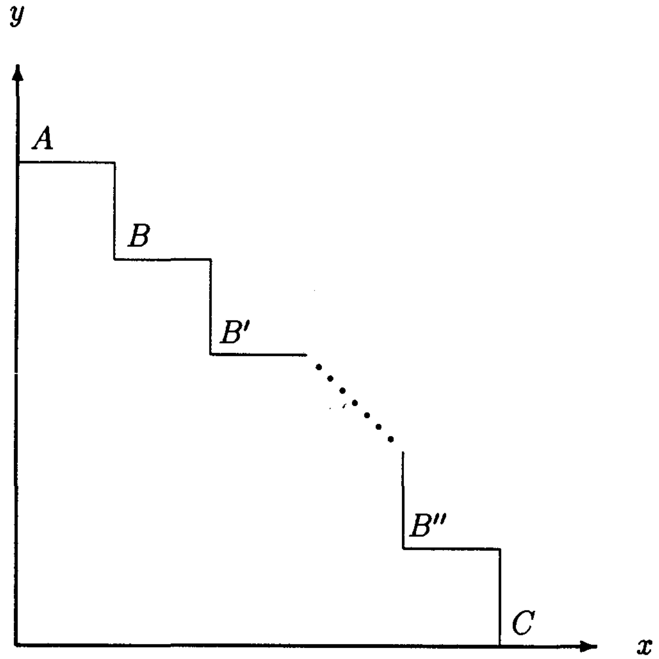

Figure 5.3: Pattern from proof of Lemma 5.1

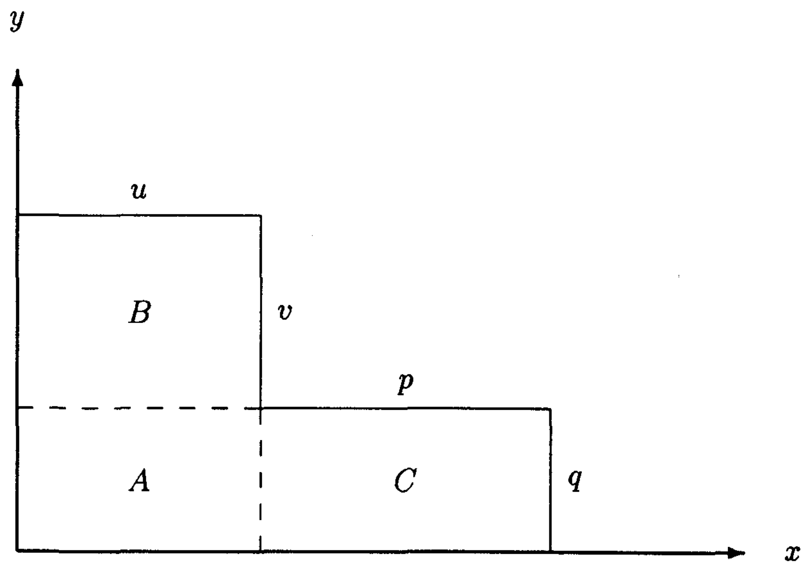

Figure 5.4: Diagram for proof of Lemma 5.2

to that vertex. So we want to know what is the maximum $x+y$ can be. Consider the diagram shown in Figure 5.4.

The total area of the diagram is: $u(v+q)+pq=n$. Furthermore, we have the following table:

BLOCK	AREA	MAXIMUM OF $(x+y)$
A	uq	$u+q-2$
B	uv	$q+u+v-2$
C	pq	$u+p+q-2$

Therefore, $d_n(s)=u+q+\max\{v,p\}-2$. ◫

As an application of Lemma 5.2, consider again the example shown in Figure 5.1. From the Lemma, we have $d_{16}(7) = 2 + 2 + 3 - 2 = 5$ and an exhaustive check confirms this is correct.

Based on Lemmas 5.1 and 5.2, Wong and Coppersmith obtained the following result.

Theorem 5.1 *For $\vec{C}\ (n, \{1, s\})$, we have $d_n(s) \geq (3n)^{1/2} - 2$.*

PROOF. Viewing d_n as a function of u, v, q and p (from Lemma 5.2), we shall minimize d_n subject to the constraints

$$u(v + q) + pq = n \text{ and } u, v, p, q \geq 0, \tag{5.1}$$

where u, v, p and q are real numbers.

Let us assume that (u, v, p, q) is a minimization point of d_n and suppose $v > p$. Define the constant

$$D = \left[\frac{(uv + uq + pq)}{(uv + uq + vq)}\right]^{1/2}$$

and let $u' = uD, q' = qD$, and $v' = p' = vD$. Now, $u'(v' + q') + p'q' = D^2(uv+uq+vq) = uv+uq+pq = n$. Thus the point (u', v', p', q') satisfies the constraints (5.1). Furthermore, $u'+q' + \max\{v', p'\} = u'+q'+v' = D(u+q+v) = D(u+q + \max\{v, p\})$, and since $p < v$ implies $D < 1$, we have that $d_n(u', v', p', q') < d_n(u, v, p, q)$ contradicting our assumption that (u, v, p, q) was a minimization point. Therefore $v \leq p$. By a similar argument we get that $p \leq v$, and hence $v = p$.

So now our problem is to minimize $u+q+v$ subject to $uv+uq+vq = n$. By Lagrange's method of multipliers, we form the function g defined by

$$g(u,q,v) = u+q+v+\lambda(uv+uq+vq).$$

Taking partial derivatives, we get

$$\begin{aligned}\partial g/\partial u &= 1+\lambda v+\lambda q\\ \partial g/\partial q &= 1+\lambda u+\lambda v, \text{ and}\\ \partial g/\partial v &= 1+\lambda u+\lambda q.\end{aligned}$$

This gives us the following system of equations:

$$\begin{aligned}1+\lambda v+\lambda q &= 0\\ 1+\lambda u+\lambda v &= 0\\ 1+\lambda u+\lambda q &= 0\\ uv+uq+vq &= n.\end{aligned}$$

From the first 3 equations we get $(v+q) = (u+v) = (u+q) = -1/\lambda$, or $u = v = q$. From the fourth equation, the equation of constraint, it follows that $u = v = q = (n/3)^{1/2}$. Thus by Lemma 5.2, the minimum value of $d_n(s)$ is $(3n)^{1/2} - 2$. □

Wong and Coppersmith then let the cardinality of the symbol be arbitrary, therefore the subsequent results apply to circulant digraphs of the form $\vec{C}\ (n, \{1, a_2, \ldots, a_k\})$. The final generalization made by Wong and Coppersmith is to allow both the positive and negative of each element in the symbol, which gives us the circulants $C(n, \{1, a_2, \ldots, a_k\})$.

