PROPERTIES OF SOME ALGEBRAICALLY DEFINED DIGRAPHS

by

Aleksandr Kodess

A dissertation submitted to the Faculty of the University of Delaware in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Mathematics

Summer 2014

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

PROPERTIES OF SOME ALGEBRAICALLY DEFINED DIGRAPHS

by

Aleksandr Kodess

Approved: _____
John Pelesko, Ph.D.
Chair of the Department of Mathematical Sciences

Approved: _____
George H. Watson, Ph.D.
Dean of the College of Arts and Sciences

Approved: _____
James G. Richards, Ph.D.
Vice Provost for Graduate and Professional Education

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Felix Lazebnik, Ph.D.
Professor in charge of dissertation

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Sebastian Cioabă, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Robert Coulter, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Jason Williford, Ph.D.
Member of dissertation committee

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor Felix Lazebnik without whom some of this would not have been finished by this time. He was invaluable in the completion of this thesis. His advice has always been and, I hope, will be of great value to me.

Many thanks go to my committee members Sebastian Cioabă and Robert Coulter from the University of Delaware and Jason Williford from the University of Wyoming for their helpful comments.

I also thank Gary Ebert from whom I took my first course in abstract algebra, Sebastian from whom I took a number of courses in combinatorics, and, of course, Felix from whom I took courses in various areas for their important contribution to my education here at Delaware.

Last but not least, I would like to thank my parents Mikhail and Irina and my brother Evgeniy for their continual love and support, especially throughout my stay at the University of Delaware.

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

This thesis is concerned with the study of a family of digraphs defined by systems of polynomial equations over finite fields. We explore the connectivity and diameter of some special classes of these digraphs, along with the structure of their isomorphism classes.

Chapter 1

INTRODUCTION

1.1 Notation and Terminology

First we will present the basic terminology and notation that will be used throughout the thesis. A *directed graph* (or just *digraph*) D consists of a non-empty finite set $V(D)$ of elements called *vertices* and a finite set $A(D)$ of ordered pairs of vertices called *arcs*. We call $V(D)$ the *vertex set* and $A(D)$ the *arc set* of D. We will often write $D = (V, A)$, which means V and A are the vertex set and arc set of D, respectively. The *order* (*size*) of D is the number of vertices (arcs) in D; the order of D will sometimes be denoted by $|D|$.

For an arc (u, v) the first vertex u is called its *tail* and the second vertex v is called its *head*. The head and tail of an arc are its *end-vertices*; we say that u is adjacent *to* v if (u, v) is an arc in G. We say that a vertex is *incident* to an arc if the vertex is the head or tail of the arc. We will often denote an arc (x, y) by xy. An arc in which its tail coincides with its head is called a *loop*.

For a vertex v in D , we consider the following two sets:

$$N^+(v) = \{u \in V : vu \in A\} \text{ and } N^-(v) = \{w \in V : wv \in A\}.$$

The sets $N^+(v)$, $N^-(v)$ and are called the *out-neighborhood* and *in-neighborhood* of v, and we call the vertices in $N^+(v)$ and $N^-(v)$ the *out-neighbors* and the *in-neighbors* of v, respectively. The cardinalities of $N^+(v)$ and $N^-(v)$ are denoted by $d^+(v)$ and $d^-(v)$, respectively, and are called the *out-degree* and *in-degree* of v. Every loop contributes one to the count of both the out-degree and the in-degree of a vertex. A digraph is called *k-regular* if out-degrees and in-degrees of all vertices are equal to k.

A digraph H is a *subdigraph* of a digraph D if $V(H) \subseteq V(D)$ and $A(H) \subseteq A(D)$. If, in addition, every arc of $A(D)$ with both end-vertices in $V(H)$ is in $A(H)$, we call H an *induced* subdigraph of D.

By *reversing the arc* xy in a digraph D, we mean that we replace the arc xy by the arc yx. The *converse* of a digraph D is the digraph H which one obtains from D by reversing all arcs.

A digraph D is called *isomorphic* to a digraph H (denoted by $D \cong H$) if there exists a bijection $\phi : V(D) \to V(H)$ such that $xy \in A(D)$ if and only if $\phi(x)\phi(y) \in A(H)$. The mapping ϕ is called an *isomorphism* from D to H. Clearly, isomorphism is an equivalence relation on the set of all digraphs.

Let $k \geq 2$. A *walk* W *from* x_1 *to* x_k in D is an alternating sequence $W = x_1a_1x_2a_2x_3 \ldots x_{k-1}a_{k-1}x_k$ of vertices x_i and arcs a_j from D such that the tail of a_i is x_i and the head of a_i is x_{i+1} for every i, $1 \leq i \leq k-1$. The *length* of a walk is the number of its arcs. If $k \geq 2$ and the vertices $x_1, x_2, \ldots, x_{k-1}$ of the walk W are distinct, and $x_1 = x_k$, W is called a *cycle*. A *k-cycle* is a cycle of length k. A loop also can be called a 1-cycle.

In a digraph D a vertex y is *reachable* from a vertex x if D has a walk from x to y. In particular, a vertex is reachable from itself. A digraph D is *strongly connected* (or, just *strong*) if, for every pair x, y of distinct vertices in D, y is reachable from x and x is reachable from y. In other words, D is strong if every vertex of D is reachable from every other vertex of D. We define a digraph with one vertex to be strongly connected. A *strong component* of a digraph D is a maximal induced subdigraph of D which is strong. If $D_1, \ldots, D_t$ are the strong components of D, then their vertex sets and arc sets partition those of D, respectively. If x and y are vertices of a digraph D, then the *distance from* x *to* y in D, denoted $\mathrm{dist}(x, y)$, is the minimum length of an (x, y)-walk, if y is reachable from x, and otherwise $\mathrm{dist}(x, y) = \infty$. The *distance from a set* X *to a set* Y of vertices in D is

$$\mathrm{dist}(X, Y) = \max\{\mathrm{dist}(x, y) \colon x \in X, y \in Y\}.$$

The *diameter* of D is $\mathrm{diam}(D) = \mathrm{dist}(V, V)$.

