Primitive Digraphs with Smallest Large Exponent

by

Shahla Nasserasr
B.Sc., University of Tabriz, Iran 1999

A Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

in the Department of Mathematics and Statistics

Primitive Digraphs With Smallest Large Exponent

by

Shahla Nasserasr

Supervisory Committee

Dr. Dale Olesky, (Department of Computer Science)
Supervisor

Dr. Pauline van den Driessche, (Department of Mathematics and Statistics)
Supervisor

Dr. Gary MacGillivray, (Department of Mathematics and Statistics)
Departmental Member

Dr. Denis Hanson, (Department of Mathematics and Statistics, University of Regina)
External Examiner

Supervisory Committee

Dr. Dale Olesky, (Department of Computer Science)
Supervisor

Dr. Pauline van den Driessche, (Department of Mathematics and Statistics)
Supervisor

Dr. Gary MacGillivray, (Department of Mathematics and Statistics)
Departmental Member

Dr. Denis Hanson, (Department of Mathematics and Statistics, University of Regina)
External Examiner

Abstract

A primitive digraph D on n vertices has large exponent if its exponent, $\gamma(D)$, satisfies $\alpha_n \leq \gamma(D) \leq w_n$, where $\alpha_n = \lfloor w_n/2 \rfloor + 2$ and $w_n = (n-1)^2+1$. It is shown that the minimum number of arcs in a primitive digraph D on $n \geq 5$ vertices with exponent equal to α_n is either $n+1$ or $n+2$. Explicit constructions are given for fixed n even and odd for a primitive digraph on n vertices with exponent α_n and $n+2$ arcs. These constructions extend to digraphs with some exponents between α_n and w_n. A necessary and sufficient condition is presented for the existence of a primitive digraph on n vertices with exponent α_n and $n+1$ arcs. For fixed n, an algorithm is given that determines whether the minimum number of arcs in such a digraph is $n+1$ or $n+2$.

Contents

List of Figures

Acknowledgements

I would like to thank my co-supervisors Dr. Dale Olesky and Dr. Pauline van den Driessche for their extreme patience and valuable guidance over the past two years. It has been an honour to work with you.

Many special thanks to Dr. Gary MacGillivray for all his help in my studies and thesis, his support and friendship. My life in Victoria was full of happiness and great experiences mostly because of having Gary and his wife Christi as brother and sister. Thank you to both of you.

Thank you to Dr. Denis Hanson, my external examiner, for his careful reading of my thesis and advice.

My deepest thanks to my family who always supported and encouraged me. In particular many thanks to my brother Reza who is always helpful in any case.

Shahla Nasserasr

Chapter 1

Introduction

1.1 Motivation

The correspondence between directed graphs and matrices has resulted in strong connections between some recent research in two major branches of mathematics, namely graph theory and linear algebra. One particular instance of this concerns the representation of a digraph by its adjacency matrix, which is a square matrix with entries from $\{0, 1\}$. The eigenvalues of an adjacency matrix determine some of the important properties of both the matrix and its associated digraph.

For an irreducible nonnegative matrix A, the eigenvalue of maximum modulus and its eigenvector are characterized in the following results of Perron and Frobenius; see [7].

1. The spectral radius $\rho(A) > 0$ is an eigenvalue, and is greater than or

equal to the modulus of any other eigenvalue.

2. There is a positive eigenvector corresponding to $\rho(A)$.

3. $\rho(A)$ is a simple root of the characteristic equation of A.

A nonnegative, irreducible matrix can have more than one eigenvalue with maximum modulus, in which case, for example, $\lim_{i\to\infty}[\frac{1}{\rho(A)}A]^i$ may not exist. The restriction of the class of nonnegative, irreducible matrices to those for which there is only one eigenvalue of maximum modulus and for which $\lim_{i\to\infty}[\frac{1}{\rho(A)}A]^i$ exists, gives the class of primitive matrices.

If A is an n by n nonnegative primitive matrix, then $\rho(A)$ is positive and greater in modulus than any other eigenvalue; see [7]. Primitive matrices have also been characterized as those square, nonnegative matrices A for which A^m is a positive matrix for some $m \geq 1$. The smallest such positive integer m is called the exponent of A, and we denote this by $\gamma(A)$. For further information on primitive matrices, the reader is referred to the book by Horn and Johnson [7].

A digraph D is primitive if and only if its adjacency matrix A is primitive, and in this case $\gamma(D(A)) = \gamma(A)$. For given n, the smallest upper bound for the exponent of a primitive digraph on n vertices, denoted by w_n, is attributed to Wielandt (see [18] and [16]). This thesis is primarily concerned with primitive digraphs having exponent approximately $w_n/2$ or greater. Such digraphs have only two different cycle lengths, and are referred to as primitive digraphs with large exponent.

The specific focus of this thesis is the minimum number of arcs in a

primitive digraph (on a given number of vertices) having the smallest large exponent. The addition of an arc to a primitive digraph cannot increase the exponent. Thus, it is interesting that, for a given number of vertices n, the unique (up to isomorphism) primitive digraph with maximum large exponent w_n, and primitive digraphs with smallest large exponent can have the same number of arcs, namely $n+1$. This fact will be shown in this thesis.

Section 1.2 provides some of the definitions and previous work relevant to this thesis. Other definitions and notation specific to a particular section are provided as needed. Section 1.3 provides an overview of what follows in each of the remaining chapters.

1.2 Definitions and Previous Work

In this section, primitive digraphs are defined and characterized and primitive digraphs with large exponent, which are the focus of this thesis, are defined.

Definition 1.2.1 *A digraph D is primitive if and only if there exists a positive integer m such that for all ordered pairs of vertices (u, v) (not necessarily distinct), there is a walk of length m from u to v. The smallest such m is called the exponent of D, and is denoted by $\gamma(D)$.*

The following result gives another characterization of primitive digraphs, which is due to Romanovsky and is used in some of our proofs; see [7, p. 517].

Theorem 1.2.2 *A digraph D is primitive if and only if it is strongly connected and the greatest common divisor of its cycle lengths equals 1.*

The *Wielandt digraph* W_n on $n \geq 3$ vertices consists the Hamilton cycle plus an additional arc that makes an $(n-1)$-cycle. The following upper bound was found by Wielandt; see [18].

Theorem 1.2.3 *If D is a primitive digraph on $n \geq 3$ vertices, then*

$$\gamma(D) \leq (n-1)^2 + 1.$$

Equality holds if and only if D is the Wielandt digraph W_n.

Thus $(n-1)^2+1$ is the smallest upper bound for the exponent of a primitive digraph on n vertices; this value is denoted by w_n.

Definition 1.2.4 [10] *A primitive digraph on $n \geq 3$ vertices with exponent $\gamma(D)$ is called a primitive digraph with large exponent if*

$$\lfloor \tfrac{w_n}{2} \rfloor + 2 \leq \gamma(D) \leq w_n.$$

Therefore, $\lfloor \frac{w_n}{2} \rfloor + 2$ is the smallest large exponent; we denote this value by α_n.

An important property of a primitive digraph with large exponent is the following result, which is frequently used in the results of this thesis; see [12].

Theorem 1.2.5 *Let D be a primitive digraph with large exponent. Then D has cycles of exactly two different lengths.*

When it is clear from the context, the cycle lengths of a primitive digraph on n vertices with large exponent are denoted by k and j with $k > j$. By Theorem 1.2.2, k and j must be relatively prime. It is clear that $k \leq n$. A lower bound for the length of the smallest cycle in a primitive digraph D with large exponent is given in [10, Theorem 1], namely $\lceil \frac{n-1}{2} \rceil \leq j$. In [11, Theorem 1.2] it was shown that a primitive digraph D on n vertices with cycle lengths k and j, $k > j$, has large exponent if and only if $j(k-2) \geq \lfloor \frac{w_n}{2} \rfloor + 2 - n$.

In the remainder of this section, some results that are concerned with arbitrary exponents of primitive digraphs and primitive graphs are presented. Rosiak [15] considered the problem of estimating the minimum exponent over all primitive digraphs on n vertices with a fixed number of arcs and girth (the length of the shortest cycle). When the number of arcs is $n+1$, this minimum exponent is equal to $n + s(s-1)$, where s is the girth [15, Theorem 6]. Note that Rosiak's problem is not restricted to primitive digraphs with large exponent.

Primitivity of a simple graph and its exponent can be defined as for a digraph. It is clear that a graph G is primitive if and only if G is connected and has at least one odd cycle; that is, G is a connected nonbipartite graph. It was shown in [13] that for $n \geq 5$ the exponent set of a primitive graph on n vertices is $\{2, 3, \ldots, 2n-4\} \backslash S$, where S is the set of all odd numbers in $\{n-2, n-1, \ldots, 2n-5\}$. Recently Kim, Song and Hwang [9] have determined the minimum number of edges in a primitive graph on n vertices with given possible exponent γ. From [8], this minimum number of edges is equal to

$\lfloor \frac{3n-2}{2} \rfloor$ for $\gamma = 2$; and from [9], this minimum is $\lfloor \frac{3n-3}{2} \rfloor$ for $\gamma = 3$; n for even γ satisfying $4 \leq \gamma \leq 2n-4$; and $n+1$ for odd γ satisfying $5 \leq \gamma \leq n-3$.

1.3 An Overview

As stated in Section 1.1, the main question in this thesis is to find the minimum number of arcs in a primitive digraph on n vertices with smallest large exponent, α_n. Chapter 2 gives the answer to this question for a small number of vertices $n \in \{3, 4, 5, 6\}$. Chapter 3 describes a family of primitive digraphs with $n+1$ arcs that can have large exponent. The exponent of these digraphs is found in terms of the number of vertices and cycle lengths. Chapter 4 explicitly gives primitive digraphs on n vertices for n even and n odd with $n+2$ arcs and exponent α_n. Chapter 5 answers the main question in this thesis by using some number theoretic results. Separate cases for n even and n odd are considered. Finally, Chapter 6 contains an algorithm that determines for a given n the minimum number of arcs (either $n+1$ or $n+2$) in a primitive digraph on n vertices with exponent α_n. Conclusions and some open problems are given in Chapter 7. In Appendix A all primitive digraphs on 5 vertices with large exponent and cycle lengths 4 and 3 are discussed to complete the answer to the question for $n = 5$ as given in Chapter 2. Appendix B contains a list of n, k, j for which there exists a primitive digraph $W(n, k, j)$ with exponent α_n. These lists are ordered by n for even $n \leq 1264$ and odd $n \leq 1551$.

Chapter 2

Primitive digraphs on 3 to 6 vertices

In this chapter, we characterize all primitive digraphs (up to isomorphism) on $3, 4$ and 5 vertices with exponent equal to α_n. It is shown that the minimum number of arcs in a primitive digraph on 3 or 5 vertices with the smallest large exponent is 4 or 7, respectively. However, there is no primitive digraph on 4 vertices with exponent equal to α_4. For $n = 6$, a primitive digraph with exponent equal to α_6 and having $7 = n + 1$ arcs is given.

Suppose that $n = 3$. All digraphs on $n = 3$ vertices with large exponent are listed in [4, Example 1.4]. From this it follows that the minimum number of arcs in a primitive digraph on $n = 3$ vertices with exponent $\alpha_3 = 4$ is equal to $4 = n + 1$, and such a digraph has cycle lengths $k = 3$ and $j = 1$. The maximum number of arcs in a primitive digraph on $n = 3$ vertices is

$5 = n + 2$; there are two such digraphs having exponent α_3, one with cycle lengths $k = 3$ and $j = 2$ and the other one with cycle lengths $k = 2$ and $j = 1$.

Suppose that $n = 4$. If $k = 3$ and $j = 2$, then $j(k-2) = 2 < \alpha_4 - 4 = 7 - 4 = 3$; thus by [11, Theorem 1.2] there is no such primitive digraph with large exponent. Similarly $k = 2,\ 3$ or 4 and $j = 1$ do not allow a primitive digraph with large exponent. Thus the only possibility for k and j in a primitive digraph on 4 vertices with large exponent is $k = 4$ and $j = 3$. By [11, Theorem 2.2] any primitive digraph with large exponent on $n = 4$ vertices such that $k = n = 4$ and $j = 3$ is isomorphic to one of the primitive digraphs in Figure 2.1. But the first digraph in Figure 2.1 has exponent $9 \neq \alpha_4$, and the second digraph in Figure 2.1 is the Wielandt digraph on 4 vertices, so its exponent is equal to $(4-1)^2 + 1 = 10$. Thus, there is no primitive digraph on 4 vertices with exponent $\alpha_4 = 7$.

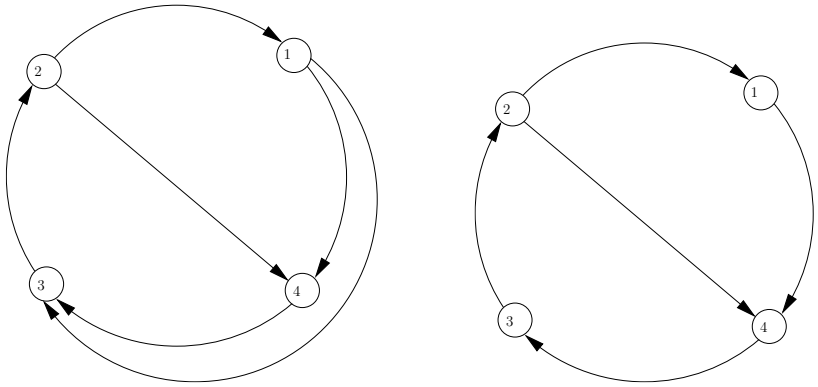

Figure 2.1: Primitive digraphs on 4 vertices with large exponent

Suppose that $n = 5$. By [11, Theorem 1.2], the possible values for k and j in a primitive digraph with large exponent on 5 vertices are $k = 5$ and $j = 4, 3, 2$ or $k = 4$ and $j = 3$. In the case $n = k = 5$ and $j = 4, 3, 2$, using [11, Theorems 2.2 and 2.3] the only digraph with exponent $\alpha_5 = 10$ is a 5-cycle with two 2-cycles, which has $7 = n + 2$ arcs (see Theorem 4.0.2 on page 21). In the case $k = 4$ and $j = 3$, the results in Appendix A imply that the primitive digraphs on 5 vertices with exponent α_5 have either $7 = n + 2$ arcs or $8 = n+3$ arcs. Therefore, the minimum number of arcs in a primitive digraph on 5 vertices with exponent $\alpha_5 = 10$ is $7 = n+2$, and the maximum number of arcs in such a digraph is $8 = n + 3$.

Suppose that $n = 6$. The digraph in Figure 2.2 has exponent $\alpha_6 = 15$ and $n+1 = 7$ arcs. This digraph is called $W(6, 5, 3)$ and such digraphs $W(n, k, j)$ are introduced later in Chapter 3.