For both the cases $\vec{C}\ (n, \{1, a_2, \ldots, a_k\})$ and $C(n, \{1, a_2, \ldots, a_k\})$, we mark off the lattice points of k-dimensional Euclidean space. In the first case, only the first "quadrant" (that is, $x_1 \geq 0, x_2 \geq 0, \ldots, x_k \geq 0$)

is considered, while in the second case, the x_i are not restricted to nonnegative values. In order to establish the required marking scheme, Wong and Coppersmith first partition the lattice points $(x_1, \ldots, x_k)$ into specially defined classes. They then recursively define the order in which the lattice points are to be visited. That is, they specify the order in which we visit the classes, as well as the order in which we visit the lattice points within each class. On each visit to a lattice point in a fixed class, we write an integer at that lattice point, based upon which class the lattice point appears in. The procedure stops once n lattice points have been visited.

It turns out that by performing the above marking scheme for the case $\vec{C}\,(n, \{1, a_2, \ldots, a_k\})$, the pattern one marks off is effectively a "triangle", in the first "quadrant". For the case $C(n, \{1, a_2, \ldots, a_k\})$, one effectively marks off a "quadrilateral" rather than a "triangle". Based on the cardinality of the above described classes, Wong and Coppersmith obtain lower bounds for the diameter of these circulants. In particular, they obtained the following result.

Theorem 5.2 *For a circulant $G = C(n, \{1, a_2, \ldots, a_k\})$,*

$$d(G) \geq \frac{1}{2}(k!n)^{1/k} - \frac{1}{2}(k+1).$$

We note that this result has $a_1 = 1$, but as pointed out earlier, this isn't a serious restriction.

5.2 Further Diameter Results

To obtain results on a lower bound for the diameter of circulants, the method used by Boesch and Wang in [11] makes use of a tree structure like that shown in Figure 5.5. The example shown in Figure 5.5 is for the case where the symbol S has cardinality 3; that is, for the circulant $C(n, \{a_1, a_2, a_3\})$; however, the method can be applied in general. Each edge in the tree represents an element of S, either positive or negative. The root of the tree corresponds to the vertex 0 of the circulant. A vertex v in the tree gets labelled with the vertex of the circulant that is reached from 0 by using the elements of S that lie on the path in the tree from 0 to v. For example, vertex $a_1 - a_2$ is reached from 0 by first using a_1, then using $-a_2$. Of course, all calculations are done modulo n.

Note that vertices in the circulant can be reached from 0 in several ways. For example, $a_1 + a_2$ can be reached by using a_1, then a_2, or by first using a_2 and then a_1. In the tree structure, only one path will be represented; hence, a_2 followed by a_1 does not appear. Also, we only want to represent the shortest possible path, so when the element a_i appears, the element $-a_i$ will never appear in the same path, as then we will get to a vertex already reached by 0. Thus, for example, in Figure 5.5, there is no edge labelled $-a_1$ from vertex a_1 to any vertex in Level 2.

Note that it is possible for vertices in different levels to be the same. For example, a_2 could equal $2a_1$. Similarly, vertices in the same level

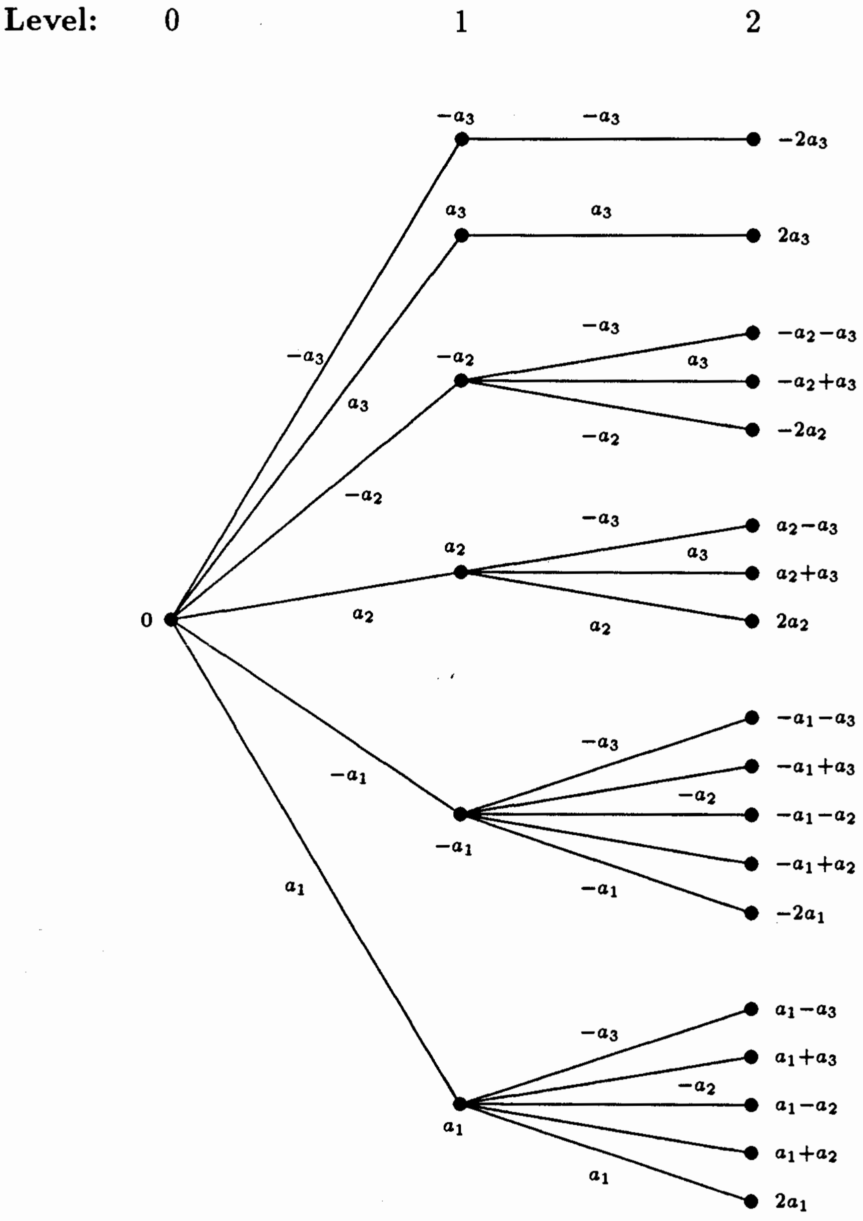

Figure 5.5: Tree structure for the case $C(n, \{a_1, a_2, a_3\})$

could be equal, such as $a_1 + a_3$ and $2a_2$.