For all missing definitions, see Bang-Jensen and Gutin [1].

1.2 The General Construction

In the following, and in all subsequent chapters, q will always represent a prime power, i.e. $q = p^e$ for some prime p and $e \geq 1$. The finite field of q elements will be denoted by $\mathbb{F}_q$. The cartesian product of k copies of $\mathbb{F}_q$ will be denoted by $\mathbb{F}_q^k$. Clearly, $\mathbb{F}_q^k$ is a vector space of dimension k over $\mathbb{F}_q$ and of dimension ke over $\mathbb{F}_p$.

Let $f_i \colon \mathbb{F}_q^2 \to \mathbb{F}_q$ be arbitrary functions, where $1 \leq i \leq l$, i and l are positive integers. The digraph $D = D(q; f_1, \ldots, f_l)$ or, just, $D(q; \mathbf{f})$, where $\mathbf{f} = (f_1, \ldots, f_l) \colon \mathbb{F}_q^2 \to \mathbb{F}_q^l$, is defined as follows. The vertex set of D is $\mathbb{F}_q^{l+1}$. There is an arc from a vertex $\mathbf{x} = (x_1, \ldots, x_{l+1})$ to a vertex $\mathbf{y} = (y_1, \ldots, y_{l+1})$ if

$$x_i + y_i = f_{i-1}(x_1, y_1), \quad \text{for all } i,\ 2 \leq i \leq l+1. \tag{1.1}$$

By convention, $\mathbf{f}(x, y) = (f_1(x, y), \ldots, f_l(x, y))$. We will refer to the functions $f_1, \ldots, f_l$ as *defining functions*. When $l = 1$, we will write $D(q; f)$, where $f = f_1$. If, moreover, $f_1(x, y) = x^m y^n$ for some integers $1 \leq m, n \leq q-1$, the corresponding digraph will be denoted by $D(q; m, n)$ and will be called a *monomial* digraph. Since $x^q = x$ for every $x \in \mathbb{F}_q$, it will be always assumed that for monomial digraphs $1 \leq m, n \leq q-1$.

The following proposition is true.

Proposition 1.2.1. *The digraph $D = D(q; f_1, \ldots, f_l)$ is q-regular, with order q^{l+1} and size q^{l+2}.*

Proof. The incidence condition (1.1) implies that an out-neighbor (in-neighbor) $\mathbf{y}$ of a vertex $\mathbf{x}$ is defined uniquely by its first coordinate y_1. By construction, $|D| = q^{l+1}$, and the size of D is q^{l+2}. □

Remark 1.2.2. These graphs can be easily constructed by computer. I have used the computer algebra package `sage` extensively for this thesis, in addition to `Mathematica` and `Magma`.

1.3 History, Motivation, Applications

The main motivation for the work in this thesis was the work of Lazebnik, Woldar [21], Viglione [27] and Dmytrenko, Lazebnik, Viglione [10]. The central objects of study in [27] are undirected bipartite graphs constructed in the following way. Let P_n and L_n be two n-dimensional vector spaces over $\mathbb{F}_q$. Elements of P_n are called *points*, and elements of L_n are called *lines*. If $a \in \mathbb{F}_q^n$ we write (a) for points and $[a]$ for lines. Let $f_i \colon \mathbb{F}_q^{2i-2} \to \mathbb{F}_q$ be arbitrary functions for $i \geq 2$; they are called *incidence functions*. The bipartite graph $B\Gamma_n = B\Gamma_n(q; f_2, \ldots, f_n)$ has P_n and L_n as its partitions sets, and a point $(p) = (p_1, p_2, \ldots, p_n)$ is adjacent to a line $[l] = [l_1, l_2, \ldots, l_n]$ if and only if the following $n-1$ relations on their coordinates hold:

$$\begin{aligned} l_2 + p_2 &= f_2(p_1, l_1), \\ l_3 + p_3 &= f_3(p_1, l_1, p_2, l_2), \\ &\vdots \\ l_n + p_n &= f_n(p_1, l_1, p_2, l_2, \ldots, p_{n-1}, l_{n-1}). \end{aligned}$$

Properties of these graphs are studied in [21]. We present some of them here.

Define an *edge-decomposition* of a graph G by a graph G' as a collection $\mathcal{C}$ of subgraphs of G, each isomorphic to G', such that $\{E(H) \colon H \in \mathcal{C}\}$ is a partition of $E(G)$. If such a collection exists, then we say that G' *decomposes* G. For any positive integers a, b, by $K_{a,b}$ we denote the complete bipartite graph with partitions sets of size a and b. The following property is proved in [21].

Proposition 1.3.1. *The graph $B\Gamma_n$ decomposes K_{q^n,q^n}.*

In [21], similar non-bipartite graphs $\Gamma_n = \Gamma(q; f_2, \ldots, f_n)$ are defined. Let $f_i \colon \mathbb{F}_q^{2i-2} \to \mathbb{F}_q$ be symmetric for all i, $2 \leq i \leq n$, in the following sense:

$$f_i(p_1, l_1, p_2, l_2, \ldots, p_{i-1}, l_{i-1}) = f_i(l_1, p_1, l_2, p_2, \ldots, l_{i-1}, p_{i-1})$$

for all i. The vertex set $V(\Gamma_n) = \mathbb{F}_q^n$, where distinct vertices (vectors) $a = \langle a_1, a_2, \ldots, a_n \rangle$ and $b = \langle b_1, b_2, \ldots, b_n \rangle$ are adjacent if and only if the following $n-1$ relations on their coordinates hold:

$$\begin{aligned} a_2 + b_2 &= f_2(a_1, b_1), \\ a_3 + b_3 &= f_3(a_1, b_1, a_2, b_2), \\ &\vdots \\ a_n + b_n &= f_n(a_1, b_1, a_2, b_2, \ldots, a_{n-1}, b_{n-1}). \end{aligned}$$

For the graphs Γ_n, the requirement that all functions f_i be symmetric is necessary to ensure that the adjacency relation is symmetric. Without this condition one obtains not graphs, but digraphs which are a generalization of those studied in this thesis.