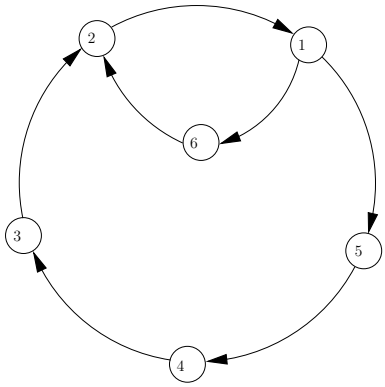

Figure 2.2: A primitive digraph on 6 vertices with exponent $\alpha_6 = 15$

Chapter 3

Digraphs $W(n, k, j)$

The aim of this chapter is to show that there is only one family of primitive digraphs on n vertices with large exponent and $n+1$ arcs. A digraph from this family with cycle lengths k and j is denoted by $W(n, k, j)$; see [11, proof of Theorem 1.2], [3, p. 44] and Definition 3.0.2 below.

Proposition 3.0.1 *If a strongly connected digraph D on $n \geq 2$ vertices has exactly one c_1-cycle, exactly one c_2-cycle with $1 \leq c_2 \leq c_1 \leq n$ and no other cycles, then the number of arcs in D is $n+1$.*

Proof. Suppose that digraph D on n vertices consists of exactly one c_1-cycle and exactly one c_2-cycle. Since D is strongly connected, the cycles intersect each other, say on p vertices and $p-1$ arcs where $1 \leq p \leq c_2$. Then the number of vertices in D is $n = c_1 + c_2 - p$ and the number of arcs is $c_1 + c_2 + 1 - p = n + 1$. ∎

Definition 3.0.2 [3, p. 44] *For $n \geq k > j \geq 2$, with $k + j \geq n + 2$ and $(k, j) = 1$, $W(n, k, j)$ denotes the primitive digraph on $n \geq 3$ vertices that consists of a k-cycle $1 \to k \to (k-1) \ldots \to 2 \to 1$ and a j-cycle containing the path $1 \to (k+1) \to (k+2) \to \ldots \to n \to (k+j-n)$ if $k \leq n-1$ or the arc $1 \to j$ if $k = n$.*

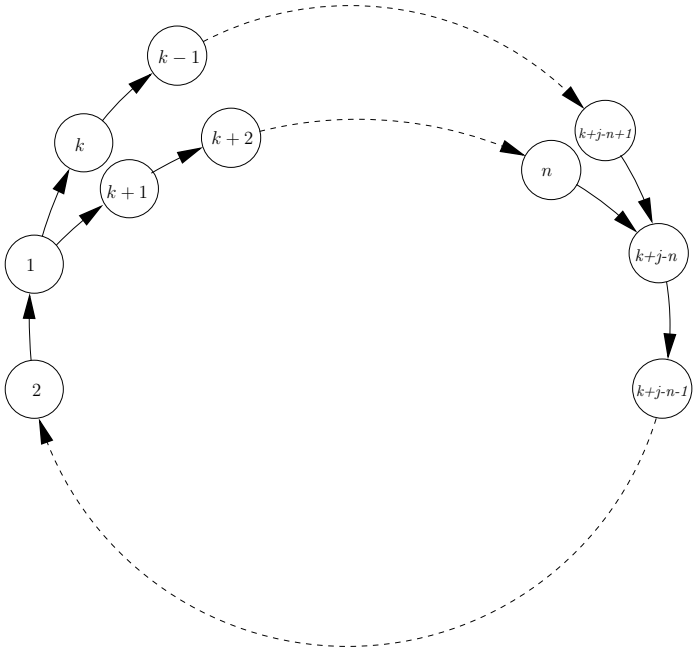

Figure 3.1: $W(n, k, j)$

Note that $W(n, k, j)$ is strongly connected and has only two cycles, which intersect on a path of length at least one; therefore by Proposition 3.0.1 it has $n + 1$ arcs. The condition $k + j \geq n + 2$ ensures that the cycles intersect in at least one arc. Figure 3.1 depicts $W(n, k, j)$, with n, k and j satisfying the conditions on Definition 3.0.2 with $k \leq n - 1$.

The following results in this chapter show that if there exists a primitive digraph on n vertices with large exponent and $n+1$ arcs, then it must be a digraph $W(n,k,j)$ for some k and j. Therefore the question of determining those n for which the minimum number of arcs in a primitive digraph on n vertices with exponent α_n is $n+1$ reduces to asking: for which n, k and j does there exist a digraph $W(n,k,j)$ with $\gamma(W(n,k,j)) = \alpha_n$?

We first show (in Corollary 3.0.4) that if $n \geq 4$, then we can restrict our consideration to digraphs with $k + j \geq n + 2$.

Proposition 3.0.3 *If D is a primitive digraph on n vertices with large exponent, exactly one k-cycle, exactly one j-cycle and $k + j = n + 1$, then $n = k = 3$ and $j = 1$.*

Proof. Suppose D is a primitive digraph on n vertices with large exponent and exactly two cycles of lengths k and j. Consider the following two cases for n.

(i) n is even:

By [11, Theorem 1.2],

$$\left\lfloor \frac{(n-1)^2+1}{2} \right\rfloor + 2 - n \quad \leq \quad (k-2)j.$$

Since n is even and $j = n + 1 - k$, this gives

$$2k^2 - 2(n+3)k + n^2 + 10 \leq 0. \tag{3.1}$$

Considering (3.1) as a quadratic equation in k, the discriminant is $\Delta = 4(n+3)^2 - 8(n^2+10) = 4(-n^2+6n-11)$, which is negative for all n. Therefore there are no real values of k for which (3.1) is satisfied, and it follows that there are no n, k and j satisfying (3.1).

(ii) n is odd:

A similar discussion to that for n even implies that k and n must satisfy

$$2k^2 - 2(n+3)k + n^2 + 9 \leq 0. \tag{3.2}$$

Considering (3.2) as a quadratic equation in k, the discriminant is $\Delta = 4(n+3)^2 - 8(n^2+9) = 4(-n^2+6n-9)$. Thus $\Delta \leq 0$ and the equality holds if and only if $n = 3$. Therefore (3.2) is satisfied only when $n = 3$, in which case $2k^2 - 12k + 18 \leq 0$ and thus $k = 3$. Since $k + j = n + 1$, it follows that $j = 1$. ∎

Corollary 3.0.4 *If D is a primitive digraph on $n \geq 4$ vertices with large exponent, then $k + j \geq n + 2$.*

Proof. By [10, Theorem 1], $j \geq \lceil \frac{n-1}{2} \rceil$. Consider the following two cases.

(i) If $j \geq \frac{n}{2}$, then since $n \geq k > j \geq \frac{n}{2}$, it follows that $k + j \geq n + 1$.

(ii) If $j = \frac{n-1}{2}$, then by [11, Theorem 1.2] $k = n$, thus $k + j = n + \frac{n-1}{2} \geq n + 1$.

In both cases $k + j \geq n + 1$, so for $n \geq 4$, by Proposition 3.0.3 it follows that $k + j \geq n + 2$. ∎

In the next two results, restrictions on the number and the length of cycles in certain primitive digraphs are proved.

Proposition 3.0.5 *If D is a primitive digraph on $n \geq 4$ vertices with large exponent and $n+1$ arcs, then it has exactly two cycles, the intersection of which is a path of length at least one.*

Proof. Suppose that D is a primitive digraph with vertex set V. Then $\sum_{v \in V} deg^+ v = e$, where $deg^+ v$ is the outdegree of vertex v and e is the number of arcs in D. Thus by assumption $\sum_{v \in V} deg^+ v = n+1$. Now, since D is strongly connected, every vertex has outdegree at least 1, which implies that exactly one of the vertices has outdegree 2 and the remaining vertices have outdegree 1. The same argument is true for the indegree of the vertices. It follows that the only possible such digraphs are those with exactly two cycles that intersect in a vertex, or those with exactly two cycles that intersect in a path of length at least 1. The digraph in the former case has $k+j = n+1$, so by Corollary 3.0.4 it cannot have large exponent. Therefore, digraph D consists of exactly two cycles that intersect in a path of length at least 1. ∎

Proposition 3.0.6 (a) *A primitive digraph on $n \geq 4$ vertices with large exponent has no 1-cycles.*

(b) *A primitive digraph on $n = 4$ or $n \geq 6$ vertices with large exponent has no 2-cycles.*

Proof. The case (a) is a simple consequence of [10, Theorem 1], since $j \geq \lceil \frac{4-1}{2} \rceil = 2$. To prove (b), first suppose that $n = 4$. If $j = 2$ then k must be 3, in which case $j(k-2) = 2 < \alpha_4 - 4 = 7 - 4 = 3$, which contradicts [11, Theorem 1.2]. For $n \geq 6$, similarly to case (a), $j \geq \lceil \frac{6-1}{2} \rceil = 3$. Thus there is no 2-cycle in such a digraph. ∎

Now we are able to deduce that the digraphs in Definition 3.0.2 are the only possible digraphs with $n+1$ arcs and large exponent.

Proposition 3.0.7 *If a primitive digraph D on $n \geq 4$ vertices has large exponent and $n+1$ arcs, then it is isomorphic to a digraph $W(n,k,j)$ for some relatively prime k and j satisfying $n \geq k > j \geq 2$ and $k + j \geq n + 2$.*

Proof. If the primitive digraph D on $n \geq 4$ vertices has large exponent, then its cycle lengths k and j are relatively prime. By Proposition 3.0.6, it follows that $n \geq k > j \geq 2$, and Corollary 3.0.4 gives $k + j \geq n + 2$. If D has $n+1$ arcs, then by Proposition 3.0.5 it has only two cycles. Therefore, D is isomorphic to a digraph $W(n,k,j)$ for some k and j. ∎

The above results imply that the only possible primitive digraphs on $n \geq 4$ vertices with $n+1$ arcs and exponent α_n are digraphs $W(n,k,j)$. The following concepts are introduced in order to determine the exponent of some primitive digraphs.

If $c_1, c_2, \ldots, c_s$ are relatively prime, then the *Frobenius-Schur index*, denoted by $\phi(c_1, c_2, \ldots, c_s)$, is the smallest integer such that every integer

greater than or equal to $\phi(c_1, c_2, \ldots, c_s)$ can be written as $a_1c_1 + a_2c_2 + \ldots + a_sc_s$, where each a_ℓ is a nonnegative integer for $\ell = 1, 2, \ldots, s$. Frobenius was one of the first to consider the evaluation of this number; see [2, p. 72]. If $s = 2$, then $\phi(c_1, c_2) = (c_1 - 1)(c_2 - 1)$.

The following terminology and the results from Theorem 3.0.9 to Corollary 3.0.11 are taken from [5].

Let $\{c_1, c_2, \ldots, c_s\}$ be the set of all cycle lengths of a primitive digraph D. For any ordered pair (u, v) of vertices, a nonnegative integer $r_{u,v}$ is defined as follows. If $u = v$ and if for all $t = 1, 2, \ldots, s$ there is a cycle through vertex u of length c_t, then $r_{u,v} = 0$; otherwise $r_{u,v}$ is the length of a shortest walk from u to v that has at least one vertex on some cycle of length c_t for all $t = 1, 2, \ldots, s$. The *circumdiameter* of D is $r = max\{r_{u,v}\}$ taken over all ordered pairs (u, v).

An ordered pair (u, v) of vertices in a primitive digraph D has the *unique path property* if every walk from vertex u to vertex v that has length greater than or equal to $r_{u,v}$ consists of some walk $\mathcal{W}$ of length $r_{u,v}$ augmented by a number of cycles, each having a vertex in common with $\mathcal{W}$. (Note that the word 'unique' in this definition refers to the length of the walk $\mathcal{W}$ rather than to the walk $\mathcal{W}$ itself.)

Example 3.0.8 *Consider the primitive digraph in Figure 3.2 with cycle lengths $k \geq 3$ and $j = k - 1$. The ordered pair $(1, k - 1)$ does not have the unique path property, because the arc $(1, k - 1)$ meets both k and $k - 1$ cycles, so $r_{1,k-1} = 1$, but the path $1 \to k \to k - 1$ has length $2 > 1 = r_{1,k-1}$*

and cannot be written as $r_{1,k-1} + a_1k + a_2j = 1 + a_1k + a_2j$ *for some non-negative integers* a_1 *and* a_2*. The ordered pair* $(k, k-1)$ *does have the unique path property. Every walk from* k *to* $k-1$ *clearly has length* $1 + a_1k + a_2j$*.*

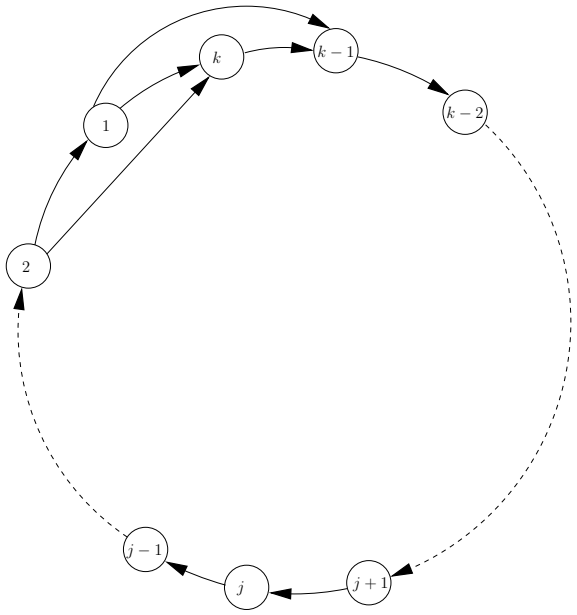

Figure 3.2: Digraph to illustrate the unique path property

Theorem 3.0.9 [5, Theorem 3] *If* D *is a primitive digraph with cycle lengths* $c_1, c_2, \ldots, c_s$ *and circumdiameter* r*, then* $\gamma(D) \leq \phi(c_1, c_2, \ldots, c_s) + r$*.*

Theorem 3.0.10 [5, Theorem 4] *If* D *is a primitive digraph with cycle lengths* $c_1, c_2, \ldots, c_s$ *in which the ordered pair of vertices* (u, v) *has the unique path property, then* $\gamma(D) \geq \phi(c_1, c_2, \ldots, c_s) + r_{u,v}$*.*

Corollary 3.0.11 [5, Corollary 2] *If, in Theorem 3.0.10,* $r_{u,v}$ *is equal to the circumdiameter* r*, then* $\gamma(D) = \phi(c_1, c_2, \ldots, c_s) + r$*.*

Thus, if a primitive digraph D with large exponent and with cycle lengths k and j has an ordered pair of vertices (u, v) with the unique path property and with $r_{u,v} = r$, then $\gamma(D) = (k-1)(j-1) + r$.

The following result, which is also proved in [3, Theorem 4.3.1], gives the exponent of a digraph $W(n, k, j)$.