To make vertex 0 reach a maximum number of vertices, we need to choose a_1, a_2 and a_3 such that the vertices in the same and different levels are distinct as many times as possible.

Let X_m denote the upper bound on the number of vertices 0 can reach by using at most m jump sizes. Then assume the number of vertices n in G satisfies

$$X_m \geq n - 1 > X_{m-1}.$$

If vertex 0 reaches all other vertices in G, then at least m jump sizes should be utilized by vertex 0. This is equivalent to saying $d(G) \geq m$. Thus m is the lower bound for the diameter of circulant graphs. Based on this, Boesch and Wang [11] obtained the following result.

Theorem 5.3 *Let $G = C(n, S)$ where $S = \{a_1, a_2, \ldots, a_k\}$ and $a_k < n/2$.*
If $X_m(k) \geq n > X_{m-1}(k)$ then $d(G) \geq m$, where

$$X_m(k) = 1 + \sum_{i=1}^{m} Y_i \quad \text{and}$$

$$Y_i = \sum_{j=1}^{\min(k,i)} \binom{k}{j} \binom{i-1}{j-1} 2^j.$$

The table shown in Figure 5.6 lists $X_m(k)$ for $1 \leq m \leq 7$, and $1 \leq k \leq 6$. As an example of how to use the table, consider the class of

m	1	2	3	4	5	6	7
k							
1	3	5	7	9	11	13	15
2	5	13	25	41	61	85	113
3	7	25	63	129	231	377	575
4	9	41	129	321	681	1289	2241
5	11	61	231	681	1683	3653	7183
6	13	85	377	1289	3653	8989	19825

Figure 5.6: Table of values for $X_m(k)$

all 29-vertex circulants with a symbol of cardinality 3. From the table, if follows that $d(G) \geq 3$.

For the case where $a_k = n/2$, Boesch and Wang obtained the following result.

Theorem 5.4 *Let $G = C(n, S)$ where $S = \{a_1, a_2, \ldots, a_{k-1}, n/2\}$, n even.*
If $Z_m \geq n - 1 > Z_{m-1}$, then $d(G) \geq m$, where

$$Z_m = \sum_{i=1}^{m}(Y_i + Y_{i-1}) \quad \textit{with} \quad Y_0 = 1,$$

and for $i \geq 1$, Y_i is defined as in Theorem 5.3.

Boesch and Wang then further consider the case for circulants which have a symbol of cardinality 2. In particular, they determine suitable values of a_1 and a_2 so that the lower bound diameter is actually achieved. First, the following lemma is needed.

Lemma 5.3 *Let r and p be two positive integers such that $1 \leq r \leq p(p+1)$. Then there exist integers a and b such that $|a| + |b| \leq p$ and $a(p+1) + bp = r$.*

PROOF. Clearly, $a(p+1) + bp = r$ is solvable for a and b since $\gcd(p, p+1) = 1$. It remains to show that there exists such an a and b so that $|a| + |b| \leq p$. Note that we can write r as $r = kp + \alpha$ for $k \geq 0$ and $0 \leq \alpha \leq p-1$. Now let

$$\begin{array}{lll} a = p, & b = 0 & \text{if } k = p+1, \\ a = \alpha - p, & b = k + 1 - \alpha + p & \text{if } 2\alpha \geq p + 1 + k, \text{ and} \\ a = \alpha, & b = k - \alpha & \text{otherwise.} \end{array}$$

It is not difficult to check that this solution satisfies the conditions. □

We are now ready to prove the following result.

Theorem 5.5 *Let $G = C(n, S)$ where $S = \{m, m+1\}$ be a circulant graph on n vertices with $n > 6$ and $m = \lceil (-1 + \sqrt{2n-1})/2 \rceil$. Then $d(G) = m$. Moreover, m is the minimum diameter over the class of all circulant graphs $C(n, S)$ with $S = \{a_1, a_2\}$ where n is fixed, $a_1 < a_2 < n/2$ but a_1 and a_2 are otherwise arbitrary.*

PROOF. Since $m = \lceil (-1 + \sqrt{2n-1})/2 \rceil$, we have $m \geq (-1 + \sqrt{2n-1})/2$, from which it follows that $n \leq 2m(m+1)+1$. Furthermore, from $m < 1+(-1+\sqrt{2n-1})/2$ we get $n > 2m(m-1)+1$. Therefore, $2m(m+1)+1 \geq n > 2m(m-1)+1$. Note that substituting $k = 2$ into the definition of $X_m(k)$ in Theorem 5.3 yields

$$X_m(2) = 2m(m+1)+1.$$

Thus we have $X_m(2) \geq n > X_{m-1}(2)$. In order to apply Theorem 5.3, we need $a_2 = m+1 < n/2$. This is the case for $n > 6$, which we have by the statement of this theorem. Therefore, by Theorem 5.3, we have

$$d(G) \geq m. \tag{5.2}$$

By Lemma 5.3, if $1 \leq r \leq m(m+1)$ then there exist integers a and b so that $a(m+1)+bm = r$ and $|a|+|b| \leq m$. This is equivalent to saying that vertex 0 can reach vertex i, for $1 \leq i \leq m(m+1)$, by using at most m steps. We have that $2m(m+1) \geq n-1$, and since $m(m+1)$ is an integer, it follows that $m(m+1) \geq \lfloor n/2 \rfloor$. Thus vertex 0 can reach half of the n vertices. By the symmetry of circulants, vertex 0 can also reach the other half of the n vertices. Since vertex 0 can reach all of the other vertices of G in m or fewer steps, we have that $d(G) \leq m$. Combining this with (5.2), we have $d(G) = m$. It follows from Theorem 5.3 that m is also the minimum diameter over all circulants $C(n, \{a_1, a_2\})$ with $a_1 < a_2 < n/2$. □

Note that the result of Theorem 5.5 is optimal, and that it is an improvement upon the result of Wong and Coppersmith for circulants with symbols of cardinality 2. (Theorem 5.2 due to Wong and Coppersmith gives $(\sqrt{2n}-3)/2$ as the lower bound.)