A statement similar to that of Proposition 1.3.1 is also proved in [21]:

Proposition 1.3.2. *The graph* $\Gamma(q; f_2, \ldots, f_n)$ *decomposes* K_{q^n}.

Propositions 1.3.1 and 1.3.2 were generalized in [18] to edge-decompositions of complete uniform q-partite hypergraphs and complete uniform hypergraphs, respectively.

The graphs $B\Gamma_n$ and Γ_n defined by systems of equations have proven useful in a number of extremal type problems. We briefly mention some of them here: see [21] for more.

Let $\mathcal{F}$ be a family of graphs. By $ex(v, \mathcal{F})$ we denote the Turán number of $\mathcal{F}$, that is, the greatest number of edges in a graph with v vertices which contains no subgraph isomorphic to a graph from $\mathcal{F}$. Let C_n denote the cycle of length $n \geq 3$. The best bounds on $ex(v, \{C_3, C_4, \ldots, C_{2k}\})$ for an arbitrary fixed k, $2 \leq k \neq 5$, obtained in Bondy, Simonovits [3], Verstraëte [26], Pikhurko [23], and recently by Bukh and Jiang [6] (for $v \geq (2k)^{8k^2}$) and Lazebnik, Ustimenko, Woldar [20] (the lower bound), are the following:

$$c_k v^{1+\frac{2}{3k-3+\epsilon}} \leq ex(v, \{C_3, C_4, \ldots, C_{2k}\}) \leq 80\sqrt{k \log k} \cdot v^{1+1/k} + 10k^2 v. \tag{1.2}$$

Here $c_k = 2^{-1-\frac{2}{3k-3}}$ and $\epsilon = 0$ if k is odd, and $c_k = 2^{-1-\frac{2}{3k-2}}$ and $\epsilon = 1$ if k is even.

The lower bound comes from the following construction introduced in Lazebnik, Ustimenko [19]. Consider the family of graphs $D(n,q) = G^q_{f_2,\dots,f_n}$, where $f_2 = p_1 l_1$, $f_3 = p_1 l_2$, and for $4 \le i \le n$,

$$f_i = \begin{cases} -p_{i-2} l_1 & i \equiv 0 \text{ or } 1 \mod 4, \\ p_1 l_{i-2} & i \equiv 2 \text{ or } 3 \mod 4. \end{cases}$$

It was shown in [19] that the length of the shortest cycle in $D(n,q)$ is at least $n+5$. By the result of [20], the graphs $D(n,q)$ are disconnected for $n \ge 6$ and the lower bound in (1.2) comes from their components.

1.4 Synopsis of the Thesis

We now briefly describe what has been accomplished in this thesis.

A large part of this thesis is concerned with understanding the connectivity of digraphs $D(q;\mathbf{f})$. The main motivation for this is the work of Viglione [27]. It is natural to try to see if there is a general method for determining the number of strong components and their structural properties of these digraphs by examining their defining functions. We address this question in Chapter 2, giving sufficient conditions for some class of digraphs $D(q;\mathbf{f})$ to be strong in terms of a certain property of the range of the defining function $\mathbf{f}$. This is done in Theorem 2.1.3 and Theorem 2.1.7. We further specialize the problem to the monomial digraph $D(q;m,n)$ as in this case our result takes on an especially simple form. The main results concerning the strong connectivity of monomial digraphs are Theorem 2.2.1 and Theorem 2.2.2. A relation between the problem of determining the diameter of monomial digraphs and some recent results in additive combinatorics is established.

Motivated by results of Viglione [27] and Dmytrenko, Lazebnik, Viglione [10], in Chapter 3 we study the question of isomorphism for monomial digraphs. In [27] it was shown that for all sufficiently large prime powers q the number of directed 4-cycles completely determines the isomorphism class of bipartite monomial graphs, while in [10] it was proved that for any prime power q there exists a complete bipartite

graph $K_{s,t}$ such that the number of subgraphs isomorphic to it is a graph invariant which determines the isomorphism class of undirected bipartite monomial graphs. For our monomial digraphs the matter seems to be more complicated. As of now we have not arrived to any one subdigraph which defines an isomorphism class. Our main Conjecture 3.7.1 is based on considering several digraph invariants. We prove the sufficiency of the conjecture in Theorem 3.1.1 and its necessity, under additional assumptions, in Theorem 3.7.1.

Chapter 2

AN EXPLORATION OF CONNECTIVITY AND DIAMETER

In this chapter we will examine some connectivity results for our algebraically defined digraphs. Noting that any function $f\colon \mathbb{F}_q^2 \to \mathbb{F}_q$ can be written as a polynomial in two variables by using Lagrange interpolation, we will always assume any function f is written as a sum of monomial terms, with all exponents taken mod q (since $a^q = a$ for all $a \in \mathbb{F}_q$). We define a *mixed monomial term* as taking the form Cx^iy^j, with $i, j > 0$, C constant. The portion of f which is a sum of only mixed monomial terms will be denoted by f^*. We first present a general criterion on the strong connectivity of the digraph $D(q; \mathbf{f})$ in case when all the defining functions can be represented by bivariate polynomials which contain mixed terms only. Then the results are specialized for the digraph $D(q; m, n)$, and the diameters of such digraphs are studied. It turns out the latter is related to Waring's problem over finite fields, which is considered now as part of additive combinatorics.

2.1 Connectivity of $D(q; \mathbf{f})$

The ideas of this section go back to similar studies of undirected bipartite graphs in [27]. The main results of this section are Theorem 2.1.3 and Theorem 2.1.7, which provide sufficient conditions for strong connectivity of the general digraph $D(q; \mathbf{f})$ for any prime power q.

When studying connectivity of our digraphs the following notion is of great importance.