Theorem 3.0.12 *For integers $n \geq k > j \geq 2$ with $k + j \geq n + 2$ and k and j relatively prime, $\gamma(W(n, k, j)) = n + (k-2)j$.*

Proof. Consider the digraph $W(n, k, j)$ in Figure 3.1. The ordered pair $(u, v) = (k, k+j-n+1)$ has the unique path property with $r_{u,v} = n-j-1+k$, and it can be easily verified that $r_{u,v} = r$. Therefore $\gamma(W(n, k, j)) = (k-1)(j-1) + n - j - 1 + k = n + (k-2)j$. ∎

By Theorem 3.0.12 and results of Chapter 2 for $n = 3, 4, 5, 6$, the problem of determining those n for which the minimum number of arcs in a primitive digraph D on n vertices with exponent α_n is equal to $n+1$ can be reduced to the following: for $n \geq 7$, determine those n, k and j with $n \geq k > j \geq \lceil \frac{n-1}{2} \rceil$, $(k, j) = 1$ and $k + j \geq n + 2$ so that

$$\alpha_n = \left\lfloor \frac{(n-1)^2 + 1}{2} \right\rfloor + 2 = n + (k-2)j. \tag{3.3}$$

Chapter 4

Digraphs with $n+2$ arcs

In this chapter, it is shown that for any $n \geq 8$, there exists a primitive digraph on n vertices with exponent α_n that has $n+2$ arcs. The primitive digraphs for the cases n even and odd are different, so we consider these two cases separately.

We first show that for even $n \geq 8$, there exists a primitive digraph with the smallest large exponent α_n and with $n+2$ arcs.

Theorem 4.0.1 *For any even $n \geq 8$, there exists a primitive digraph D on n vertices with cycle lengths $k = n-1$ and $j = n/2$ and $n+2$ arcs for which $\gamma(D) = \alpha_n$.*

Proof. Consider the primitive digraph D in Figure 4.1 with an $(n-1)$-cycle $1 \to n-1 \to \ldots \to 2 \to 1$ and the arcs $\frac{n}{2} - 3 \to n-4$, $1 \to n$ and $n \to \frac{n}{2} - 1$ that make two j-cycles. Thus D has n vertices and $n+2$ arcs.

The ordered pair of vertices $(n-1, n-3)$ has the unique path property with $r_{n-1,n-3} = 2+n-1 = n+1$. Since $r_{u,v} \leq r_{n-1,n-3}$ for any other ordered pair (u, v), it follows from Corollary 3.0.11 that $\gamma(D) = (k-1)(j-1)+r_{n-1,n-3} = (n-2)(\frac{n}{2}-1)+n+1 = \frac{n^2-2n+6}{2} = \alpha_n$. ∎

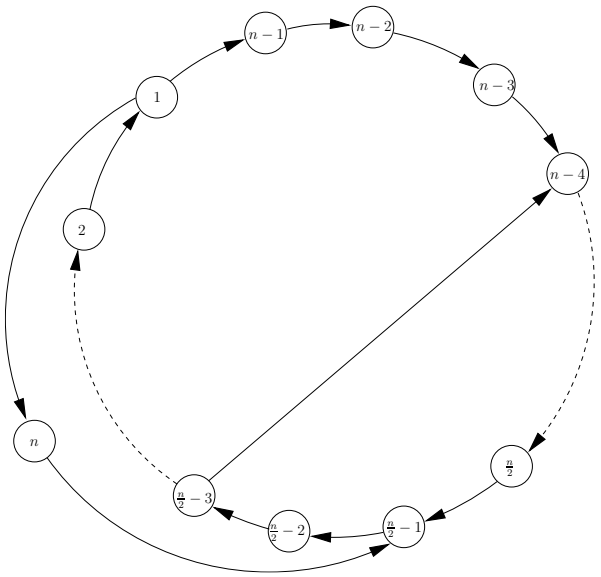

Figure 4.1: Digraph D with $n+2$ arcs and $\gamma(D) = \alpha_n$ for n even

No arc can be removed from the digraph D in Figure 4.1 to give a primitive digraph with exponent equal to α_n. By deleting the arc $n/2-3 \to n-4$, the maximum distance between vertices that have the unique path property increases, thus $\gamma(D) > \alpha_n$. If any other arc is deleted, then the resulting digraph is not strongly connected. Therefore, for even $n \geq 8$ (and in fact from Chapter 2 for even $n \geq 6$), the minimum number of arcs in a digraph with exponent equal to α_n is less than or equal to $n+2$. The digraph in

Figure 4.1 is a subdigraph of the digraph described in [11, Theorem 3.4 (b)].

Note that this result does not hold for $n = 6$, since there is no vertex with label $n/2 - 3 = 0$. For $n = 6$, the digraph $W(6, 5, 3)$ is a primitive digraph on 6 vertices with exponent equal to α_6; this digraph has $n + 1 = 7$ arcs (see Figure 2.2).

An analogous result to Theorem 4.0.1 for odd n is now presented. The case $n = 5$ is also given in Chapter 2.

Theorem 4.0.2 *For any odd $n \geq 5$, there exists a primitive digraph D on n vertices with cycle lengths $k = n$ and $j = \frac{n-1}{2}$ that has $n + 2$ arcs and for which $\gamma(D) = \alpha_n$.*

Proof. Consider the digraph D in Figure 4.2 with the Hamilton cycle $1 \to n \to n-1 \to \ldots \to 2 \to 1$ and the arcs $1 \to j$ and $j \to n-2$ that make j-cycles. Thus D has n vertices and $n + 2$ arcs. The ordered pair $(n, n-1)$ has the unique path property with $r_{n,n-1} = n + 1$. Since $r_{i,j} \leq r_{n,n-1}$ for any other ordered pair (i, j), it follows from Corollary 3.0.11 that $\gamma(D) = (k-1)(j-1) + r_{n,n-1} = (n-1)(\frac{n-1}{2} - 1) + n + 1 = \frac{(n-1)^2}{2} + 2 = \alpha_n$. ∎

Note that no arc can be removed from D to give a primitive digraph with exponent equal to α_n. By deleting any chord, the maximum distance between vertices that have the unique path property increases, thus $\gamma(D) > \alpha_n$. If any arc in the Hamilton cycle is deleted, then the resulting digraph is not strongly connected. Therefore, for odd $n \geq 5$, the minimum number of arcs in a digraph with exponent equal to α_n is less than or equal to $n + 2$.

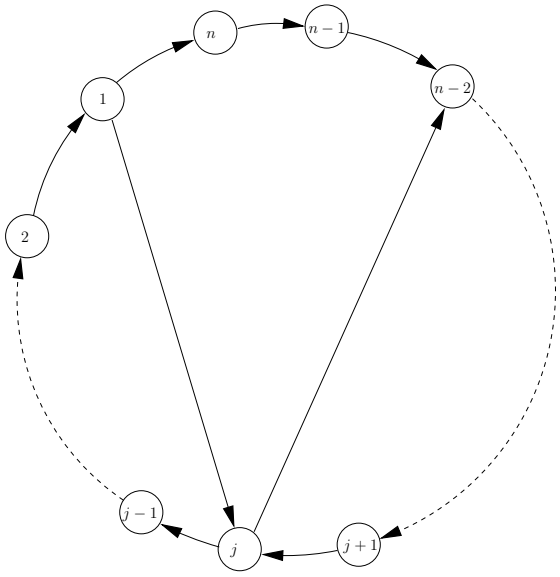

Figure 4.2: Digraph D with $n + 2$ arcs and $\gamma(D) = \alpha_n$ for n odd

The digraph in Figure 4.2 is an instance of the digraph described in [11, Theorem 2.3].

Chapter 5

Digraphs with $n+1$ arcs

5.1 Main Result

In this section, necessary and sufficient conditions for the existence of a primitive digraph D on n vertices with exponent $\gamma(D) = \alpha_n$ and $n+1$ arcs are proved.

Theorem 5.1.1 *Let D be a primitive digraph on $n \geq 5$ vertices with $\gamma(D) = \alpha_n$ and cycle lengths k, j. The minimum number of arcs in D is $n+1$ if and only if there exist positive integers x, y, t satisfying*

$$x^2 + y^2 = \begin{cases} (x+t)^2 - 2, & \text{if } n \text{ is even} \\ (x+t)^2 - 1, & \text{if } n \text{ is odd} \end{cases} \tag{5.1}$$

where $n = 2x + y + t + 2$, $k = n - y$, $j = n - x - 2$ with $(k, j) = 1$ and $\lceil \frac{n-1}{2} \rceil \leq j < k \leq n$. If no such solution exists, then the minimum number of

arcs in D is $n+2$.

Proof. Suppose that the minimum number of arcs in D is $n+1$ with $n \geq 5$. By Proposition 3.0.7, digraph D is isomorphic to a digraph $W(n,k,j)$ with $(k,j) = 1$ and $\lceil \frac{n-1}{2} \rceil \leq j < k \leq n$; for the lower bound on j, see [10, Theorem 1]. Since by Theorem 3.0.12, $\gamma(W(n,k,j)) = n + (k-2)j$ and $\alpha_n = \lfloor \frac{(n-1)^2+1}{2} \rfloor + 2$, it follows that

$$\left\lfloor \frac{(n-1)^2+1}{2} \right\rfloor + 2 = n + (k-2)j. \tag{5.2}$$

Let $k = n-h$ and $j = n-i$ for integers i and h with $i > h \geq 0$. We consider respectively the cases n is even and n is odd.

(**i**) Suppose n is even. Then from (5.2)

$$\frac{(n-1)^2+1}{2} + 2 = n + (n-h-2)(n-i) \Leftrightarrow n^2 - 2(i+h)n + 4i + 2ih - 6 = 0 \tag{5.3}$$

which is a quadratic equation in n. Since (5.3) has an integer solution, there exists a positive integer z such that

$$(i+h)^2 - 4i + 6 - 2ih = i^2 + h^2 - 4i + 6 = (i-2)^2 + h^2 + 2 = z^2.$$

Denoting $x = i - 2 = n - j - 2$ and $y = h = n - k \geq 0$,

$$x^2 + y^2 = z^2 - 2. \tag{5.4}$$

The integers $x,\ y,\ z$ must satisfy $x \geq 1,\ y \geq 1,\ z \geq 2$, because $j \leq n-1$ and $x = n - j - 2$ imply that $x \geq -1$. If $x = -1$ then $j = n-1$, so $k = n$ giving the Wielandt digraph W_n, which has exponent w_n, thus $x \geq 0$. It is clear that $y \geq 0$ and $z \geq 2$. Now, if $x = 0$ or $y = 0$, then there are no integer solutions to (5.4). Thus $x,\ y,\ z$ are all positive integers.

(**ii**) Suppose n is odd. Then from (5.2)

$$\frac{(n-1)^2}{2} + 2 = n + (n-h-2)(n-i) \Leftrightarrow n^2 - 2(i+h)n + 4i + 2ih - 5 = 0, \quad (5.5)$$

which is a quadratic equation in n. Since (5.5) has an integer solution, there exists a positive integer z such that

$$(i+h)^2 - 4i + 5 - 2ih = i^2 + h^2 - 4i + 5 = (i-2)^2 + h^2 + 1 = z^2.$$

With x and y as in case (**i**),

$$x^2 + y^2 = z^2 - 1 \quad (5.6)$$

for some integers $x,\ y,\ z$ with $x \geq -1,\ y \geq 0,\ z \geq 1$. As in case (**i**), $x \neq -1$. If $x = 0$, then $y \geq 1$ gives no integer solutions for z. If $x = 0$, then $y = 0$ gives $z = 1$, implying that $i = 2$ and $h = 0$, which from (5.5) gives $n = 1$ or $n = 3 < 5$. Thus $x,\ y,\ z$ are all positive integers.

Clearly z is greater than x in (5.4) and (5.6), so letting $z = x+t$ for some positive integer t, the equations can be considered respectively as

$$x^2 + y^2 = (x+t)^2 - 2 \tag{5.7}$$

for n even and

$$x^2 + y^2 = (x+t)^2 - 1 \tag{5.8}$$

for n odd.

Therefore, in both cases by (5.7) and (5.8), $x,\ y$ and t satisfy (5.1) with $k = n-y$ and $j = n-x-2$. From (5.3) and (5.5), $n = i+h+z = 2x+y+t+2$. Note that the solution $n = i+h-z$ of (5.3) and (5.5) gives $t = 2-k < 0$, which is not feasible since $k > \lceil \frac{n-1}{2} \rceil$, thus $k \geq 3$ for $n \geq 5$.

For the converse, assume that there exist positive integers $x,\ y,\ t$ satisfying (5.1). First note that $k+j = 2n-x-y-2 = 3x+y+2t+2 = n+x+t \geq n+2$ (since x and t are both positive). We again consider respectively the cases n is even and n is odd, and show that $\gamma(W(n,k,j)) = \alpha_n$ in each case.

(**i**) Suppose n is even. Using (5.7) and n, k and j as in the statement of the theorem,

$$\begin{aligned} \gamma(W(n,k,j)) &= n + (k-2)j \\ &= 2x + y + t + 2x^2 + 2xy + tx + ty + y^2 + 4, \end{aligned}$$

and

$$\begin{aligned}\alpha_n &= \frac{(n-1)^2+1}{2}+2 \\ &= 2x+y+t+2x^2+2xy+tx+ty+y^2+4=\gamma(W(n,k,j)).\end{aligned}$$

(**ii**) Suppose n is odd. Using (5.8) and n, k and j as in the statement of the theorem,

$$\begin{aligned}\gamma(W(n,k,j)) &= n+(k-2)j \\ &= 2x+y+t+2x^2+2xy+tx+ty+y^2+3,\end{aligned}$$

and

$$\begin{aligned}\alpha_n &= \frac{(n-1)^2}{2}+2 \\ &= 2x+y+t+2x^2+2xy+tx+ty+y^2+3=\gamma(W(n,k,j)).\end{aligned}$$

Therefore, the above, together with the conditions on $n,\ k$ and j in the assumption, imply that there is a primitive digraph $W(n,k,j)$ with exponent $\gamma(W(n,k,j))=\alpha_n$ in both cases n even and n odd.

For $n=6$, the digraph $W(6,5,3)$ has exponent $\alpha_6=15$ and $n+1=7$ arcs; see Figure 2.2. By Theorems 4.0.1 and 4.0.2, for even $n\geq 8$ and odd $n\geq 5$, there exists a primitive digraph D on n vertices with $\gamma(D)=\alpha_n$ and $n+2$ arcs. Thus the last statement of the theorem is proved. ∎

5.1.1 Special Case: $t = 1$

For $t = 1$, an infinite family of solutions x, y for (5.1) exists for both n even and n odd, where n, k, j are as given in Theorem 5.1.1. In other words, there exists an infinite family of primitive digraphs on n vertices with exponent α_n and with $n + 1$ arcs for both n even and n odd. These families are now considered.