Other authors have obtained the above result, using various different methods. In [39], Yebra, Fiol, Morillo and Alegre obtain diameter results for general circulants with a symbol of cardinality 2, and for particular circulants with a symbol of cardinality 3. Their objective is to determine the maximum possible number of vertices that such circulants can have for a given diameter. The approach used by Yebra et al. is to associate the adjacency pattern of the vertices of a circulant with a tessellation of the plane.

As circulants are vertex-transitive, when studying their diameter one need only consider the distances from the vertex 0 to each of the other vertices. Let $C(n, \{a_1, a_2\})$ be the circulant under consideration, and let d be a given diameter. We wish to determine the maximum possible value for n.

Note that the 4 vertices $\pm a_1, \pm a_2$ are at distance one from vertex 0, the 8 vertices $\pm 2a_1, \pm a_1 \pm a_2, \pm 2a_2$ are at distance at most two, the 12 vertices $\pm 3a_1$, $\pm 2a_1 \pm a_2$, $\pm a_1 \pm 2a_2, \pm 3a_2$ are at distance at most three, and so on, where all calculations are done modulo n. If all the numbers $xa_1 + ya_2$ (modulo n), where $|x| + |y| \leq d$, were different, we would then get the maximum possible number of vertices n_d, for which we thus have $n_d = 1 + \sum_{i=1}^{d} 4i = 2d^2 + 2d + 1$. So we have $n \leq n_d$, and Yebra et al. show that this bound can be achieved.

Let the integers which represent the vertices that can be reached from vertex 0 in a specific number of steps be arranged in the pattern shown in Figure 5.7. That is, each step along an indicated edge is a one unit step in either positive or negative a_1 or a_2. As alluded to above, the situation we seek is one in which each of the n_d numbers in the pattern is distinct. That is, we want each of the numbers $0, 1, \ldots, n_d - 1$ to appear exactly once in the pattern. Clearly, the size of the pattern depends on d.

Note that in order to have each of the numbers $0, 1, \ldots, n_d - 1$ appear in the pattern, vertex 0 must be able to reach each of the other vertices in the circulant. This is only possible if the circulant is connected, which by Theorem 4.10 is the case if and only if $\gcd(n, a_1, a_2) = 1$.

Now, suppose we position this pattern on the Euclidean plane so that the integer 0 in the pattern corresponds to the lattice point $(0, 0)$, and the integer obtained by taking x steps in the a_1 direction and y steps in the a_2 direction corresponds to the lattice point (x, y). Note that since all calculations are done modulo n, the pattern will repeat itself. In particular, suppose at lattice point (x_0, y_0) we have the integer i. Then all lattice points $\{(x_0 + x, y_0 + y) : xa_1 + ya_2 \equiv 0 \pmod{n}\}$ will also contain the integer i. Thus we get a periodic repetition of the pattern on the plane. This fact is shown in Figure 5.8 where we have used the example $n = n_3 = 25, a_1 = 3$ and $a_2 = 4$.

If we view the pattern as a tile, then as Figure 5.8 demonstrates, these tiles will tessellate the plane. Thus, we must show that for an arbitrary diameter d and for $n = 2d^2 + 2d + 1$, there exist suitable values of a_1 and a_2 that result in such a tessellation. Note that the tessellation is characterized by the positions of the 0's throughout the plane, as they appear in each tile. This leads to the following system