Definition 2.1.1. For any vector function $\mathbf{f} = (f_1, \ldots, f_l)$, l a positive integer, $f_i \colon \mathbb{F}_q^2 \to \mathbb{F}_q$ for every i, $1 \leq i \leq l$, any positive integer $k \geq 2$ and any k-tuple $(x_1, \ldots, x_k) \in \mathbb{F}_q^k$ we call the sum

$$\mathbf{f}(x_1, x_2) - \mathbf{f}(x_2, x_3) + \cdots + (-1)^{k-1}\mathbf{f}(x_{k-1}, x_k)$$

a *linked alternating sum* of $\mathbf{f}$ of *length* $k-1$. Let $LS_k(\mathbf{f})$ be the set of all possible linked alternating sums of $\mathbf{f}$ of *length* $k-1$, and let

$$LS(\mathbf{f}) := \bigcup_{k \geq 2} LS_k(\mathbf{f}).$$

We call $LS(\mathbf{f})$ the set of *linked alternating sums* of $\mathbf{f}$.

In the following, if $X \subseteq \mathbb{F}_q^l$, where q is a power of some prime p, $\langle X \rangle$ will denote the span of X in $\mathbb{F}_q^l$ with coefficients from $\mathbb{F}_p$. The dimension $\dim\langle X \rangle$ of $\langle X \rangle$ will always be taken over $\mathbb{F}_p$. If X is empty, we define $\dim\langle X \rangle$ to be zero.

For $X, Y \subseteq \mathbb{F}_q^l$ and $\mathbf{v} \in \mathbb{F}_q^l$ we define $X + Y := \{\mathbf{x} + \mathbf{y} \colon \mathbf{x} \in X, \mathbf{y} \in Y\}$. If $X = \{\mathbf{v}\}$, instead of $\{\mathbf{v}\} + Y$ we will write $\mathbf{v} + Y$.

For any function $\mathbf{f} \colon \mathbb{F}_q^2 \to \mathbb{F}_q^l$, we define the image of $\mathbf{f}$ to be

$$\mathrm{Im}(\mathbf{f}) := \{(f_1(x, y), \ldots, f_l(x, y)) \colon x, y \in \mathbb{F}_q\}.$$

We observe the following

Lemma 2.1.1. *Let q be an odd prime power, and $\mathbf{f} \colon \mathbb{F}_q^2 \to \mathbb{F}_q^l$. Let $\mathbf{g}(x) = \mathbf{f}(x, 0)$, $\mathbf{h}(x) = \mathbf{f}(0, x)$, $\mathbf{f}_0(x, y) = \mathbf{f}(x, y) - \mathbf{f}(0, 0)$, and $\mathbf{f}^*(x, y) = \mathbf{f}_0(x, y) - \mathbf{g}(x) - \mathbf{h}(y)$ for all $x, y \in \mathbb{F}_q$. The following statements hold:*

(i) $D(q; \mathbf{f}) \cong D(q; \mathbf{f}_0)$.

(ii) If, in addition, $\mathbf{g} = \mathbf{h}$, *then*

$$D(q; \mathbf{f}) \cong D(q; \mathbf{f}_0) \cong D(q; \mathbf{f}^*).$$

Proof. (i) The map $\phi \colon V(D(q; \mathbf{f}))) \to V(D(q; \mathbf{f}_0)))$ given by

$$(x, \mathbf{y}) \mapsto (x, \mathbf{y} - \frac{1}{2}\mathbf{f}(0, 0))$$

is clearly a bijection. We check that ϕ preserves adjacency and non-adjacency. Assume that $\Big((x_1, \mathbf{x}_2), (y_1, \mathbf{y}_2)\Big) \in E(D(q; \mathbf{f}))$, that is, $\mathbf{x}_2 + \mathbf{y}_2 = \mathbf{f}(x_1, y_1)$. Then, since $\phi((x_1, \mathbf{x_2})) = (x_1, \mathbf{x}_2 - \frac{1}{2}\mathbf{f}(0,0))$ and $\phi((y_1, \mathbf{y_2})) = (y_1, \mathbf{y}_2 - \frac{1}{2}\mathbf{f}(0,0))$, we have

$$\Big(\mathbf{x}_2 - \frac{1}{2}\mathbf{f}(0,0)\Big) + \Big(\mathbf{y}_2 - \frac{1}{2}\mathbf{f}(0,0)\Big) = \mathbf{f}(x_1, y_1) - \mathbf{f}(0,0) = \mathbf{f}_0(x_1, y_1),$$

and so $\Big(\phi((x_1, \mathbf{x}_2)), \phi((y_1, \mathbf{y}_2))\Big) \in E(D(q; \mathbf{f}_0))$. Thus, $D(q; \mathbf{f}) \cong D(q; \mathbf{f}_0)$, and the proof of (i) is complete.

(ii) Define $\psi \colon V(D(q; \mathbf{f}_0)) \to V(D(q; \mathbf{f}^*))$ by $(x, \mathbf{y}) \mapsto (x, \mathbf{y} - \mathbf{g}(x))$. Trivially, ψ is a bijection, and so we check that ψ preserves adjacency and non-adjacency. Assume that $\Big((x_1, \mathbf{x}_2), (y_1, \mathbf{y}_2)\Big) \in E(D(q; \mathbf{f}_0))$, that is, $\mathbf{x}_2 + \mathbf{y}_2 = \mathbf{f}_0(x_1, y_1)$. Then, since $\psi((x_1, \mathbf{x_2})) = (x_1, \mathbf{x}_2 - \mathbf{g}(x_1))$ and $\psi((y_1, \mathbf{y_2})) = (y_1, \mathbf{y}_2 - \mathbf{g}(y_1))$, we have

$$\Big(\mathbf{x}_2 - \mathbf{g}(x_1)\Big) + \Big(\mathbf{y}_2 - \mathbf{g}(y_1)\Big) = \mathbf{f}_0(x_1, y_1) - \mathbf{g}(x_1) - \mathbf{h}(x_1) = \mathbf{f}^*(x_1, y_1),$$

and so $\Big(\psi((x_1, \mathbf{x}_2)), \psi((y_1, \mathbf{y}_2))\Big) \in E(D(q; \mathbf{f}^*))$. Thus, $D(q; \mathbf{f}_0) \cong D(q; \mathbf{f}^*)$, and combining this with (i) the proof of (ii) is complete. □

An important class of functions to which Lemma 2.1.1 can be applied is the class of symmetric functions.