First consider the case n even. The following result shows that if $u \equiv 4 (\text{mod } 17)$, then $(k, j) \neq 1$, where $k = 4u^2 + 4u + 5$ and $j = 2u^2 + 4u + 3$.

Lemma 5.1.2 *If $u = 17q + 4$ with q a nonegative integer and*

$$d = (4u^2 + 4u + 5, 2u^2 + 4u + 3),$$

then $17|d$.

Proof. If $u = 17q + 4$ for some $q \in N \cup \{0\}$, then $k = 4u^2 + 4u + 5 = 17q' + 85 = 17q_1$ for some integer q_1, and $j = 2u^2 + 4u + 3 = 17q_2$ for some integer q_2. It follows that $d = (17q_1, 17q_2) = 17(q_1, q_2)$, which implies that $17|d$. ∎

Using the above lemma, the following theorem proves that for n even, there are infinitely many solutions to (5.1) when $t = 1$, and an infinite proper subset of these solutions generates a family of nonisomorphic primitive digraphs $W(n, k, j)$ with exponent α_n.

Theorem 5.1.3 *If $t = 1$, then $x = \frac{y^2+1}{2}$, $y = 2u + 1$ with u a nonnegative integer gives an infinite family of integer solutions to the equation $x^2 + y^2 = (x + t)^2 - 2$ where $n = 2x + y + t + 2 = 4u^2 + 6u + 6$ is even. For $u \not\equiv 4 (\text{mod } 17)$ an infinite sub-family of these solutions generates an infinite family of primitive digraphs $W(n, k, j)$ with exponent α_n, where $k = 4u^2 + 4u + 5$ and $j = 2u^2 + 4u + 3$.*

Proof. Consider (5.7) and let $t = 1$. Hence

$$x^2 + y^2 = (x + 1)^2 - 2 = x^2 + 2x + 1 - 2 \Rightarrow y^2 = 2x - 1.$$

Therefore, y is odd, so let $y = 2u + 1$ for some nonnegative integer u. Then $x = \frac{y^2+1}{2}$, which is a positive integer. Suppose that $x, y, t = 1$ is a solution to (5.7). By Theorem 5.1.1

$$n = 2x + y + 3 = y^2 + y + 4 = 4u^2 + 6u + 6.$$

Therefore, $k = n - y = y^2 + 4$ and $j = n - x - 2 = \frac{y^2}{2} + y + \frac{3}{2}$. Since $y = 2u + 1$,

$$k = 4u^2 + 4u + 5 \text{ and } j = 2u^2 + 4u + 3.$$

The conditions on n, k and j to verify that $W(n, k, j)$ exists and has exponent α_n are:

(i) $k + j \geq n + 2$,

(ii) $(k, j) = 1$,

(iii) $\lceil \frac{n-1}{2} \rceil \leq j < k \leq n$.

For (i), $k+j \geq n+2$ is equivalent to $y^2+4+y^2/2+y+3/2 \geq y^2+y+4+2$, equivalently $y^2/2 - 1/2 \geq 0$, which is always true for $y \geq 1$.

For (ii) let $d = (k, j)$ as in Lemma 5.1.2. Since k and j are odd, d is also odd. Now $d|j \Rightarrow d|2j$ and $2j = 4u^2 + 8u + 6$. Also $d|k$ and $k = 4u^2 + 4u + 5$, thus $d|(2j - k)$ and $2j - k = 4u + 1$, so

$$d|(4u + 1). \tag{5.9}$$

On the other hand, $d|5j$ and $5j = 10u^2 + 20u + 15$. Also $d|3k$ and $3k = 12u^2 + 12u + 15$, thus $d|(5j - 3k)$ and $(5j - 3k) = 2u^2 - 8u = 2u(u - 4)$. Since d is odd

$$d|u(u - 4). \tag{5.10}$$

Now consider the following three cases:

(1) Suppose $d|u$, then $d|4u$, so (5.9) implies $d|1$ giving $d = (k, j) = 1$.

(2) Suppose $d|(u - 4)$, then $d|4(u - 4)$, thus (5.9) implies that $d|(4u + 1) - (4u - 16)$. Thus $d|17$, which implies that $d = 1$ or 17. In this case, d is always equal to 1 except in the case that $u - 4 = 17q$ for some positive integer q. On the other hand, by Lemma 5.1.2 if $u = 17q + 4$, then $17|d$. It follows that $d = 17$ whenever $u = 17q + 4$, for some positive integer q. In other words, $(k, j) = 17$ if $y = 2u + 1 = 34q + 9$ for some positive integer q, and $(k, j) = 1$ otherwise.

(3) Suppose $d \nmid u$ and $d \nmid (u-4)$. Let $d = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, where $p_1, p_2, \dots, p_r$ are distinct primes and $e_1, e_2, \dots, e_r$ are positive integers. Since $p_i|d$, for all

$i = 1, 2, \ldots, r$, by (5.10) each p_i either divides u or $u - 4$ or both. Without loss of generality, suppose $p_1|u$. Then as in case (1) it follows that $p_1 = 1$, contradicting the assumption that p_1 is a prime. Therefore, $p_i|(u-4)$ for all $i = 1, 2, \ldots, r$, which implies $d|(u-4)$, and the result follows as in case (2).

Finally, for (iii) consider a positive integer y. Then since $y^2+4 < y^2+y+4$, it is obvious that $k \leq n$, and in fact $k < n$. Since $0 < (y-1)^2 + 1 \Rightarrow 0 < y^2 - 2y + 2 \Rightarrow 0 < y^2/2 - y + 1 \Rightarrow y^2/2 + y + 3 < y^2 + 4$, it follows that $j < k$. The left hand side inequality in (iii) is true because $\lceil \frac{y^2+y+3}{2} \rceil \leq y^2/2+y+3/2$, for any $y \geq 1$.

These three conditions (i), (ii) and (iii) imply that if $n = 4u^2 + 6u + 6$, $k = 4u^2 + 4u + 5$ and $j = 2u^2 + 4u + 3$, then $\gamma(W(n,k,j)) = \alpha_n$, whenever $u \not\equiv 4 (\text{mod } 17)$; if $u \equiv 4 (\text{mod } 17)$, then $W(n,k,j)$ is not defined. ∎

The following example illustrates the above theorem.

Example 5.1.4 *If* $u = 4$ $(u \equiv 4(\text{mod } 17))$*, then* $y = 9$ *and* $x = 41$*, thus* $n = 94$*,* $k = 85$ *and* $j = 51$*; but since* $(85, 51) = 17$*, the condition that* $(k, j) = 1$ *in Theorem 5.1.1 is not satisfied. However, if* $u = 5$ $(u \not\equiv 4(\text{mod } 17))$*, then* $y = 11$ *and* $x = 61$*, thus* $n = 136$*,* $k = 125$ *and* $j = 73$ *with* $(125, 73) = 1$ *and* $\lceil \frac{135}{2} \rceil = 68 \leq 73 < 125 \leq 136$*, so all of the conditions on* n, k *and* j *in Theorem 5.1.1 are satisfied. Thus* $W(136, 125, 73)$*, which has* 137 *arcs, has exponent equal to* α_{136}*.*

Now consider the case n odd. The following result shows that if $v \equiv 10(\text{mod } 13)$, then $(k, j) \neq 1$, where $k = 4v^2 + 3$ and $j = 2v^2 + 2v + 1$.

Lemma 5.1.5 *If $v = 10 + 13q$ with q a nonegative integer and*

$$d = (4v^2 + 3, 2v^2 + 2v + 1),$$

then $13|d$.

Proof. If $v = 10+13q$ for some $q \in N$, then $k = 4v^2+3 = 13q'+403 = 13q_1$ for some integer q_1, and $j = 2v^2 + 2v + 1 = 13q_2$ for some integer q_2. It follows that $d = (13q_1, 13q_2) = 13(q_1, q_2)$, which implies that $13|d$. ∎

Using the above lemma, the following theorem proves that for n odd, there are infinitely many solutions to (5.1) when $t = 1$, and an infinite proper subset of these solutions generates a family of nonisomorphic primitive digraphs $W(n, k, j)$ with exponent α_n.

Theorem 5.1.6 *If $t = 1$, then $x = \frac{y^2}{2}$, $y = 2v$ with v a positive integer gives an infinite family of integer solutions to the equation $x^2 + y^2 = (x + y)^2 - 1$, where $n = 2x + y + t + 2 = 4v^2 + 2v + 3$ is odd. For $v \not\equiv 10 (\text{mod } 13)$, an infinite sub-family of these solutions generates an infinite family of primitive digraphs $W(n, k, j)$ with exponent α_n, where $k = 4v^2+3$ and $j = 2v^2+2v+1$.*

Proof. Consider (5.8) and let $t = 1$. Hence

$$x^2 + y^2 = (x + 1)^2 - 1 = x^2 + 2x + 1 - 1 \Rightarrow y^2 = 2x.$$

Therefore, y is even, so let $y = 2v$ for some positive integer v. Thus $x = y^2/2$ is a positive integer. Suppose that $x, y, t = 1$ is a solution to (5.8). Then by Theorem 5.1.1

$$n = 2x + y + 3 = y^2 + y + 3 = 4v^2 + 2v + 3.$$

Therefore, $k = n - y = y^2 + 3$ and $j = n - x - 2 = \frac{y^2}{2} + y + 1$. Since $y = 2v$,

$$k = 4v^2 + 3 \text{ and } j = 2v^2 + 2v + 1.$$

The conditions on n, k and j to verify are the same as for the case n even as stated in the proof of Theorem 5.1.3.

For (i), $k+j \geq n+2$ is equivalent to $y^2+3+y^2/2+y+1 \geq y^2+y+3+2$, equivalently $y^2/2 - 1 \geq 0$, which is always true since $y \geq 2$.

For (ii) let $d = (k, j)$ as in Lemma 5.1.5. Since k and j are odd, d is also odd. Now $d|j \Rightarrow d|2j$ and $2j = 4v^2 + 4v + 2$. Also $d|k$ and $k = 4v^2 + 3$, thus $d|(2j - k)$ and $2j - k = 4v - 1$, so

$$d|(4v - 1). \tag{5.11}$$

On the other hand, $d|3j$ and $3j = 6v^2 + 6v + 3$. Also $d|k$ and $k = 4v^2 + 3$, thus $d|(3j - k)$ and $3j - k = 2v^2 + 6v = 2v(v + 3)$. Since d is odd

$$d|v(v + 3). \tag{5.12}$$

Now consider the following three cases:

(1) Suppose $d|v$, then $d|4v$, so (5.11) implies $d|1$ giving $d = (k, j) = 1$.

(2) Suppose $d|(v + 3)$, then $d|4(v + 3)$, thus (5.11) implies that $d|(4v + 12) - (4v - 1)$. Thus $d|13$ which implies that $d = 1$ or 13. In this case, d is always equal to 1 except in the case that $v + 3 = 13q_1$ for some positive

integer q_1 or equivalently $v = 10 + 13q$ for some positive integer q. On the other hand, by Lemma 5.1.5, if $v = 10 + 13q$, then $13|d$. It follows that $d = 13$ whenever $v = 10 + 13q$, for some positive integer q. In other words, $(k, j) = 13$ if $y = 2v = 26q+20$ for some nonnegative integer q, and $(k, j) = 1$ otherwise.

(3) Suppose $d \not| v$ and $d \not| (v+3)$, then $d = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, where $p_1, p_2, \dots, p_r$ are distinct prime numbers and $e_1, e_2, \dots, e_r$ are positive integers. Since $p_i|d$, for all $i = 1, 2, \dots, r$, by (5.12) each p_i either divides v or $v + 3$ or both. Without loss of generality suppose $p_1|v$, then as in case (1) it follows that $p_1 = 1$, contradicting the assumption that p_1 is a prime. Therefore, $p_i|(v+3)$ for all $i = 1, 2, \dots, r$, implying $d|(v+3)$, and the result follows as in case (2).

Finally for (iii) consider a positive integer y. Then $(y-1)^2 + 3 > 0 \Rightarrow y^2 - 2y + 4 > 0 \Rightarrow y^2/2 - y + 2 > 0 \Rightarrow y^2 + 3 > y^2/2 + y + 1$. It follows that $k > j$.

These three conditions $(i), (ii)$ and (ii) imply that if $n = 4v^2 + 2v + 3$, $k = 4v^2 + 3$ and $j = 2v^2 + 2v + 1$, then $\gamma(W(n, k, j)) = \alpha_n$ whenever $v \not\equiv 10 (\text{mod } 13)$; if $v \equiv 10 (\text{mod } 13)$, then $W(n, k, j)$ is not defined. ∎

The following example illustrates the above theorem.

Example 5.1.7 *If* $v = 10$, $(v \equiv 10 (\text{mod } 13))$, *then* $y = 20$ *and* $x = 200$, *thus* $n = 423$, $k = 403$ *and* $j = 221$; *but since* $(403, 221) = 13$, *the condition that* $(k, j) = 1$ *in Theorem 5.1.1 is not satisfied. However, if* $v = 11$, $(v \not\equiv 10 (\text{mod } 13))$, *then* $y = 22$ *and* $x = 242$, *thus* $n = 509$, $k = 487$ *and* $j = 265$

with $(487, 265) = 1$ *and* $\lceil \frac{508}{2} \rceil = 254 \leq 265 < 487 \leq 509$*, so all of the conditions on* n, k, j *in Theorem 5.1.1 are satisfied. Thus* $W(509, 487, 265)$*, which has* 510 *arcs, has exponent equal to* α_{509}*.*

5.2 Some Number Theory Results

In this section, some results from number theory are stated for use in the following sections to solve the equations in Theorem 5.1.1. Most of the number theoretic definitions and results from Theorem 5.2.1 through Theorem 5.2.12 are taken from the book by Apostol [1].

Theorem 5.2.1 [1, Theorem 5.14] *Assume* $(a, m) = d$ *and suppose that* $d|b$*. Then the linear congruence* $as \equiv b (\mathrm{mod}\ m)$ *has exactly* d *solutions modulo* m*.*

The following definitions are from [14, p. 32 and 84], respectively.

Definition 5.2.2 *A reduced residue system modulo* m *is a set of integers* $\{r_1, r_2, \ldots, r_\ell\}$ *such that* $(r_i, m) = 1$*,* $r_i \not\equiv r_\ell (\mathrm{mod}\ m)$ *for* $i \neq \ell$*, and such that every integer relatively prime to* m *is congruent modulo* m *to exactly one member* r_i *of the set.*

Definition 5.2.3 *If* a *and* m *are positive integers with* $(a, m) = 1$*, then* a *is a quadratic residue modulo* m *if the congruence* $s^2 \equiv a \pmod{m}$ *has a solution. If the congruence* $s^2 \equiv a \pmod{m}$ *has no solutions, then* a *is a quadratic nonresidue modulo* m*.*

Theorem 5.2.4 [1, Theorem 9.1] *Let p be an odd prime. Then every reduced residue system modulo p contains exactly $(p-1)/2$ quadratic residues and exactly $(p-1)/2$ quadratic nonresidues modulo p. The quadratic residues belong to the residue classes containing the numbers*

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2. \tag{5.13}$$

We next state Lagrange's Theorem.