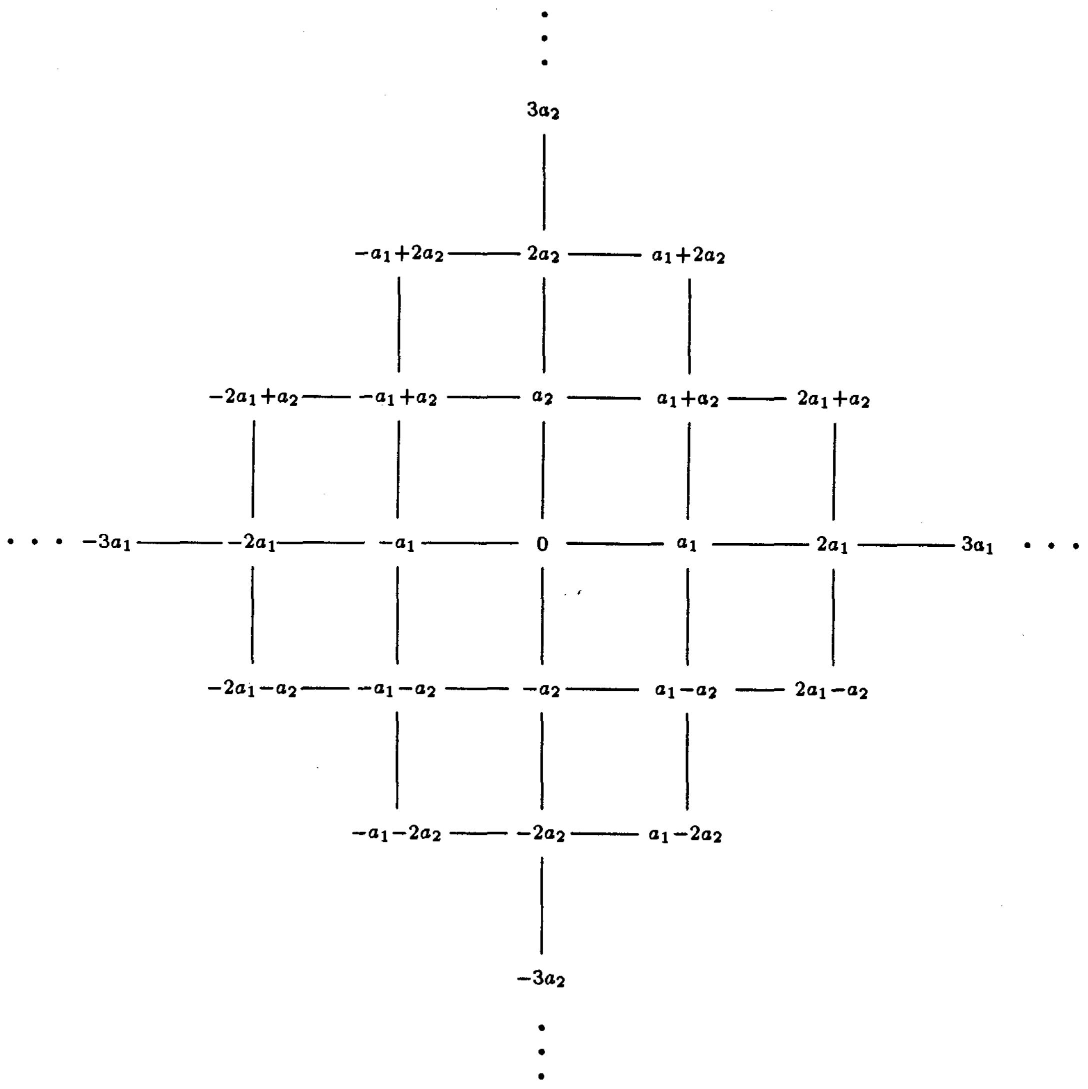

Figure 5.7: Pattern of vertices reachable from 0

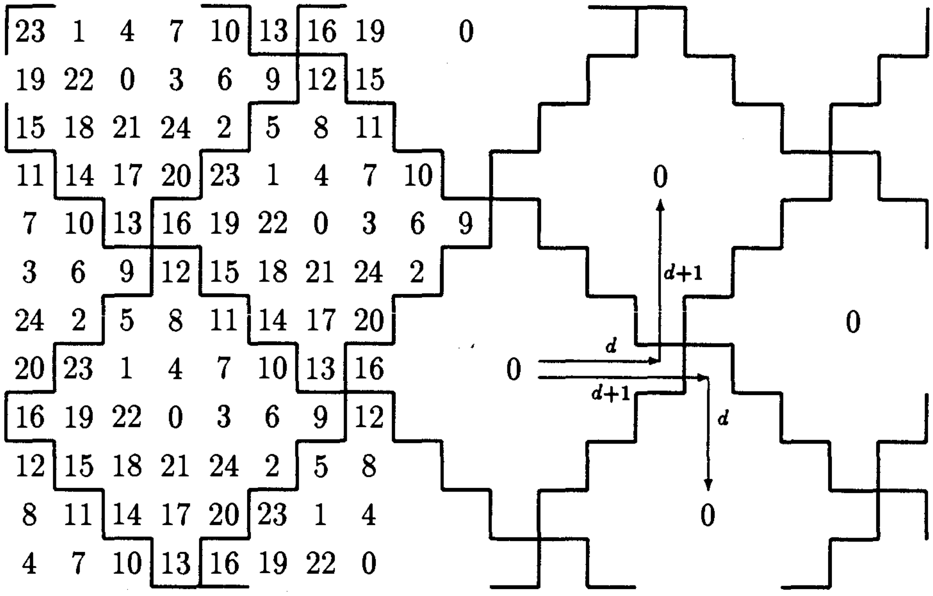

Figure 5.8: Tessellation of the plane ($n = 25, a_1 = 3, a_2 = 4$).

of equations:

$$\begin{aligned} (d+1)a_1 - da_2 &\equiv 0 \pmod{n} \\ da_1 + (d+1)a_2 &\equiv 0 \pmod{n}. \end{aligned} \tag{5.3}$$

In matrix form we get:

$$A\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \equiv 0 \quad \text{or} \quad A\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} n,$$

$$\text{where } A = \begin{pmatrix} d+1 & -d \\ d & d+1 \end{pmatrix}.$$

Now, $\det(A) = (d+1)^2 + d^2 = 2d^2 + 2d + 1 \equiv 0 \pmod{n}$, thus the homogeneous system (5.3) has non-trivial solutions. Solving for a_1 and a_2 gives us the following:

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} d+1 & d \\ -d & d+1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \quad \text{for some } \alpha, \beta \in Z.$$

By setting values to α and β, we obtain particular solutions. For example, letting $\alpha = 0$ and $\beta = 1$, we obtain the solution $a_1 = d$ and $a_2 = d+1$. Since $\gcd(n, d, d+1) = 1$ for all d, this solution satisfies the connected condition and hence is admissible. Note that this solution was used to obtain the example in Figure 5.8.

Another solution that is valid for all d is the following. Let $\alpha = \beta = 1$, which gives $a_1 = 2d+1$ and $a_2 = 1$. This solution trivially satisfies the connected condition. Solutions obtained by setting other values to α and β may lead to previously obtained solutions, or may not even be admissible, depending on the value of d. For example, letting $\alpha = 1$ and $\beta = 2$ gives us the solution $a_1 = 3d + 1$ and $a_2 = d + 2$. For $d = 3$, this leads to $n = 25, a_1 = 10$ and $a_2 = 5$ for which we get $\gcd(25, 10, 5) = 5 \neq 1$.

So we have for values of n which satisfy

$$2(d-1)^2 + 2(d-1) + 1 < n \leq 2d^2 + 2d + 1,$$

d is the smallest possible diameter for a circulant with n vertices. Furthermore, in [39], Yebra et al. state that for such values of n, the circulant $C(n, \{d, d+1\})$ achieves this minimum diameter. Note that if we solve the inequality $n \leq 2d^2 + 2d + 1$ for d, we get

$$d \geq -\frac{1}{2} + \frac{1}{2}\sqrt{2n-1},$$

which agrees with Boesch and Wang's result in Theorem 5.5.

The results that Yebra et al. obtained for circulants with a symbol of cardinality 3 apply only to circulants of the form $C(n, \{a_1, a_2, a_1 + a_2\})$. Letting $a_3 \equiv -(a_1 + a_2)$ modulo n, we get the pattern shown in Figure 5.9, where each edge represents a one unit step in either positive or negative a_1, a_2 or a_3. In this case, the maximum possible number of vertices is $n_d = 1 + \sum_{i=1}^{d} 6i = 3d^2 + 3d + 1$. As before, the situation we seek is one in which each of the n_d numbers in the pattern is distinct.