Corollary 2.1.2. *Let q be an odd prime power, and $\mathbf{f} \colon \mathbb{F}_q^2 \to \mathbb{F}_q^l$ be a symmetric function, i.e. $\mathbf{f}(x, y) = \mathbf{f}(y, x)$ for all $x, y \in \mathbb{F}_q$. If functions $\mathbf{f}_0$ and $\mathbf{f}^*$ are defined as in Lemma 2.1.1, then $D(q; \mathbf{f}) \cong D(q; \mathbf{f}_0) \cong D(q; \mathbf{f}^*)$.*

Proof. Since the conditions of Lemma 2.1.1, part (i) are satisfied, we have $D(q; \mathbf{f}) \cong D(q; \mathbf{f}_0)$. To conclude that $D(q; \mathbf{f}_0) \cong D(q; \mathbf{f}^*)$, note that since $\mathbf{f}$ is symmetric, so is $\mathbf{f}_0$, and we have $\mathbf{f}_0(x, 0) = \mathbf{g}(x) = \mathbf{f}_0(0, x) = \mathbf{h}(x)$ for any $x \in \mathbb{F}_q$. By Lemma 2.1.1, (ii), $D(q; \mathbf{f}_0) \cong D(q; \mathbf{f}^*)$ as claimed. □

From now on we only consider digraphs $D(q; \mathbf{f})$, for which functions $\mathbf{g}$ and $\mathbf{h}$, defined in Lemma 2.1.1, are equal. As $D(q; \mathbf{f}) \cong D(q; \mathbf{f}^*)$ in this case, we will only

study strong connectivity of $D(q;\mathbf{f}^*)$. The key property of $\mathbf{f}^*$ that will be used later is that

$$\mathbf{f}^*(x,0) = \mathbf{f}^*(0,x)\,(=\mathbf{0}) \tag{2.1}$$

for every $x \in \mathbb{F}_q$. Note that if $\mathbf{f}^* = (f_1^*, \ldots, f_l^*)$, then each f_i^*, $1 \le i \le l$, can be represented by a bivariate polynomial containing only mixed terms.

We now prove main theorems of this section.

Theorem 2.1.3. *Let $p \ge 3$ be a prime, e a positive integer, $q = p^e$, $\mathbf{f}^*\colon \mathbb{F}_q^2 \to \mathbb{F}_q^l$. Let $d = \dim\langle \mathrm{Im}(\mathbf{f}^*)\rangle$. Then,*

(i) the vertex set of the strong component containing some vertex $(u,\mathbf{v}) \in \mathbb{F}_q \times \mathbb{F}_q^l$ of the digraph $D = D(q;\mathbf{f}^*)$ is

$$\Big\{(x, \mathbf{v} + \langle \mathrm{Im}(\mathbf{f}^*)\rangle)\colon x \in \mathbb{F}_q\Big\} \cup \Big\{(x, -\mathbf{v} + \langle \mathrm{Im}(\mathbf{f}^*)\rangle)\colon x \in \mathbb{F}_q\Big\}; \tag{2.2}$$

in particular, D is strong if and only if $\langle \mathrm{Im}(\mathbf{f}^*)\rangle = \mathbb{F}_q^l$ or, equivalently, $d = le$.

(ii) there are $(p^{le-d}+1)/2$ strong components in D. One of them contains vertices of the form $(u,\mathbf{v})$, $u \in \mathbb{F}_q$, $\mathbf{v} \in \langle \mathrm{Im}(\mathbf{f}^*)\rangle$, and is of order p^{e+d}. All other components are of order $2p^{e+d}$;

(iii) all strong components of equal order are isomorphic.

Proof. (i) Let $(u,\mathbf{v}) \in D(q;\mathbf{f}^*)$ be an arbitrary vertex. We show that for every $a \in \mathbb{F}_q$ and every $\mathbf{y} \in \langle \mathrm{Im}(\mathbf{f}^*)\rangle$, $(a, \mathbf{v}+\mathbf{y})$ is reachable from $(u,\mathbf{v})$. Let $\alpha_1, \ldots, \alpha_d \in \mathrm{Im}(\mathbf{f}^*)$ be the elements of a basis of $\langle \mathrm{Im}(\mathbf{f}^*)\rangle$ over $\mathbb{F}_p$. Let $x_i, y_i \in \mathbb{F}_q$ be such that $\mathbf{f}^*(x_i, y_i) = \alpha_i$ for all i, $1 \le i \le d$. Fix an arbitrary $\mathbf{y} \in \langle \mathrm{Im}(\mathbf{f}^*)\rangle$, and write

$$\mathbf{y} = a_1\alpha_1 + \cdots + a_d\alpha_d$$

for some $a_i \in \mathbb{F}_p$, $1 \le i \le d$.