Theorem 5.2.5 [1, Theorem 5.22] *Let p be a prime and $f(x) = c_0 + c_1x + \ldots + c_nx^n$ be a polynomial of degree n with integer coefficients such that $c_n \not\equiv 0 (\text{mod } p)$. Then the polynomial congruence $f(x) \equiv 0 (\text{mod } p)$ has at most n solutions.*

Using Lagrange's Theorem, we show that the quadratic congruence $s^2 \equiv a (\text{mod } p)$ has either two solutions or no solutions.

Corollary 5.2.6 *If p is an odd prime and $(a, p) = 1$, then the quadratic congruence $s^2 \equiv a (\text{mod } p)$ has exactly two solutions or no solutions.*

Proof. By Lagrange's Theorem the quadratic congruence $s^2 \equiv a (\text{mod } p)$, where p is an odd prime and $a \not\equiv 0 (\text{mod } p)$, has at most two solutions. Moreover, if s is a solution, then so is $-s$, hence the number of solutions modulo p is either 0 or 2. ∎

The following definition is from [1, p. 179].

Definition 5.2.7 *If p denotes an odd prime and $(a,p) = 1$, then the Legendre symbol $(\frac{a}{p})$ is defined to be 1 if a is a quadratic residue, -1 if a is a quadratic nonresidue modulo p. If $(a,p) \neq 1$, then $(\frac{a}{p}) = 0$.*

Therefore, by Corollary 5.2.6, $s^2 \equiv a(mod\ p)$ has exactly two distinct solutions if and only if $(\frac{a}{p}) = 1$, otherwise it has no solutions. The following result is called Fermat's Little Theorem, and then we state Euler's Criterion.

Theorem 5.2.8 [1, Theorem 5.19] *If p is a prime and a is an integer, then $a^p \equiv a \pmod{p}$.*

Theorem 5.2.9 [1, Theorem 9.2] *Let p be an odd prime. Then $a^{(p-1)/2} \equiv (\frac{a}{p}) \pmod{p}$ for all a.*

Theorem 5.2.10 [1, Theorem 9.3] *For p an odd prime, Legendre's symbol $(\frac{n}{p})$ is a completely multiplicative function of n, i.e. $(\frac{mn}{p}) = (\frac{m}{p})(\frac{n}{p})$.*

Theorem 5.2.11 [1, Theorem 9.4] *For every odd prime p*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases} \tag{5.14}$$

Theorem 5.2.12 [1, Theorem 9.5] *For every odd prime p*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{8} \\ -1 & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases} \tag{5.15}$$

The following lemma shows that the problem of solving the congruence $s^2 \equiv -a \pmod{t}$, where $t = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, can be reduced to that of a system of congruences $s^2 \equiv -a \pmod{p_i^{e_i}}$ for $i = 1, 2, \dots, r$.

Lemma 5.2.13 *If p is an odd prime and $(a, p) = 1$, then each solution to the congruence $s^2 \equiv -a \pmod{p^e}$, $e \geq 2$, generates a solution to the congruence $s^2 \equiv -a \pmod{p}$ and conversely.*

Proof. Suppose for some $e \geq 2$ the congruence $s^2 \equiv -a \pmod{p^e}$ or equivalently

$$s^2 + a \equiv 0 \pmod{p^e} \tag{5.16}$$

has a solution s_1, where s_1 is chosen so that it lies in the interval $0 < s_1 < p^e$. This solution also satisfies each of the congruences $s^2 \equiv -a \pmod{p^f}$ for $f < e$. In particular, s_1 satisfies the congruence

$$s^2 + a \equiv 0 \pmod{p^{e-1}}. \tag{5.17}$$

Now divide s_1 by p^{e-1} and write $s_1 = qp^{e-1} + r$, where $0 \leq r < p^{e-1}$. Since $r \equiv s_1 \pmod{p^{e-1}}$ the number r is also a solution to (5.17). In other words, every solution s_1 of (5.16) in the interval $0 < s_1 < p^e$ generates a solution r of (5.17) in the interval $0 \leq r < p^{e-1}$.

Now suppose we start with a solution r to (5.17) in the interval $0 \leq r < p^{e-1}$ and ask whether there is a solution s_2 to (5.16) in the interval

$0 < s_2 < p^e$ that r generates. Since $e \geq 2$,

$$(r + qp^{e-1})^2 + a = r^2 + 2rqp^{e-1} + q^2p^{2e-2} + a \equiv r^2 + a + 2rqp^{e-1} (\text{mod } p^e)$$

where q is an integer to be specified. But r satisfies (5.17) so there is an integer u such that $r^2 + a = up^{e-1}$ and the last congruence becomes

$$(r + qp^{e-1})^2 + a \equiv r^2 + a + 2rqp^{e-1} = (2rq + u)p^{e-1} (\text{mod } p^e).$$

Now let $s_2 = r + qp^{e-1}$. Then s_2 satisfies (5.16) if and only if $2rq + u \equiv 0 (\text{mod } p)$, which is a linear congruence on q modulo p.

Note that p does not divide $2r$. Otherwise, since p is odd $p|r$, hence $p|r^2$. But, by assumption $p^{e-1}|(r^2 + a)$ thus $p|(r^2 + a)$, it follows that $p|a$ contradicting $(a, p) = 1$. Therefore, by Theorem 5.2.1, $2rq + u \equiv 0 (\text{mod } p)$ has exactly one solution q and the result is proved. ∎

The following theorem is proved in [14, Theorem 2.18].

Theorem 5.2.14 *Let $N(m)$ denote the number of solutions to the congruence $f(x) \equiv 0 \pmod{m}$. Then $N(m) = \prod_{i=1}^{r} N(p_i^{e_i})$ if $m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ where $p_1, p_2, \dots, p_r$ are distinct primes and $e_i \in N$ for all $1 \leq i \leq r$.*

5.3 Solutions to (5.1) for n even

In this section, the above results are used to determine those values of t for which (5.1) has a solution, and the number of such solutions for the case n even; see Theorem 5.3.7. It is shown that if a solution $x,\ y,\ t$ to (5.1) for n even exists, then each prime factor of t is congruent to 1 or 3 modulo 8. The equation to be solved in this case is (5.7)

$$x^2 + y^2 = (x + t)^2 - 2.$$

Lemma 5.3.1 *If p is an odd prime, then the congruence $s^2 \equiv -2 \pmod{p}$ has exactly two distinct solutions if and only if $p \equiv 1, 3 \pmod{8}$, and no solutions otherwise.*

Proof. Suppose $p \equiv 1 (\text{mod } 8)$. Then $p \equiv 1 (\text{mod } 4)$. Thus by Theorems 5.2.10, 5.2.11 and 5.2.12, $(\frac{-2}{p}) = (\frac{2}{p})(\frac{-1}{p}) = (1)(1) = 1$. Suppose $p \equiv 3 (\text{mod } 8)$. Then again by Theorems 5.2.10, 5.2.11 and 5.2.12, $(\frac{-2}{p}) = (\frac{2}{p})(\frac{-1}{p}) \equiv (-1)(-1) = 1$. Thus in each case the congruence has a solution, so by Corollary 5.2.6 it has exactly two distinct solutions.
For the converse, suppose the congruence $s^2 \equiv -2 \pmod{p}$ has exactly two distinct solutions. Thus $(\frac{-2}{p}) = 1$. It follows that $(\frac{-1}{p}) = (\frac{2}{p}) = 1$ and then $p \equiv 1 (\text{mod } 8)$, or $(\frac{-1}{p}) = (\frac{2}{p}) = -1$ giving $p \equiv 3 (\text{mod } 8)$. ∎

Corollary 5.3.2 *If $t = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ where $p_1, p_2, \dots, p_r$ are distinct odd primes and $r, e_i \in N$, then the congruence $s^2 \equiv -2 \pmod{t}$ has exactly*

2^r *distinct solutions if and only if each* p_i, $i = 1, 2, \ldots, r$ *is congruent to* 1 *or* 3 *modulo* 8, *and no solutions otherwise.*

Proof. If $r = 1$, then the result follows from Lemmas 5.3.1 and 5.2.13. Suppose each p_i, $i = 1, 2, \ldots, r$, $r \geq 2$ is congruent to 1 or 3 modulo 8, then the result follows from Lemmas 5.3.1 and 5.2.13 and Theorem 5.2.14. For the converse, suppose the congruence $s^2 \equiv -2 \pmod{t}$ has exactly 2^r distinct solutions. Using Theorem 5.2.14, for any i, $i = 1, 2, \ldots, r$ the congruence $s^2 \equiv -2 \pmod{p_i}$ has a solution and Lemma 5.3.1 implies that p_i is congruent to 1 or 3 modulo 8 for all $i = 1, 2, \ldots, r$. ∎

Proposition 5.3.3 *If* t *is odd, then* m *is a solution to* $y^2 \equiv t^2 - 2 (\text{mod } 2t)$ *if and only if it is an odd solution to* $y^2 \equiv -2 (\text{mod } t)$.

Proof. Let $y = m$ be a solution to $y^2 \equiv t^2 - 2 (\text{mod } 2t)$, which must be odd (since t is odd). Thus there exists an integer q such that $m^2 - t^2 + 2 = 2tq$, so $m^2 + 2 = t(2q + t)$. Hence $m^2 \equiv -2 (\text{mod } t)$, which implies that m is a solution to $y^2 \equiv -2 (\text{mod } t)$. If m is an odd solution to $y^2 \equiv -2 (\text{mod } t)$, then m is also a solution to $y^2 \equiv t^2 - 2 (\text{mod } t)$. Since $m^2 - t^2 + 2$ is even and t odd, it follows that m is a solution to $y^2 \equiv t^2 - 2 (\text{mod } 2t)$. ∎

Therefore, if all of the solutions to $y^2 \equiv -2 (\text{mod } t)$ are odd, then they all generate distinct solutions to $y^2 \equiv t^2 - 2 (\text{mod } 2t)$. However, if $y^2 \equiv -2 (\text{mod } t)$ has an even solution y, then $y + t$ is an odd solution to $y^2 \equiv$

$-2(\text{mod } t)$, so by Proposition 5.3.3 it is also a solution to $y^2 \equiv t^2 - 2(\text{mod } 2t)$. It follows that choosing 2^r distinct solutions to $y^2 \equiv -2(\text{mod } t)$ to be odd gives exactly 2^r distinct solutions to $y^2 \equiv t^2 - 2(\text{mod } 2t)$. This proves the following corollary.

Corollary 5.3.4 *If $t = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ where $p_1, p_2, \dots, p_r$ are distinct odd primes and $r, e_i \in N$, then the congruence $y^2 \equiv t^2 - 2(\text{mod } 2t)$ has exactly 2^r distinct solutions modulo $2t$ if and only if every prime divisor of t is congruent to 1 or 3 modulo 8, and no solutions otherwise.*

Lemma 5.3.5 *Let a be an integer. Then $a^2 \equiv 0, 1(\text{mod } 4)$.*

Proof. If $a = 2m$ for some $m \in Z$, then $a^2 = 4m^2 \equiv 0(\text{mod } 4)$. If $a = 2m+1$ for some $m \in Z$, then $a^2 = 4m^2 + 4m + 1 \equiv 1(\text{mod } 4)$. ∎

Proposition 5.3.6 *If $x,\ y,\ t$ are positive integers such that $x^2 + y^2 = (x + t)^2 - 2$, then $x,\ y$ and t are all odd.*

Proof. If $x,\ y,\ t$ are positive integers satisfying $x^2 + y^2 = (x+t)^2 - 2$, then x and y cannot be both even, since otherwise $x^2 + y^2 \equiv 0(\text{mod } 4)$, which implies that $(x + t)^2 \equiv 2(\text{mod } 4)$, contradicting Lemma 5.3.5.

Moreover x and y have the same parity. Otherwise, without loss of generality, suppose x is even and y is odd. Then $x^2 + y^2 \equiv 1(\text{mod } 4)$, and using (5.7), $(x + t)^2 - 2 \equiv 1(\text{mod } 4)$. Thus $(x + t)^2 \equiv 3(\text{mod } 4)$, which contradicts

Lemma 5.3.5. Therefore x and y have the same parity, and hence they both are odd.

Now since x and y are odd, it follows that $x^2 + y^2$ is even. From (5.7), $(x + t)^2$ is even, that is $x + t$ is even, which implies that t is odd. ∎

Theorem 5.3.7 *The equation $x^2 + y^2 = (x + t)^2 - 2$ has integer solutions x, y and t if and only if every prime divisor of t is congruent to 1 or 3 modulo 8. For any such t there are infinitely many solutions.*

Proof. If x, y and t are integers such that $x^2 + y^2 = (x + t)^2 - 2$, then $y^2 = 2tx + t^2 - 2$ and it follows that $y^2 \equiv t^2 - 2 (\mathrm{mod}\ 2t)$. By Corollary 5.3.4, every prime divisor of t is congruent to 1 or 3 modulo 8.