Let the infinite plane be divided into equal hexagons which we number as in the pattern. We will then get a periodic repetition of the pattern on the plane, and if we view the pattern as a tile, we get a tessellation of the plane as shown in Figure 5.10. The tessellation is

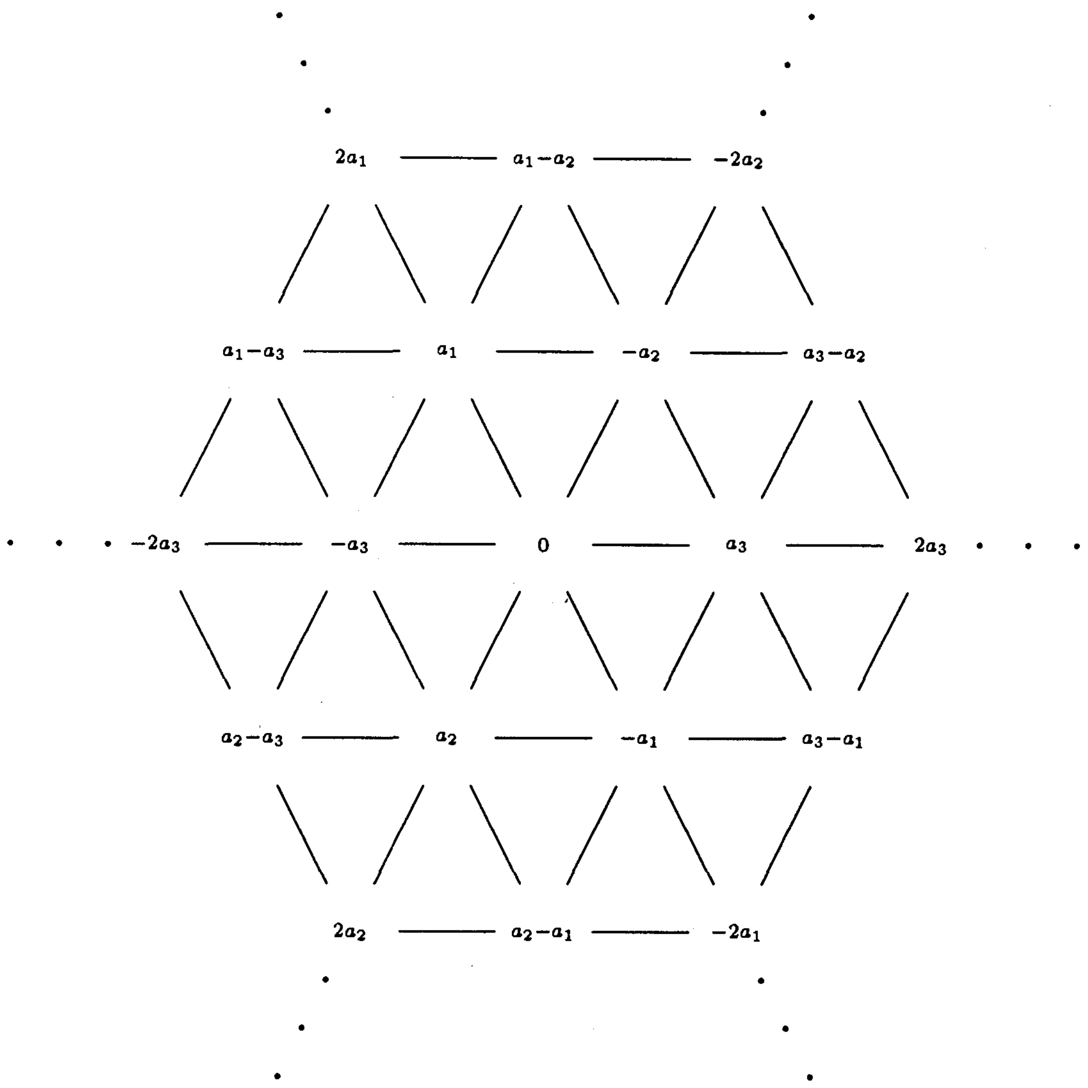

Figure 5.9: Pattern for symbol of cardinality 3.

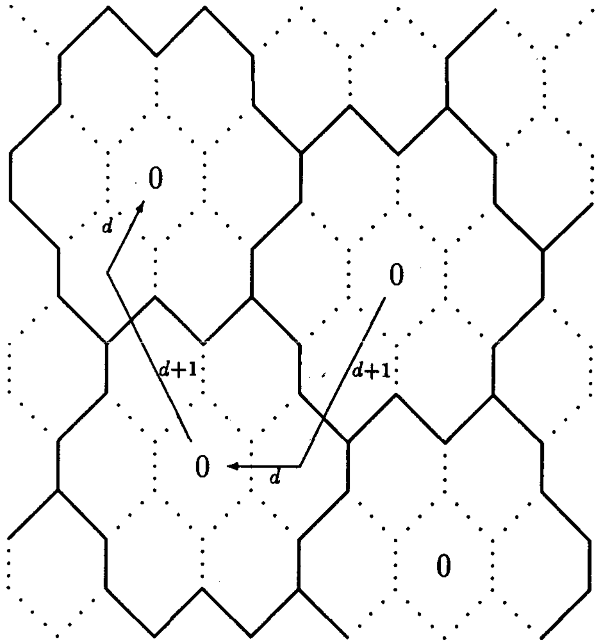

Figure 5.10: Tessellation of the plane with hexagonal tiles.

characterized by the positions of the 0's, from which we get the following system of equations:

$$\begin{array}{llllll}(d+1)a_1 & -\, da_2 & & \equiv & 0 \pmod{n} \\ & (d+1)a_2 & -\, da_3 & \equiv & 0 \pmod{n} \\ a_1 & +\, a_2 & +\, a_3 & \equiv & 0 \pmod{n}. \end{array} \tag{5.4}$$

Note that the third equation in (5.4) follows from the definition of a_3.

Letting A denote the coefficient matrix of system (5.4), we have that $\det(A) = (d+1)(2d+1) + d^2 = 3d^2 + 3d + 1 \equiv 0 \pmod{n}$. Hence the homogeneous system has non-trivial solutions.

Solving for a_1, a_2 and a_3 we get:

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} d^2 & 2d+1 & d \\ d(d+1) & -d & d+1 \\ (d+1)^2 & -d-1 & -2d-1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}, \quad \text{for } \alpha, \beta, \gamma \in Z.$$

As an example of a particular solution, let $\alpha = 0, \beta = 1$ and $\gamma = 1$, for which we get

$$a_1 = 3d + 1, \qquad a_2 = 1, \qquad a_3 = -3d - 2.$$

Furthermore, we note that this solution is admissible since $\gcd(n, 3d + 1, 1, -3d - 2) = 1$. Solving the inequality $n \leq 3d^2 + 3d + 1$ gives us the lower bound

$$d \geq -\frac{1}{2} + \frac{1}{2}\sqrt{(4n-1)/3}$$

for the diameter of a circulant of the form $C(n, \{a_1, a_2, a_1 + a_2\})$.