Remembering that $\mathbf{f}^*(x,0) = \mathbf{f}^*(0,x) = \mathbf{f}^*(0,0) = 0$, we consider the following directed walk in $D(q;\mathbf{f}^*)$:

$$\begin{aligned}(u,\mathbf{v}) &\to (0,-\mathbf{v})\\ &\to (0,\mathbf{v}+\mathbf{f}^*(0,0))\\ &\to (x_1,-\mathbf{v}-\mathbf{f}^*(0,0)+\mathbf{f}^*(0,x_1))\\ &\to (y_1,\mathbf{v}+\mathbf{f}^*(0,0)-\mathbf{f}^*(0,x_1)+\mathbf{f}^*(x_1,y_1)\\ &\to (0,-\mathbf{v}-[\mathbf{f}^*(0,0)-\mathbf{f}^*(0,x_1)+\mathbf{f}^*(x_1,y_1)-\mathbf{f}^*(y_1,0)])\\ &= (0,-\mathbf{v}-\alpha_1).\end{aligned} \tag{2.3}$$

Traveling through vertices whose first coordinates are 0, x_1, y_1 and 0 again as many times as needed, one can reach vertex $(0,-\mathbf{v}-a_1\alpha_1)$. Performing the same procedure with x_i and y_i instead of x_1 and y_1, respectively, one can reach vertex

$$(0,-\mathbf{v}-a_1\alpha_1-\cdots-a_i\alpha_i)$$

for any $1 \le i \le d$. Continuing (2.3) we get

$$\begin{aligned}&\to \dots\\ &\to (0,-\mathbf{v}-a_1\alpha_1)\\ &\to \dots\\ &\to (0,-\mathbf{v}-\sum_{i=1}^{d} a_i[\mathbf{f}^*(0,0)-\mathbf{f}^*(0,x_i)+\mathbf{f}^*(x_i,y_i)-\mathbf{f}^*(y_i,0)])\\ &= (0,-\mathbf{v}-\sum_{i=1}^{d} a_i\alpha_i)\\ &\to (a,\mathbf{v}+\sum_{i=1}^{d} a_i\alpha_i) = (a,\mathbf{v}+\mathbf{y}),\end{aligned}$$

and so $(a,\mathbf{v}+\mathbf{y})$ is reachable from $(u,\mathbf{v})$ for any $a \in \mathbb{F}_q$ and any $\mathbf{y} \in \langle \mathrm{Im}(\mathbf{f}^*)\rangle$ as claimed. A similar argument proves that $(a,-\mathbf{v}+\mathbf{y})$ is reachable from $(u,\mathbf{v})$.

The digraph D is strong if and only if $\langle \mathrm{Im}(\mathbf{f}^*)\rangle = \mathbb{F}_q^l$ or, equivalently, $d = le$, and (i) is established.

For (ii), it is trivial to see that for any $\mathbf{v} \in \mathbb{F}_q^l$,

$$\mathbf{v} \in \langle \mathrm{Im}(\mathbf{f}^*)\rangle \Leftrightarrow \mathbf{v} + \langle \mathrm{Im}(\mathbf{f}^*)\rangle = -\mathbf{v} + \langle \mathrm{Im}(\mathbf{f}^*)\rangle,$$

$$\mathbf{v} \notin \langle \mathrm{Im}(\mathbf{f}^*)\rangle \Leftrightarrow \mathbf{v} + \langle \mathrm{Im}(\mathbf{f}^*)\rangle \cap -\mathbf{v} + \langle \mathrm{Im}(\mathbf{f}^*)\rangle = \emptyset.$$

It follows from these two statements that the number of strong components of D is

$$1 + \frac{|\mathbb{F}_q^l/\langle \mathrm{Im}(\mathbf{f}^*)\rangle| - 1}{2} = \frac{p^{\dim(\mathbb{F}_q^l) - \dim\langle \mathrm{Im}(\mathbf{f}^*)\rangle} + 1}{2} = \frac{p^{le-d} + 1}{2}.$$

Furthermore, it follows from part (i) that the component containing any vertex $(u, \mathbf{v})$ with $u \in \mathbb{F}_q$, $\mathbf{v} \in \langle \mathrm{Im}(\mathbf{f}^*)\rangle$ is of order $|\mathbb{F}_q| \cdot |\langle \mathrm{Im}(\mathbf{f}^*)\rangle| = p^{e+d}$. All other strong components are evidently of order $2p^{e+d}$.

For (iii), let D_1 and D_2 be two distinct strong components of D of order $2p^{e+d}$ each. Then there exist $\mathbf{v}_1 \notin \langle \mathrm{Im}(\mathbf{f}^*)\rangle$ and $\mathbf{v}_2 \notin \langle \mathrm{Im}(\mathbf{f}^*)\rangle$ such that for an arbitrary $x \in \mathbb{F}_q$, D_1 and D_2 contain vertices $(x, \mathbf{v}_1)$ and $(x, \mathbf{v}_2)$, respectively.

Consider the map $\phi : V(D_1) \to V(D_2)$ via

$$(x, \pm\mathbf{v}_1 + \mathbf{y}) \mapsto (x, \pm\mathbf{v}_2 + \mathbf{y}), \text{ for any } x \in \mathbb{F}_q,\ \mathbf{y} \in \langle \mathrm{Im}(\mathbf{f}^*)\rangle.$$

Note that ϕ is obviously injective and, by the result of part (i), is also surjective. Hence, ϕ is a bijection between $V(D_1)$ and $V(D_2)$.

To see that ϕ preserves adjacency and non-adjacency let

$$\Big((x_1, \pm\mathbf{v}_1 + \mathbf{y}), (x_2, \mp\mathbf{v}_1 - \mathbf{y} + \mathbf{f}(x_1, x_2))\Big)$$

be an arc in D_1. Since

$$\phi((x_1, \pm\mathbf{v}_1 + \mathbf{y})) = (x_1, \pm\mathbf{v}_2 + \mathbf{y}), \text{ and}$$

$$\phi((x_2, \mp\mathbf{v}_1 - \mathbf{y} + \mathbf{f}(x_1, x_2))) = (x_2, \mp\mathbf{v}_2 - \mathbf{y} + \mathbf{f}(x_1, x_2)),$$

ϕ preserves adjacency. Hence ϕ is an isomorphism of digraphs D_1 and D_2. □

The problem of strong connectivity for digraphs defined by functions, which do not satisfy (2.1), is more complicated. For such functions we can have that $LS(\mathbf{f}) \neq \langle \mathrm{Im}(\mathbf{f}) \rangle$ even if $\langle \mathrm{Im}(\mathbf{f}) \rangle = \mathbb{F}_q^l$. Consider the following example.