For the converse, suppose $t = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ with every p_i, $i = 1, 2, \dots, r$, congruent to 1 or 3 modulo 8. By Corollary 5.3.4, $y^2 \equiv t^2 - 2 (\mathrm{mod}\ 2t)$ has 2^r distinct solutions. Let m be such a solution that is also the least residue of y modulo $2t$. Now x, y, t with $y = m + 2tq$, $x = \frac{y^2 - t^2 + 2}{2t} = (2tq^2 + 2mq) + \frac{m^2 - t^2 + 2}{2t}$ is a solution to the equation $x^2 + y^2 = (x + t)^2 - 2$, for $q = 0, 1, 2, \dots$. Therefore, for any such t there are infinitely many solutions. ∎

5.4 Solutions to (5.1) for n odd

The aim of this section is to determine those values of t for which (5.1) has a solution, and the number of such solutions for the case n odd; see Theorem

5.4.6. Results are parallel to those of Section 5.3 for n even. It is shown that if a solution $x,\ y,\ t$ to (5.1) for n odd exists, then each prime factor of t is congruent to 1 modulo 4. The equation to be solved is (5.8)

$$x^2 + y^2 = (x + t)^2 - 1.$$

Lemma 5.4.1 *If p is an odd prime, then the congruence $s^2 \equiv -1 (\text{mod } p)$ has exactly two solutions if and only if $p \equiv 1 (\text{mod } 4)$, and no solutions otherwise.*

Proof. By Theorem 5.2.11, the congruence $s^2 \equiv -1 (\text{mod } p)$ has a solution if and only if $p \equiv 1 (\text{mod } 4)$, and by Corollary 5.2.6 if it has a solution it has exactly two distinct solutions. ∎

Corollary 5.4.2 *If $t = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ where $p_1, p_2, \dots, p_r$ are distinct odd primes, then the congruence $s^2 \equiv -1 \pmod{t}$ has exactly 2^r distinct solutions if and only if each p_i is congruent to 1 modulo 4, and no solutions otherwise.*

Proof. If $r = 1$, then the result follows from Lemmas 5.4.1 and 5.2.13. Suppose each p_i, $i = 1, 2, \dots, r$, is congruent to 1 modulo 4. Then the result follows from Lemma 5.4.1 and Theorem 5.2.14. Suppose the congruence $s^2 \equiv -1 \pmod{t}$ has exactly 2^r distinct solutions. Using Theorem 5.2.14, for any i, $i = 1, 2, \dots, r$, the congruence $s^2 \equiv -1 \pmod{p}$ has a solution and by Lemma 5.2.13 it has exactly two distinct solutions. Lemma 5.4.1 implies that for each $i = 1, 2, \dots, r$, p_i is congruent to 1 modulo 4. ∎

Proposition 5.4.3 *If t is odd, then m is a solution to $y^2 \equiv t^2 - 1 (\text{mod } 2t)$ if and only if it is an even solution to $y^2 \equiv -1 (\text{mod } t)$.*

Proof. If m is a solution to $y^2 \equiv t^2 - 1 (\text{mod } 2t)$, then m is even and also a solution to $y^2 \equiv -1 (\text{mod } t)$. Let m be even and a solution to $y^2 \equiv -1 (\text{mod } t)$. Then m is a solution to $y^2 \equiv t^2 - 1 (\text{mod } t)$. Since $m^2 - t^2 + 1$ is even and t odd, it follows that m is also a solution to $y^2 \equiv t^2 - 1 (\text{mod } 2t)$. ∎

Therefore, if all of the solutions to $y^2 \equiv -1 (\text{mod } t)$ are even, then they all generate distinct solutions to $y^2 \equiv t^2 - 1 (\text{mod } 2t)$. However, if $y^2 \equiv -1 (\text{mod } t)$ has an odd solution y, then $y + t$ is an even solution to $y^2 \equiv -1 (\text{mod } t)$, so by Proposition 5.4.3, it is also a solution to $y^2 \equiv t^2 - 1 (\text{mod } 2t)$. It follows that choosing 2^r distinct solutions to $y^2 \equiv -2 (\text{mod } t)$ to be even gives exactly 2^r distinct solutions to $y^2 \equiv t^2 - 2 (\text{mod } 2t)$. This proves the following corollary.

Corollary 5.4.4 *If $t = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ where $p_1, p_2, \dots, p_r$ are distinct odd primes and $r, e_i \in N$, then the congruence $y^2 \equiv t^2 - 1 (\text{mod } 2t)$ has exactly 2^r distinct solutions modulo $2t$ if and only if every prime divisor of $t = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ is congruent to 1 modulo 4, and no solutions otherwise.*

Proposition 5.4.5 *If $x,\ y,\ t$ are positive integers such that $x^2 + y^2 = (x + t)^2 - 1$, then x and y are even and t is odd.*

Proof. If $x,\ y,\ t$ are positive integers satisfying $x^2 + y^2 = (x + t)^2 - 1$, then x and y cannot be both odd, since otherwise $x^2 + y^2 \equiv 2 (\text{mod } 4)$, which implies that $(x + t)^2 \equiv 3 (\text{mod } 4)$, contradicting Lemma 5.3.5.

Moreover, by an argument as in Proposition 5.3.6, x and y have the same parity. Now t must be odd, because since x and y are even, it follows that $x^2 + y^2$ is even. Thus $(x+t)^2 - 1$ is even, that is $x + t$ is odd, which implies t is odd. ∎

Theorem 5.4.6 *The equation $x^2 + y^2 = (x + t)^2 - 1$ has integer solutions x, y and t if and only if every prime divisor of t is congruent to 1 modulo 4. For any such t there are infinitely many solutions.*

Proof. If x, y and t are integers such that $x^2 + y^2 = (x + t)^2 - 1$, then $y^2 = 2tx + t^2 - 1$ and it follows that $y^2 \equiv t^2 - 1 (\text{mod } 2t)$. By Corollary 5.4.4, every prime divisor of t is congruent to 1 modulo 4.

For the converse, suppose $t = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ with every p_i, $i = 1, 2, \dots, r$, congruent to 1 modulo 4. By Corollary 5.4.4, $y^2 \equiv t^2 - 1 (\text{mod } 2t)$ has 2^r distinct solutions. Let m be such a solution that is also the least residue of y modulo $2t$. Now x, y, t with $y = m + 2tq$ and $x = \frac{y^2 - t^2 + 1}{2t} = (2tq^2 + 2mq) + \frac{m^2 - t^2 + 1}{2t}$ is a solution to the equation $x^2 + y^2 = (x+t)^2 - 1$, for $q = 0, 1, 2, \dots$. Therefore, for any such t there are infinitely many solutions. ∎

Theorems 5.3.7 and 5.4.6 imply that there are infinitely many solutions to (5.1) for n even and n odd, respectively. By Theorem 5.1.1 any such solution generates a primitive digraph $W(n, k, j)$ with exponent α_n if and only if n, k and j satisfy $(k, j) = 1$ and $\lceil \frac{n-1}{2} \rceil \leq j < k \leq n$, where $n = 2x + y + t + 2$, $k = n - y$ and $j = n - x - 2$. The above conditions on j and k must be satisfied.

For example, $x = 5, y = 13, t = 9$ is a solution to $x^2 + y^2 = (x + t)^2 - 2$ that gives $n = 39, k = 26, j = 32$ but $(k, j) \neq 1$, and $x = 7, y = 25, t = 19$ is a solution to this equation that gives $n = 60, k = 35, j = 51$ but $j > k$. Similarly, there are examples of solutions to $x^2 + y^2 = (x + t)^2 - 1$ that do not satisfy the conditions on n, k, j given in Theorem 5.1.1. However, there is an infinite sub-family of solutions to (5.1) that generates a family of nonisomorphic primitive digraphs $W(n, k, j)$ with exponent α_n (see, for example, the case for $t = 1$ in Section 5.1.1). The next chapter finds all such solutions for given n.

5.5 General t for n odd

The aim of this section is to identify all the solutions of equation (5.8), namely $x^2 + y^2 = (x + t)^2 - 1$. A complete solution of this equation was given by Catalan in 1885; see for example [6]. The solution is $x = 2(pr + qs), y = 2(qr - ps)$ and $x + t = 2m + 1$ such that $r^2 + s^2 = m$ and $p^2 + q^2 = m + 1$. In other words, we can find a solution to the equation whenever there are two consecutive integers m and $m + 1$, each of which is a square or the sum of two squares. This gives the solution $n = x + y + x + t + 2 = 2(pr + qs) + 2(qr - ps) + 2m + 1 + 2$, $k = n - y = 2(pr + qs) + 2m + 1 + 2$, $j = n - x - 2 = 2(qr - ps) + 2m + 1$ for our problem whenever n, k, j satisfy the conditions of Theorem 5.1.1.

Another approach is to find all x and y satisfying equation (5.8) for any

given fixed value of t. Since by Theorem 5.4.6 every prime divisor of t is congruent to 1 modulo 4, t is also congruent to 1 modulo 4, thus there exists an integer b such that $t-1=4b$. By Proposition 5.4.5 y is even so let $y=2p$ for some positive integer p. From the equation $x^2+y^2=(x+t)^2-1$, it follows that $y^2=2tx+t^2-1$, so $x=\frac{y^2-(t^2-1)}{2t}=\frac{y^2-2t[(t-1)/2]-(t-1)}{2t}$. Hence $2t|(y^2-2t[(t-1)/2]-(t-1))$, so $2t|y^2-(t-1)$ which implies that $2t|4p^2-4b=4(p^2-b)$. Since t is odd, $t|p^2-b$. It follows that $p^2-b=tc$ for some integer c, so $p^2=tc+b=tc+\frac{t-1}{4}=\frac{4tc+t-1}{4}=\frac{4(4b+1)c+4b+1-1}{4}$, that is $p^2=(4b+1)c+b$.

For example if $t=5$, then $b=1$, so $p^2=5c+1$. Thus $5c=(p-1)(p+1)$. Since 5 is prime, it divides either $p-1$ or $p+1$ but not both. Thus $p=5q+1$ or $p=5q-1$ for some positive integer q.

Therefore, for $t=5$, if we let $y=2(5q\pm1)$ then $x=\frac{4(25q^2\pm10q+1)-(5^2-1)}{2(5)}=10q^2\pm4q-2$. Thus $n=20q^2+18q+5$, $k=20q^2+8q+3$ and $j=10q^2+14q+5$, or $n=20q^2+2q+1$, $k=20q^2-8q+3$ and $j=10q^2+6q+1$. These are solutions to our problem provided that they satisfy the conditions of Theorem 5.1.1.

But this approach does not work for all t because, for example, it is not always possible to factor the expression analogous to p^2-1 for the case $t=5$ above. For given t, $b=\frac{t-1}{4}$ and $p^2=tc+b$; but if b is not a perfect square, then p^2-b cannot be factored over the integers.

Chapter 6

Algorithm

As shown in Chapter 4, the minimum number of arcs in a primitive digraph on $n \geq 5$ vertices with exponent α_n is less than or equal to $n+2$. By the main result in Chapter 5, this minimum number is equal to $n+1$ if and only if (5.1) has an integer solution satisfying the conditions given in Theorem 5.1.1. We now address the following question: for a given integer $n \geq 5$, what is the minimum number of arcs in a primitive digraph on n vertices with exponent α_n? The answer is either $n+1$ or $n+2$. This chapter presents an algorithm, and in fact a program, that gives the answer to this question.

Note that by Theorems 5.3.7 and 5.4.6, there is a solution to the equation (5.1)

$$x^2 + y^2 = \begin{cases} (x+t)^2 - 2, & \text{if } n \text{ is even} \\ (x+t)^2 - 1, & \text{if } n \text{ is odd} \end{cases}$$

if and only if every prime divisor of t is congruent to 1 or 3 modulo 8 for even n, and every prime divisor of t is congruent to 1 modulo 4 for odd n. However, there may not exist a primitive digraph $W(n,k,j)$ with exponent equal to α_n for every such solution. By Theorem 5.1.1, a solution x,y,t to the above equation generates a primitive digraph $W(n,k,j)$ with exponent α_n only if $n = 2x+y+t+2$, $k = n-y$ and $j = n-x-2$ satisfy $(k,j) = 1$ and $\lceil \frac{n-1}{2} \rceil \leq j < k \leq n$.

Consider a solution x,y,t to (5.1). Using $\frac{n-1}{2} \leq \lceil \frac{n-1}{2} \rceil \leq \frac{n}{2}$ and $\lceil \frac{n-1}{2} \rceil \leq j < k \leq n$, it follows that

(i) $\frac{n+1}{2} \leq k = n-y \Rightarrow y \leq \frac{n-1}{2}$,

(ii) $\frac{n-1}{2} \leq j = n-x-2 \Rightarrow x \leq \frac{n+1}{2} - 2 = \frac{n-3}{2}$.

Let $i = 1$ or 2. Then by (5.1), $(x+t)^2 - i = x^2+y^2 \leq (\frac{n+1}{2}-2)^2 + (\frac{n-1}{2})^2 = \frac{n^2}{2} - 2n + \frac{5}{2}$. Thus $(x+t)^2 \leq \frac{n^2}{2} - 2n + \frac{5}{2} + i \leq \frac{n^2}{2} - 2n + \frac{9}{2} \Rightarrow x+t \leq (\frac{n^2}{2} - 2n + \frac{9}{2})^{1/2} \Rightarrow t \leq (\frac{n^2}{2} - 2n + \frac{9}{2})^{1/2} - x$. Since x is always positive, $t \leq (\frac{n^2}{2} - 2n + \frac{9}{2})^{1/2} \leq \frac{n}{\sqrt{2}}$ if $n \geq 3$.

Note that the only conditions of Theorem 5.1.1 on n,k,j that the algorithm must check are $(k,j) = 1$ and $j < k$ since

(1) $n \geq k$ is automatically true because $k = n-y$ and y in (5.1) is positive,

(2) $\lceil \frac{n-1}{2} \rceil \leq j$ is true since $x \leq \frac{n-3}{2}$ and $j = n-x-2$,

(3) $k+j \geq n+2$ is automatically satisfied since $k+j = n-y+n-x-2 = 3x+y+2t+2 > 2x+y+t+2+2 = n+2$.

Therefore, for any positive integer $n \geq 5$, our algorithm should check all positive integers $y \leq \frac{n-1}{2}$, $x \leq \frac{n-3}{2}$ and $t \leq \frac{n}{\sqrt{2}}$, with t satisfying the

conditions of Theorems 5.3.7 and 5.4.6, to determine solutions to (5.1). If there exits such a solution for which $n = 2x+y+t+2$, $k = n-y$, $j = n-x-2$, $(k, j) = 1$ and $j < k$, then there exists a primitive digraph $W(n, k, j)$ with exponent α_n; in other words, it follows that there is a primitive digraph on n vertices with $n + 1$ arcs and exponent equal to α_n.

By Corollaries 5.3.4 and 5.4.4, for any such $t = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, there are exactly 2^r distinct solutions for y, and by the proofs of Theorems 5.3.7 and 5.4.6, for any of these solutions y, there are infinitely many solutions x, y, t to (5.1). From these solutions, the ones satisfying Theorem 5.1.1 give $W(n, k, j)$.

The following program (in Maple) decides if there is such a solution for a given n and if so, it outputs the solution. If there is no such solutions, then the output will be 'no solution', which implies that the minimum number of arcs in a primitive digraph on the given number of vertices n with exponent α_n is equal to $n + 2$. Since any integer congruent to 1 or 3 modulo 8 is also congruent to 1 or 3 modulo 4, respectively, to avoid specifying separate values for t when n is even or odd, we consider t to be congruent to 1 or 3 modulo 4 in both cases.

Note that for given n, there may not be a unique primitive digraph $W(n, k, j)$ on n vertices with exponent α_n. In other words, for given n there may exist more than one solution to (5.1) that give digraphs with different cycle lengths k and j having $(k, j) = 1$ and $j < k$. As examples, for $n = 2086$, there are two primitive digraphs $W(2086, 1541, 1411)$ and $W(2086, 1579, 1377)$ with exponent equal to α_{2086}; for $n = 933$, there are

two primitive digraphs $W(933, 691, 629)$ and $W(933, 903, 481)$ with exponent equal to α_{933}. Moreover, for given n, there may exist more than two such digraphs; from the output of the following algorithm, if $n = 4404$ then there are three primitive digraphs $W(4404, 3365, 2881)$, $W(4404, 3821, 2537)$ and $W(4404, 3955, 2451)$ each with exponent equal to α_{4404}.