5.3 Results for Distributed Loop Networks

As stated at the beginning of this chapter, the ring network is a very popular network topology. However, it has relatively large diameter. One way to decrease the diameter of such a network is to add links to the nodes. The resulting networks are called *loop networks.* A specific example of these are *double loop networks*, which in terms of our circulant definitions, are equivalent to the circulants $C(n, \{1, s\})$, for some integer $s < n/2$. Note that in this section, we are dealing with loop networks in which the underlying graph is *undirected.* For the directed case, several results on lower and upper bounds for the minimum diameter and on upper bounds for the maximum number of nodes can be found in Hsu and Jia [21].

In [17], Du, Hsu, Li and Xu obtain results for double loop networks. In particular, they determine several infinite classes of values of n, the number of nodes, for which there exists a network that achieves the lower bound given by Theorem 5.5.

Let LB(n) denote the lower bound for the diameter of a circulant with n vertices, and symbol of cardinality 2. That is, LB(n) $= \lceil(-1 + \sqrt{2n-1})/2\rceil$. By *optimal diameter*, which we shall denote as $d(n)$, we mean the smallest possible diameter for a fixed n, over all valid values of s. That is, $d(n) = \min\{d(C(n, \{1, s\})) : 1 < s < (n+1)/2\}$. Furthermore, let $[0, i]$ denote the set of integers from 0 to i, inclusive.

A circulant $G = C(n, \{1, s\})$ is said to be *optimal* if it has the optimal diameter, and it is said to be *tight* if its diameter equals LB(n).

It is clear that tightness implies optimality, but the converse does not hold.

The approach of Du et al. is to establish a suitable upper bound on the diameter, then determine for which values of n, if any, this upper bound equals the lower bound. In particular, they obtained the following result.

Theorem 5.6 *Given n and s, let $G = C(n, \{1, s\})$, $b = \lfloor n/s \rfloor$ and $m = n - bs$. Then $d(G) \leq \max\{b+1, m-2, s-m-1\}$.*

The technique used by Du et al. to prove this theorem involves placing the nodes of the network on a line, and labelling them 0 to n, where n is understood to be the same node as 0. By suitably partitioning the integers $[0, n]$ based on the value of s, Du et al. then determine the maximum number of steps required to travel from node 0 or n to each of the other nodes, using steps of size ± 1 and $\pm s$. The problem of optimization is thus reduced to selecting the number s so that b, m and $s - m$ are as small as possible.

In seeking values of n for which there exist networks with the lower bound diameter, Du et al. make use of a form of the following result.

Lemma 5.4 *Every positive integer n can be uniquely represented as either $n = 2t^2 + 2t + 1$ or $n = 2t^2 + kt - h$ where $0 \leq t$, $-1 \leq k \leq 2$, and $0 \leq h < t$, and either $h \neq t - 1$ or $k \neq -1$.*

A proof of Lemma 5.4 appears in Hsu and Shapiro [23].

By using appropriate values of n and s in Theorem 5.6, Du et al. obtained the following result.

Theorem 5.7 *For $n = 2t^2+kt+h$, where $1 \leq h \leq 3$ and $2 \leq k \leq h+3$, let $G = C(n, \{1, 2t+(k-1)\})$. Then $d(G) = t+1 = LB(n)$. Moreover, for $G = C(2t^2+3t, \{1, 2t+2\})$, $d(G) = t+1 = LB(2t^2+3t)$.*

Theorem 5.7 gives us 13 infinite classes of n for which the lower bound can be achieved. Specifically, for $n = 2t^2 + kt + h$, we get the classes where

$$\begin{aligned}(k,h) &= (2,1),(2,2),(2,3),(3,0),(3,1),(3,2),(3,3),\\ &\quad (4,1),(4,2),(4,3),(5,2),(5,3),(6,3).\end{aligned}$$

Du et al. then define closed segments of integers in $[0, n-1]$ in a certain way, and obtain some results based on properties of these segments. In particular, they derive the following.

Theorem 5.8 *Let $n = 2t^2 + kt + h$, where $1 \leq h \leq t$ and $2 \leq k \leq 6$, and let $G = C(n, \{1, 2t+(k-3)\})$. Then $d(G) = t+1 = LB(n)$ for the following circulants: $C(n, \{1, 2t+(k-3)\}$ with $(k,h) = (3,-1),(3,0),(3,1),(3,2),(4,1),(4,2),(4,3),(5,3),(5,4)$, and $(6,5)$.*

Note that the infinite classes of n with $(k,h) = (3,-1),(5,4)$, and $(6,5)$ were not picked up by Theorem 5.7.

In [17], Du et al. also determine some infinite classes of n for which the lower bound diameter cannot be achieved. In particular, they obtained the following result.

Theorem 5.9 *Let $n = 2t^2+6t+4$. Then the circulant $G = C(n, \{1, 2t+3\})$ has the optimal diameter $d(G) = t+2 = d(n)$.*

Note that for values of n satisfying the statement of Theorem 5.9, $\mathrm{LB}(n) = t+1$, so we have $d(n) = \mathrm{LB}(n) + 1$.

In [23], Hsu and Shapiro introduce the concept of *one-optimality*, which is defined as follows. Given two positive integers n and s, $s < n$, there exists a unique pair q and r of non-negative integers such that $n = qs+r$ and $0 \leq r < s$. Now for any vertex labelled v in $C(n, \{1, s\})$, define

(a) $d(v) = \min\{|i| + |j| : v = i \cdot s + j \cdot 1 \pmod{n}\}$, and

(b) $d_1(v) = \min\{|i| + |j| : v = i \cdot s + j \cdot 1 \pmod{n} \text{ and } |i| \leq q\}$.

For $G = C(n, \{1, s\})$, we have $d(G) = \max\{d(v) : v \in V(G)\}$. Let $d_1(G) = \max\{d_1(v) : v \in V(G)\}$. Then the circulant $G = C(n, \{1, s\})$ is said to be *one-optimal* if $d_1(G) = d(n)$, the optimal diameter. It turns out that $d(n) \leq d(G) \leq d_1(G)$, hence one-optimality is a stronger concept than that of optimality.

Hsu and Shapiro [22] make use of the concept of one-optimality to obtain the following result, which gives an upper bound for the minimum diameter.

Theorem 5.10 *For any positive integer n, let $d(G)$ be the diameter of the circulant $G = C(n, \{1, s\})$, where $1 < s < (n+1)/2$. Let $d(n) = min\{d(G) : 1 < s < (n+1)/2\}$. Then $d(n) \leq (n/2)^{1/2} + (n/8)^{1/4} + 2$.*

Bibliography

[1] D. Bauer, F. Boesch, C. Suffel, and R. Tindell, Connectivity Extremal Problems and the Design of Reliable Probabilistic Networks. *The Theory and Applications of Graphs* (G. Chartrand, Y. Alavi, D. Goldsmith, L. Lesniak-Foster, and D. Lick, Eds.) Wiley, New York (1981) 45–54.