Example 2.1.4. Let $p \geq 3$ be prime, $e = 2$, $q = p^e$, $\mathbb{F}_q \cong \mathbb{F}_p(\xi)$. Let $f \colon \mathbb{F}_q^2 \to \mathbb{F}_q$ be defined as

$$f(x,y) = \begin{cases} 0, & \text{if } x = y = 0, \\ 1, & \text{if } y = 0, x \neq 0, x \neq 1, \\ 2, & \text{if } x = 0, y \neq 0, y \neq 1, \\ 2\xi, & \text{if } x = y = 1, \\ \xi, & \text{if } x = 1, y \neq 1, \\ \xi, & \text{if } x \neq 1, y = 1, \\ 0, & \text{if } x \neq 0, x \neq 1, y \neq 0, y \neq 1. \end{cases}$$

It is easy to see that if $(u,v) \in V(D(q;f))$ is reachable from vertex $(0,0)$, then $v \in \mathbb{F}_p \cup (\xi + \mathbb{F}_p)$, since in any linked alternating sum, which appears in the second coordinate of a vertex reachable from $(0,0)$, the first occurrence of ξ $(-\xi)$ will be immediately followed by either $-\xi$ (respectively, ξ) or by -2ξ (respectively, 2ξ). Hence, $D(q;f)$ is not strong. By a computer verification for $3 \leq p \leq 13$, we found that each of these digraphs has $(p+1)/2$ strong components. Clearly, however, for every p, $\langle \mathrm{Im}(\mathbf{f}) \rangle = \mathbb{F}_q^2$.

In case when $\mathbf{g} \neq \mathbf{h}$, using an argument similar to the one from the proof of Theorem 2.1.3, part (i), we can prove that $D(q;\mathbf{f})$ is strong given that linked alternating sums of $\mathbf{f}$ of even length form a basis. We first present this argument for a prime p and $l = 1$. We write f instead of $\mathbf{f}$ in this case.

Theorem 2.1.5. *Let p be an odd prime, and let $f \colon \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$. If f is not a symmetric function, i.e. there exist $x_1, x_2 \in \mathbb{F}_p$ for which $f(x_1,x_2) \neq f(x_2,x_1)$, then $D(p;f)$ is strong.*

Proof. Suppose $(a,b),(c,d) \in V(D(p;f))$ are distinct and arbitrary. We construct a directed walk from (a,b) to (c,d). We have

$$\begin{aligned}
(a,b) &\to (x_1, -b + f(a,x_1)) \\
&\to (x_2, b - f(a,x_1) + f(x_1,x_2)) \\
&\to (x_1, -b + f(a,x_1) + 1\cdot[f(x_2,x_1) - f(x_1,x_2)]) \\
&\to (x_2, b - f(a,x_1) - 1\cdot[f(x_2,x_1) - f(x_1,x_2)] + f(x_1,x_2)) \\
&\to (x_1, -b + f(a,x_1) + 2\cdot[f(x_2,x_1) - f(x_1,x_2)]) \\
&\to (x_2, b - f(a,x_1) - 2\cdot[f(x_2,x_1) - f(x_1,x_2)] + f(x_1,x_2)) \\
&\to \dots \\
&\to (x_2, b - f(a,x_1) - (k-1)\cdot[f(x_2,x_1) - f(x_1,x_2)] + f(x_1,x_2)) \\
&\to (x_1, -b + f(a,x_1) + k\cdot[f(x_2,x_1) - f(x_1,x_2)]) \\
&\to (c, b - f(a,x_1) - k\cdot[f(x_2,x_1) - f(x_1,x_2)] + f(x_1,c)) \\
&= (c,d)
\end{aligned}$$

if and only if there exists a positive integer k for which

$$k\cdot[f(x_2,x_1) - f(x_1,x_2)] = b - f(a,x_1) + f(x_1,c) - d. \tag{2.4}$$

Since $a,b,c,d,x_1 \in \mathbb{F}_p$ are fixed, the right-hand side of (2.4) is also a fixed element of $\mathbb{F}_p$. Since $f(x_1,x_2) \neq f(x_2,x_1)$, it follows $f(x_2,x_1) - f(x_1,x_2)$ is a basis of $\mathbb{F}_p$, and k with the required property exists. Hence, any vertex in $D(p;f)$ is reachable from any other vertex, and so $D(p;f)$ is strong. □

We note that the argument of the proof of Theorem 2.1.5 can be generalized for functions that have linked alternating sums of arbitrary even length forming a basis of $\mathbb{F}_q^l$, and for arbitrary odd prime powers q. In the theorem we had a linked alternating sum of length 2 which formed a basis of $\mathbb{F}_p$. If $\mathbf{f}$ is such that there exist le linked alternating sums of even lengths which span $\mathbb{F}_q^l \cong \mathbb{F}_p^{le}$, we show that $D(q;\mathbf{f})$ is strong.

Theorem 2.1.6. *Let $p \geq 3$ be prime, e be a natural number, and $q = p^e$. Let $\mathbf{f}\colon \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q^l$ be such that there exist positive integers $t_1, \ldots, t_{le}$, and $x_{i,j} \in \mathbb{F}_q$, $1 \leq i \leq le$, $1 \leq j \leq 2t_j$, for which the following le linked alternating sums of lengths $2t_1, \ldots, 2t_{le}$*

$$\alpha_1 := \mathbf{f}(x_{1,1}, x_{1,2}) - \mathbf{f}(x_{1,2}, x_{1,3}) + \cdots + \mathbf{f}(x_{1,2t_1-1}, x_{1,2t_1}) - \mathbf{f}(x_{1,2t_1}, x_{1,1}),$$

$$\alpha_2 := \mathbf{f}(x_{2,1}, x_{2,2}) - \mathbf{f}(x_{2,2}, x_{2,3}) + \cdots + \mathbf{f}(x_{2,2t_2-1}, x_{2,2t_2}) - \mathbf{f}(x_{2,2t_2}, x_{2,1}),$$

$$\ldots$$

$$\alpha_{le} := \mathbf{f}(x_{le,1}, x_{le,2}) - \mathbf{f}(x_{le,2}, x_{le,3}) + \cdots + \mathbf{f}(x_{le,2t_e-1}, x_{le,2t_{le}}) - \mathbf{f}(x_{e,2t_{le}}, x_{le,1}),$$

form a basis of $\mathbb{F}_q^l$ over $\mathbb{F}_p$. Then $D(q; \mathbf{f})$ is strong.