The following algorithm finds all primitive digraphs D on n vertices such that $\gamma(D) = \alpha_n$. It is given here for the case $n = 4404$. Note that the output shows that the minimum number of arcs in a primitive digraph on 4404 vertices with exponent α_{4404} is $4405 = 4404 + 1$.

```
n1 := 4404 :
d := floor(n1/sqrt(2.0)) :
flag := 0 :
if 2 * floor(n1/2) = n1 then c1 := -1 : c2 := 2 : c3 := 1 :
  else c1 := 0 : c2 := 1 : c3 := 2 :
end if :
for c from 1 by 2 to 3 do :
  for i from 0 to (d - 1)/4 do :
    t := 4 * i + c :
      for m from c3 by 2 to (2 * t + c1) do :
        if (m^2 - t^2 + c2) mod (2 * t) = 0 then :
          q := 0 :
          y := 2 * t * q + m :
          x := (2 * t * q^2 + 2 * m * q) + ((m^2 - t^2 + c2)/(2 * t)) :
          while (x <= (n1 - 3)/2) and (y <= (n1 - 1)/2) do :
            n := 2 * x + y + t + 2 :
            k := n - y :
            j := n - x - 2 :
            if gcd(k, j) = 1 and (j < k) and n = n1 then :
              print(x, y, t, q, m, n, k, j) :
              flag := 1 :
            end if :
            q := q + 1 :
            y := 2 * t * q + m :
            x := (2 * t * q^2 + 2 * m * q) + ((m^2 - t^2 + c2)/(2 * t)) :
          end do :
        end if :
      end do :
  end do :
end do :
if flag = 0 then :
  print('no solution') :
end if;
```

1865, 583, 89, 3, 49, 4404, 3821, 2537
1521, 1039, 321, 1, 397, 4404, 3365, 2881
1951, 449, 51, 4, 41, 4404, 3955, 2451

Chapter 7

Conclusions

In this chapter, some conclusions and ideas for future research are given. As stated in Theorem 5.1.1, the existence of a primitive digraph on n vertices with $n+1$ arcs and exponent α_n depends on the existence of integer solutions to equation (5.7) or (5.8) that satisfy additional constraints. For given n, the algorithm in Chapter 6 is used to determine whether or not there exists such a digraph with $n+1$ arcs. If no such digraph exists, then the results in Chapter 4 illustrate that the minimum number of arcs is $n+2$.

The following are some unanswered questions for further research. Lewin and Vitek [12] determined all of the integers in the interval $[\alpha_n, w_n]$ that can be the exponent of a primitive digraph on n vertices, and they showed that there are some gaps in this exponent set for primitive digraphs on n vertices. Thus, a question similar to that answered in Theorem 5.1.1 can be asked for any possible large exponent: *for a given n and γ_n with $\alpha_n < \gamma_n < w_n$*

such that γ_n is a possible exponent for a primitive digraph on n vertices, does there exist a primitive digraph on n vertices with $n+1$ arcs and exponent γ_n? In other words, for which n does there exist a digraph $W(n,k,j)$ with exponent γ_n? Note that since $\gamma(W(n,k,j)) = n + (k-2)j$, the question reduces to finding integral solutions to the equation $\gamma_n = n + (k-2)j$, which can be solved by an algorithm similar to that presented in Chapter 6. If there are no such solutions for even $n \geq 10$, consider D as the digraph obtained from Figure 4.1 by deleting the arc $\frac{n}{2} - 3 \to n - 4$ and adding one arc $\frac{n}{2} - r + 1 \to n - r$ that makes a j-cycle, where $5 \leq r \leq n - \frac{n}{2}$. Following the proof of Theorem 4.0.1, for this digraph D the exponent is equal to $\alpha_n + \ell$, where $\ell \in \{1, 2, \ldots, \frac{n}{2} - 4\}$ and the number of arcs is $n + 2$. Thus for even $n \geq 10$, if there is no digraph $W(n,k,j)$ with exponent $\alpha_n \leq \gamma_n \leq \alpha_n + \frac{n}{2} - 4$, then the minimum number of arcs in a primitive digraph with exponent γ_n is $n+2$. Similarly, for odd $n \geq 7$, using Theorem 4.0.2 and Figure 4.2 it can be shown that for $\ell \in \{1, 2, \ldots, \frac{n-5}{2}\}$ there exists a primitive digraph on n vertices with exponent $\alpha_n + \ell$ and $n+2$ arcs. But for an exponent γ_n greater than the above values, we do not know the minimum number of arcs in such digraphs when the equation $\gamma(W(n,k,j)) = n + (k-2)j$ does not have an integer solution.

Instead of the minimum number of arcs, we can consider the maximum number of arcs in a primitive digraph on n vertices with given large exponent. By the results from Chapter 2 and Appendix A, the maximum number of arcs in a digraph with exponent α_n for $n = 3$ and $n = 5$ is 5 and 8, respectively.

Since $j \geq \lceil \frac{n-1}{2} \rceil$ by [10], for $n \geq 6$ there are no loops nor 2-cycles. Thus the adjacency matrix of the digraph has at most $\frac{n^2-n}{2} = \binom{n}{2}$ ones. This implies that for $n \geq 6$ the maximum number of arcs in a primitive digraph on n vertices with large exponent is less than or equal to $\binom{n}{2}$. A related problem has been investigated in [17]. Let $f(n, r)$ be the maximum number of arcs in a primitive digraph on n vertices with exponent greater than or equal to r^2n^2, with $0 < r < 1$. Shen and Wyels [17] have shown that $(1 - r)^2/3$ is the asymptotic value for $f(n, r)/n^2$ whenever $r \geq \sqrt{2}/2$. Letting $r = \sqrt{2}/2$, the maximum number of arcs in a primitive digraph on n vertices with large exponent is asymptotically equal to $0.0286n^2 + O(n)$.

Other questions related to this area of research are the determination of the minimum cycle length, maximum cycle length or any other properties of a primitive digraph on n vertices with a given exponent.

Appendix A

Digraphs on 5 vertices

All nonisomorphic digraphs on $n = 5$ vertices with large exponent and cycle lengths $k = 4$ and $j = 3$ are given in this Appendix. In each the exponent is computed from the adjacency matrix of the digraph using MATLAB.

Since $k = 4$, the digraph D has a 4-cycle. First consider the digraph in Figure A.1. We claim that there can be no arcs from vertex 5 to two nonadjacent vertices in D. Suppose that there exist such arcs and without loss of generality let $5 \to 2$ and $5 \to 4$ be two of them. Since D is strongly connected, there is at least one arc into vertex 5. Since there is no 2-cycle, the arcs $2 \to 5$ and $4 \to 5$ cannot exist. Now if $1 \to 5$ exists, then $1 \to 5 \to 4 \to 3 \to 2 \to 1$ is a 5-cycle, and if $3 \to 5$ exists, then $3 \to 5 \to 2 \to 1 \to 4 \to 3$ is a 5-cycle, both of which are contradictions. This implies that there are no arcs into vertex 5, which contradicts the strongly connectivity of digraph D. Therefore, there are no outgoing arcs from vertex 5 to nonadjacent vertices

on the 4-cycle. Thus, there is an arc from vertex 5 to at most two adjacent vertices on the 4-cycle; without loss of generality suppose $5 \to 2$ and $5 \to 3$ are such arcs. Now since there is no 2-cycle, the only arcs into vertex 5 can be $1 \to 5$ and $4 \to 5$; see Figure A.2.

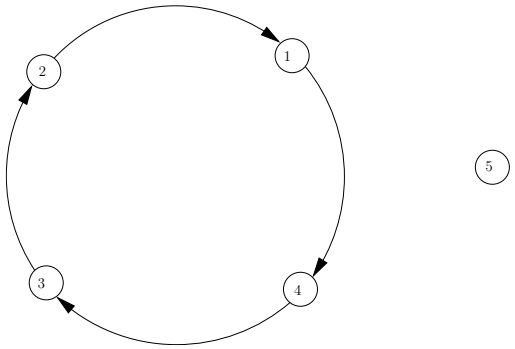

Figure A.1:

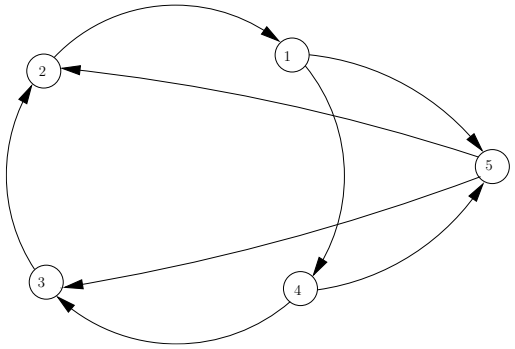

Figure A.2:

If $1 \to 5$ and $4 \to 5$ are both arcs of the digraph in Figure A.2, then $1 \to 4 \to 5 \to 3 \to 2 \to 1$ is a 5-cycle, which is a contradiction. So only one of the arcs $1 \to 5$ or $4 \to 5$ can exist. Without loss of generality, consider

the arc $1 \to 5$ in digraph D as in Figure A.3.

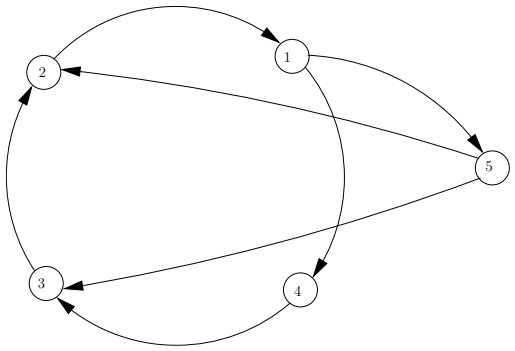

Figure A.3: $n = 5, k = 4, j = 3, \gamma = 11 > \alpha_5 = 10$

By adding $1 \to 3$ or $3 \to 1$ (not both) to the digraph in Figure A.3, the digraph still has only cycles of lengths 3 and 4, and the exponent is $10 = \alpha_5$ or $9 < \alpha_5$, respectively; see Figures A.4 and A.5. By adding $2 \to 4$ or $4 \to 2$ (not both) to the digraph in Figure A.3, the digraph still has only cycles of lengths 3 and 4 and the exponent is 10; see Figures A.6 and A.7.

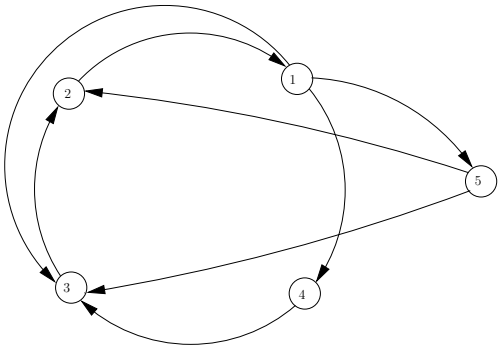

Figure A.4: $\gamma = 10 = \alpha_5$, number of arcs$= 8 = n + 3$

The above analysis implies that the digraphs in Figures A.4, A.5, A.6 and

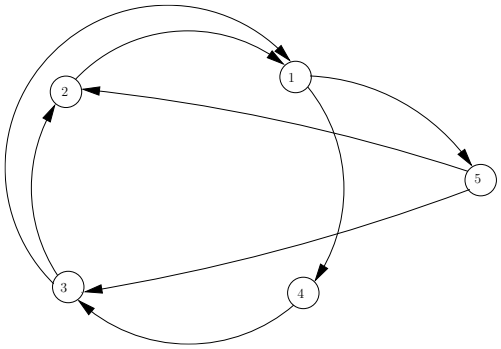

Figure A.5: $\gamma = 9 < \alpha_5$

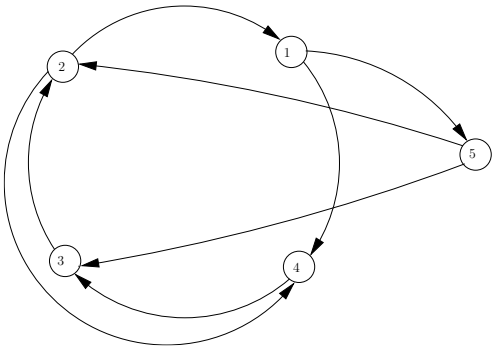

Figure A.6: $\gamma = 10 = \alpha_5$, number of arcs$= 8 = n + 3$

A.7 (which have $n + 3$ arcs) and some of their subdigraphs are the only possible primitive digraphs with large exponent on 5 vertices with cycle lengths $k = 4$ and $j = 3$. Note that no subdigraph of A.3 can have an exponent < 11. We now consider which subdigraphs of these primitive digraphs are also primitive with large exponent, and are nonisomorphic to the previous digraphs.

1) Three subdigraphs of the digraph in Figure A.4 are still primitive, and two of them have exponent α_5 with $n+2 = 7$ arcs; the other one is isomorphic

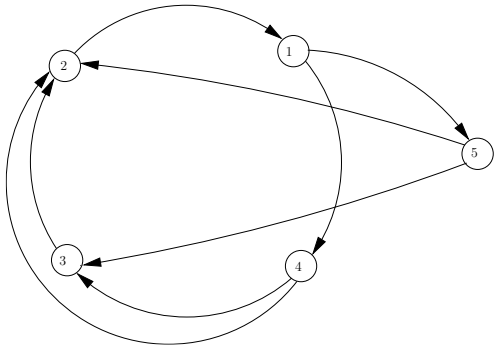

Figure A.7: $\gamma = 10 = \alpha_5$, number of arcs$= 8 = n + 3$

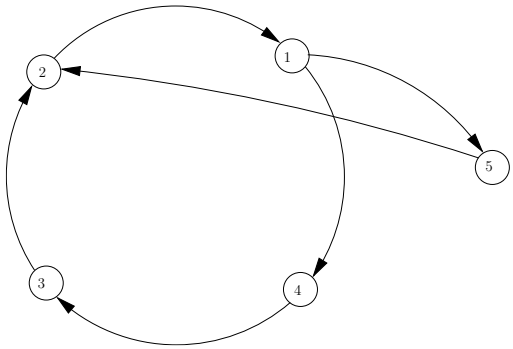

Figure A.8: $\gamma = 11$

to the digraph in Figure A.3. Deletion of one arc $5 \rightarrow 2$, $5 \rightarrow 3$ or $1 \rightarrow 3$ results in the digraph in Figure A.9, A.10 or A.3, respectively. Deletion of any other arc results in a digraph that is not strongly connected.

2) Two subdigraphs of the digraph in Figure A.5 are primitive, with exponent equal to α_5 and $n + 2 = 7$ arcs and are nonisomorphic to the previous digraphs. Deletion of one arc $5 \rightarrow 2$ or $5 \rightarrow 3$ results in the digraphs in Figure A.11 or A.12, respectively. Deletion of any other arcs results in a digraph that is isomorphic to either the digraph in Figure A.3 or A.4.