[2] J.L. Berggren, An Algebraic Characterization of Symmetric Graphs with a Prime Number of Vertices. *Bull. Austral. Math. Soc.* **7** (1972) 131–134.

[3] J.C. Bermond, O. Favaron, and M. Maheo, Hamiltonian Decomposition of Cayley Graphs of Degree 4. *J. Combinatorial Theory B* **46** (1989) 142–153.

[4] F. Boesch and R. Tindell, Circulants and Their Connectivities. *J. Graph Theory* **8** (1984) 487–499.

[5] F. Boesch and R. Tindell, Connectivity and Symmetry in Graphs. *Graphs and Applications—Proc. First Colorado Symp. Graph Theory* (F. Harary and J. Maybee, Eds.) Wiley (1985) 53–67

[6] F.T. Boesch, Synthesis of Reliable Networks—A Survey. *IEEE Trans. Reliability* **R-35** (1986) 240–246.

[7] F.T. Boesch, On Unreliability Polynomials and Graph Connectivity in Reliable Network Synthesis. *J. Graph Theory* **10** (1986) 339–352.

[8] F.T. Boesch and A.P. Felzer, A General Class of Invulnerable Graphs. *Networks* **2** (1972) 261–283.

[9] F.T. Boesch and A.P. Felzer, On the Invulnerability of the Regular Complete k-partite Graphs. *SIAM J. Appl. Math.* **20** (1971) 176–182.

[10] F.T. Boesch and R.E. Thomas, On Graphs of Invulnerable Communication Nets. *IEEE Trans. Circuit Theory* **17** (1971) 183–192.

[11] F.T. Boesch and J.F. Wang, Reliable Circulant Networks with Minimum Transmission Delay. *IEEE Trans. Circuits and Systems* **Cas-32** (1985) 1286–1291.

[12] F.T. Boesch and J.F. Wang, Super Line-Connectivity Properties of Circulant Graphs. *SIAM J. Algebraic and Discrete Methods* **7** (1986) 89–98.

[13] B. Bollobás, A Problem of the Theory of Communication Networks. *Acta Mathematica (Hungary)* **19** (1968) 75–80.

[14] J.A. Bondy and U.S.R. Murty, *Graph Theory with Applications.* North-Holland, New York, NY (1982).

[15] C.Y. Chao, On the Classification of Symmetric Graphs with a Prime Number of Vertices. *Trans. Amer. Math. Soc.* **158** (1971) 247–256.

[16] N. Deo and M.S. Krishnamoorthy, Toeplitz Networks and Their Properties. *IEEE Trans. Circ. Sys.* **36** (1989) 1089–1092.

[17] D.Z. Du, D.F. Hsu, Q. Li, J. Xu, A Combinatorial Problem Related to Distributed Loop Networks. *Networks* **20** (1990) 173–180.

[18] Y.O. Hamidoune, On the Connectivity of Cayley Digraphs. *Europ. J. Combinatorics* **5** (1984) 309–312.

[19] F. Harary, The Maximum Connectivity of a Graph. *Proc. Natl. Acad. Sci. USA* **48** (1962) 1142–1146.

[20] F. Harary, *Graph Theory.* Addison-Wesley, Reading, MA (1969).

[21] D.F. Hsu and X. Jia, Extremal Problems in the Construction of Distributed Loop Networks, Preprint.

[22] D.F. Hsu and J. Shapiro, Bounds for the Minimal Number of Transmission Delays In Double Loop Networks, Preprint.

[23] D.F. Hsu and J. Shapiro, A Census of Tight One-Optimal Double Loop Networks, Preprint.

[24] F.T. Leighton, Circulants and the Characterization of Vertex-Transitive Graphs. *J. Res. Natl. Bur. Stand.* **88** (1983) 395–402.

[25] W. Mader, Über den Zusammenhäng symmetrischer Graphen. *Arch. Math. (Basel)* **21** (1970) 331–336.

[26] W. Mader, Minimale n-fach zusammenhangende Graphen mit maximaler kantenzahl. *J. Reine Angew. Math.* **249** (1971) 201–207.

[27] W. Mader, Eine Eigenschaft der Atome endlicher Graphen. *Arch. Math. (Basel)* **22** (1971) 333–336.

[28] W. Mader, Minimale n-fach kantenzusammenhängende Graphen. *Math. Ann.* **191** (1971) 21–28.

[29] G. Sabidussi, The Composition of Graphs. *Duke Math. J.* **26** (1959) 693–696.

[30] R. Tindell, The Connectivities of a Graph and its Complement. *Ann. Discrete Math.* **13** (1982) 191–202.

[31] J. Turner, Point-Symmetric Graphs with a Prime Number of Points.
J. Combinatorial Theory **3** (1967) 136–145.

[32] J.F. Wang, An Investigation of the Network Reliability Properties of Circulant Graphs. Doctoral dissertation, Stevens Institute of Technology (1983).

[33] M.E. Watkins, Some Classes of Hypoconnected Vertex-transitive Graphs. *Recent Progress in Combinatorics—Proc. Third Water-*

loo Conf. on Combinatorics (W.T. Tutte and C.St.J.A. Nash-Williams, Eds.) Academic Press, New York, (1969) 323–328.

[34] M.E. Watkins, Connectivity of Transitive Graphs. *J. Combinatorial Theory* **8** (1970) 23–29.

[35] M.E. Watkins, Computing the Connectivity of Circulant Graphs. *Congressus Numer.* **49** (1985) 247–258.

[36] H. Whitney, Congruent Graphs and the Connectivity of Graphs. *Amer. J. Math.* **54** (1932) 150–168.

[37] R.S. Wilkov, Analysis and Design of Reliable Computer Networks. *IEEE Trans. Commun.* **20** (1972) 660–678.

[38] Wong, Coppersmith, A Combinatorial Problem Related to Multimodule Memory Organization. *J. Assoc. Comp. Mach.* **21** (1974) 392–402.

[39] J.L.A. Yebra, M.A. Fiol, P. Morillo, and I. Alegre, The Diameter of Undirected Graphs Associated to Plane Tessellations. *Ars Combinatoria* **20-B** (1985) 159–171.