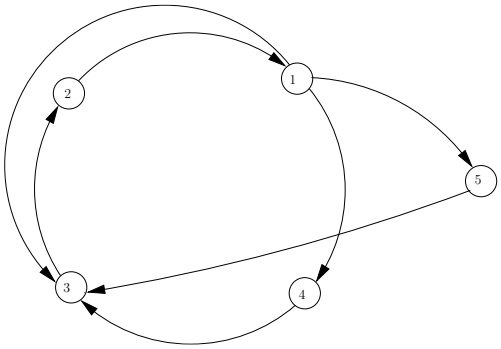

Figure A.9: $\gamma = 10 = \alpha_5$, number of arcs$= 7 = n + 2$

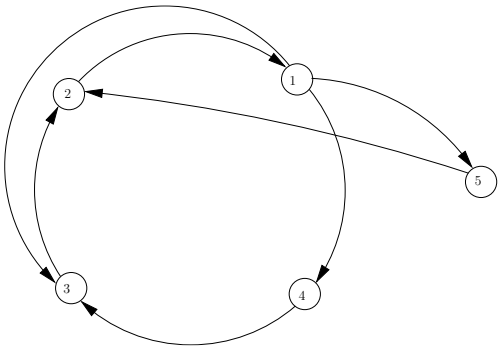

Figure A.10: $\gamma = 10 = \alpha_5$, number of arcs$= 7 = n + 2$

3) Figure A.14 contains a subdigraph of the digraph in Figure A.6 that is nonisomorphic to previous digraphs, has exponent α_5 and $n + 2 = 7$ arcs. Deletion of one arc $5 \to 2$, $5 \to 3$ or $1 \to 4$ in Figure A.6 gives the digraph in Figures A.13, A.14 or A.15, respectively. The digraph in Figure A.15 is isomorphic to the digraph in Figure A.12. Deletion of any other arcs results in a digraph isomorphic to that in either Figure A.3 or A.4.

4) The digraph in Figure A.7 has two subdigraphs with exponent α_5 and $n + 2 = 7$ arcs and two other subdigraphs with large exponent. If the arc

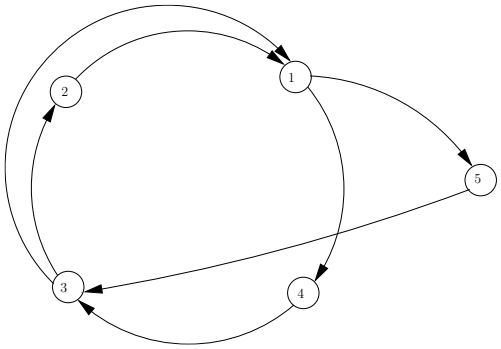

Figure A.11: $\gamma = 10 = \alpha_5$, number of arcs$= 7 = n + 2$

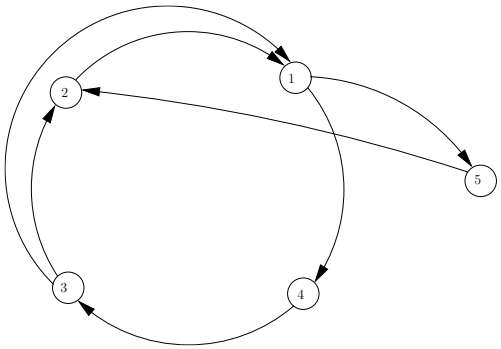

Figure A.12: $\gamma = 10 = \alpha_5$, number of arcs$= 7 = n + 2$

$5 \to 2$ is deleted, then the result is the digraph in Figure A.16, which is isomorphic to the digraph in Figure A.3. If the arc $5 \to 3$ or $4 \to 3$ is deleted, then the result is the digraph in Figure A.17 or A.18, respectively; these digraphs are isomorphic. If the arc $5 \to 2$ is deleted from the digraph in Figure A.18, then the result is as in Figure A.19, which is isomorphic to the digraph in Figure A.8.

Therefore, there are three primitive digraphs (up to isomorphism) on $n = 5$ vertices with cycle lengths $k = 4$ and $j = 3$ and exponent equal to 11;

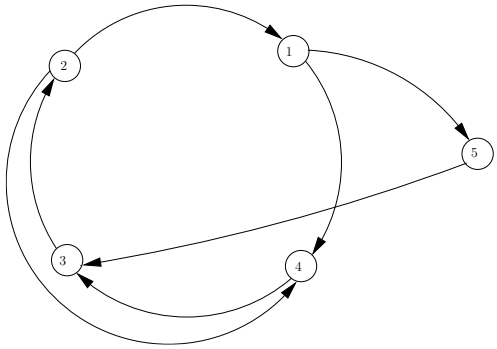

Figure A.13: $\gamma = 11$

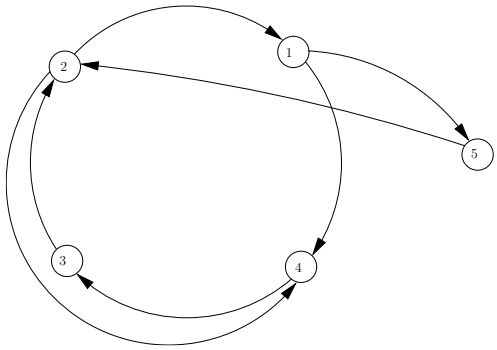

Figure A.14: $\gamma = 10 = \alpha_5$, number of arcs$= 7 = n + 2$

see Figures A.3, A.8 and A.13. There are nine such primitive digraphs with exponent $10 = \alpha_5$; see Figures A.4, A.6, A.7, A.9, A.10, A.11, A.12, A.14 and A.17. The digraphs in Figures A.4, A.6 and A.7 have $8 = n+3$ arcs and the remaining digraphs have $7 = n + 2$ arcs.

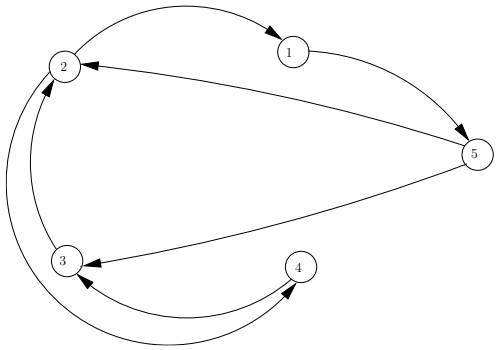

Figure A.15: $\gamma = 10 = \alpha_5$, number of arcs$= 7 = n + 2$

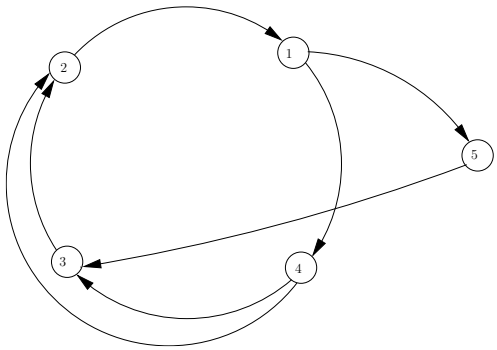

Figure A.16: $\gamma = 11$

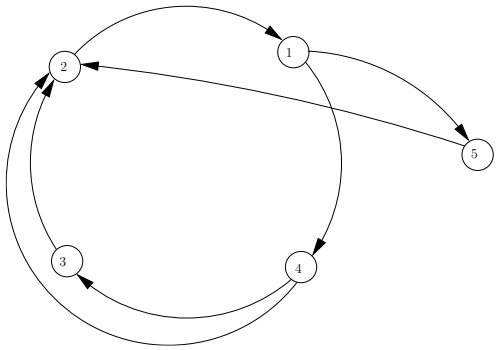

Figure A.17: $\gamma = 10 = \alpha_5$, number of arcs$= 7 = n + 2$

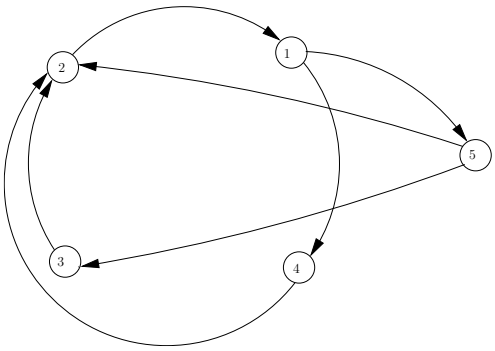

Figure A.18: $\gamma = 10 = \alpha_5$, number of arcs$= 7 = n + 2$

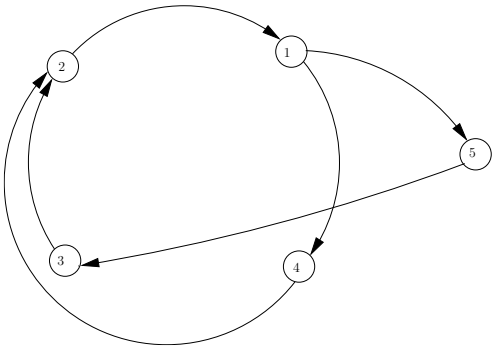

Figure A.19: $\gamma = 11$

Appendix B

Digraphs $W(n, k, j)$ with exponent α_n

The following list gives values of n, k, j for which there exists a digraph $W(n, k, j)$ with exponent α_n. These results, ordered by n, are obtained by executing programs in Maple for even $n \leq 1264$ and odd $n \leq 1551$. Note that for $n = 933$, there exist two different values of k and j giving two different digraphs, namely $W(933, 691, 629)$ and $W(933, 903, 481)$. Execution of this program for sufficiently large values of n, shows that $n = 933$ is the smallest n for which k and j are not unique.

n	k	j
6	5	3
16	13	9
26	19	17
34	29	19
54	43	33
60	53	33
72	59	43
84	61	57
116	99	67
136	125	73
140	109	89
142	101	99
186	173	99
190	139	129
196	155	123
202	179	113
230	189	139
236	211	131
244	229	129
250	203	153
274	211	177
282	221	179
306	221	211
310	293	163
312	283	171
318	269	187
344	253	233
354	323	193
384	365	201
412	299	283
446	411	241
448	389	257
456	349	297
466	445	243
480	341	337
498	395	313
502	389	323
508	419	307
546	403	369
556	533	289
588	475	363
604	563	323
636	491	411
640	539	379
654	629	339
662	619	353
672	491	459
686	523	449
738	661	411
744	659	419
760	733	393
786	739	417
796	589	537
808	581	561
810	701	467
818	579	577
826	605	563
846	755	473
874	845	451
890	805	491
906	749	547
924	749	569
928	725	593
952	731	619
960	763	603
964	733	633
978	851	561
992	939	523
996	965	513
1028	813	649
1082	909	643
1086	875	673
1094	811	737
1098	781	771
1100	1005	601
1122	923	681
1126	1093	579
1134	869	739
1136	819	787
1150	1043	633
1152	973	681
1158	1019	657
1202	1035	697
1222	1163	641
1262	1021	779
1264	1229	649

n	k	j
9	7	5
23	19	13
43	31	29
45	39	25
75	67	41
85	67	53
113	103	61
121	99	73
125	91	85
159	147	85
187	159	109
195	151	125
213	199	113
239	207	137
241	171	169
255	187	173
275	259	145
307	243	193
329	291	185
339	279	205
345	327	181
353	271	229
379	307	233
397	355	221
433	319	293
449	379	265
487	351	337
509	487	265
511	463	281
559	427	365
595	543	325
603	579	313
657	571	377
659	487	445
665	567	389
677	559	409
689	547	433
695	567	425
705	679	365
719	511	505
733	675	397
769	663	445

n	k	j
797	643	493
807	711	457
809	627	521
813	619	533
815	787	421
831	699	493
833	771	449
933	691	629
933	903	481
995	927	533
1059	1027	545
1069	907	629
1077	831	697
1079	967	601
1111	1039	593
1115	847	733
1129	811	785
1135	939	685
1145	903	725
1159	1027	653
1193	1159	613
1231	979	773
1255	931	845
1269	1147	701
1299	1131	745
1333	1119	793
1335	1299	685
1349	1107	821
1375	1107	853
1377	1075	881
1381	1195	797
1395	987	985
1397	1023	953
1429	1347	757
1465	1111	965
1469	1191	905
1477	1051	1037
1479	1263	865
1485	1447	761
1489	1167	949
1509	1327	857
1551	1191	1009

Bibliography

[1] T. A. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, 1976.

[2] R.A. Brualdi, and H. J. Ryser, *Combinatorial Matrix Theory*, Cambridge University Press, 1991.

[3] L.F. Dame, The Exponent and Circumdiameter of Primitive Directed Graphs, M.Sc. thesis, Department of Mathematics and Statistics, University of Victoria (2004).

[4] L.F. Dame, D. Olesky and P. van den Driessche, The exponent and circumdiameter of primitive digraphs, *Lin. Alg. Appl.* **396** (2005), 243 – 258.

[5] A. L. Dulmage and N. S. Mendelsohn, Gaps in the exponent set of primitive matrices, *Illinois Journal of Mathematics* **8** (1964), 642– 656.

[6] O. Frink, Almost pythagorean triples, *Mathematics Magazine* **60** (1987), 234 – 236.

[7] R. A. Horn, and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, 1985.

[8] B. M. Kim, B. C. Song and W. Hwang, Nonnegative primitive matrices with exponent 2, *Lin. Alg. Appl.* **407** (2005), 162 – 168.

[9] B. M. Kim, B. C. Song and W. Hwang, Primitive graphs with given exponents and minimum number of edges, *Lin. Alg. Appl.* **420** (2007), 648 – 662.

[10] S. Kirkland, A note on the eigenvalues of a primitive matrix with large exponent, *Lin. Alg. Appl.* **253** (1997), 103 – 112.

[11] S. Kirkland, D. Olesky and P. van den Driessche, Digraphs with large exponent, *Lin. Alg. Appl.* **364** (2003), 243 – 251.

[12] M. Lewin and Y. Vitek, A system of gaps in the exponent set of primitive matrices, *Illinois J. Math.*, **25** (1981), 87–98.

[13] B. Liu, B. D. McKay, N. C. Wormald and K. Zhang, The exponent set of symmetric primitive $(0, 1)$ matrices with zero trace, *Lin. Alg. Appl.* **133** (1990), 121 – 131.

[14] I. Niven and H.S. Zuckerman, *An Introduction To The Theory Of Numbers*, John Wiley & Sons, 1979.

[15] J. Rosiak, The minimum exponent of the primitive digraphs on the given number of arcs, *Opuscula Mathematica* **24/2** (2004), 197 – 202.

[16] H. Schneider, Wielandt's proof of the exponent inequality for primitive nonnegative matrices, *Lin. Alg. Appl.* **353** (2002), 5 – 10.

[17] J. Shen, C. J. Wyels, On the number of arcs in primitive digraphs with large exponents, *Lin. Alg. Appl.* **364** (2003), 243 – 251.

[18] H. Wielandt, Unzerlegbare, nicht negative Matrizen, *Math. Zeit*, **52** (1950), 642–645.