Proof. We apply an argument similar to the one used in the proof of Theorem 2.1.5. Suppose $(a, \mathbf{b}), (c, \mathbf{d}) \in \mathbb{F}_q \times \mathbb{F}_q^l = V(D(q; \mathbf{f}))$ are distinct and arbitrary. As $\alpha_1, \ldots, \alpha_{le}$ form a basis of $\mathbb{F}_q^l$ over $\mathbb{F}_p$, and a, c and all $x_{i,j} \in \mathbb{F}_q$, $1 \leq i \leq le$, $1 \leq j \leq 2t_j$ are fixed, there exist $a_1, \ldots, a_{le} \in \mathbb{F}_p$, such that

$$\mathbf{d} = (-1)^{le+1}(a_1\alpha_1 - a_2\alpha_2 + \cdots - a_{le}\alpha_{le}) +$$

$$+(-1)^{le+1}(b - \mathbf{f}(a, x_{1,1}) + \mathbf{f}(x_{1,1}, x_{2,1}) - \cdots + \mathbf{f}(x_{le-1,1}, x_{le,1})) + \mathbf{f}(x_{le,1}, c).$$

We construct a directed walk from $(a, \mathbf{b})$ to $(c, \mathbf{d})$. We have

$$
\begin{aligned}
(a, \mathbf{b}) &\to (x_{1,1}, -\mathbf{b} + \mathbf{f}(a, x_{1,1})) \\
&\to (x_{1,2}, \mathbf{b} - \mathbf{f}(a, x_{1,1}) + \mathbf{f}(x_{1,1}, x_{1,2})) \\
&\to (x_{1,3}, -\mathbf{b} + \mathbf{f}(a, x_{1,1}) - \mathbf{f}(x_{1,1}, x_{1,2}) + \mathbf{f}(x_{1,2}, x_{1,3})) \\
&\to \dots \\
&\to (x_{1,2t_1}, \mathbf{b} - \mathbf{f}(a, x_{1,1}) + \mathbf{f}(x_{1,1}, x_{1,2}) - \dots + \mathbf{f}(x_{1,2t_1-1}, x_{1,2t_1})) \\
&\to (x_{1,1}, -\mathbf{b} + \mathbf{f}(a, x_{1,1}) - \mathbf{f}(x_{1,1}, x_{1,2}) + \dots - \mathbf{f}(x_{1,2t_1-1}, x_{1,2t_1}) + \mathbf{f}(x_{1,2t_1}, x_{1,1})) \\
&= (x_{1,1}, -\mathbf{b} + \mathbf{f}(a, x_{1,1}) - \alpha_1) \\
&\to \dots \\
&\to (x_{1,1}, -\mathbf{b} + \mathbf{f}(a, x_{1,1}) - a_1\alpha_1) \\
&\to (x_{2,1}, \mathbf{b} - \mathbf{f}(a, x_{1,1}) + a_1\alpha_1 + \mathbf{f}(x_{1,1}, x_{2,1})) \\
&\to (x_{2,2}, -\mathbf{b} + \mathbf{f}(a, x_{1,1}) - \mathbf{f}(x_{1,1}, x_{2,1}) - a_1\alpha_1 + \mathbf{f}(x_{2,1}, x_{2,2})) \\
&\to \dots \\
&\to (x_{2,2t_2}, -\mathbf{b} + \mathbf{f}(a, x_{1,1}) - \mathbf{f}(x_{1,1}, x_{2,1}) - a_1\alpha_1 + \mathbf{f}(x_{2,1}, x_{2,2}) - \dots + \mathbf{f}(x_{2,2t_2-1}, x_{2,2t_2})) \\
&\to (x_{2,1}, \mathbf{b} - \mathbf{f}(a, x_{1,1}) + \mathbf{f}(x_{1,1}, x_{2,1}) + a_1\alpha_1 - \mathbf{f}(x_{2,1}, x_{2,2}) + \dots - \mathbf{f}(x_{2,2t_2-1}, x_{2,2t_2}) + \\
&+ \mathbf{f}(x_{2,2t_2}, x_{2,1})) \\
&= (x_{2,1}, \mathbf{b} - \mathbf{f}(a, x_{1,1}) + \mathbf{f}(x_{1,1}, x_{2,1}) + a_1\alpha_1 - \alpha_2) \\
&\to \dots \\
&\to (x_{2,1}, \mathbf{b} - \mathbf{f}(a, x_{1,1}) + \mathbf{f}(x_{1,1}, x_{2,1}) + a_1\alpha_1 - a_2\alpha_2) \\
&\to \dots \\
&\to (x_{le,1}, (-1)^{le}(a_1\alpha_1 - a_2\alpha_2 + \dots + a_{le}\alpha_{le}) + \\
&+ (-1)^{le}(\mathbf{b} - \mathbf{f}(a, x_{1,1}) + \mathbf{f}(x_{1,1}, x_{2,1}) - \dots + \mathbf{f}(x_{le-1,1}, x_{le,1}))) \\
&\to (c, (-1)^{le+1}(a_1\alpha_1 - a_2\alpha_2 + \dots - a_{le}\alpha_{le}) + \\
&+ (-1)^{le+1}(\mathbf{b} - \mathbf{f}(a, x_{1,1}) + \mathbf{f}(x_{1,1}, x_{2,1}) - \dots + \mathbf{f}(x_{le-1,1}, x_{le,1})) + \mathbf{f}(x_{le,1}, c)) \\
&= (c, \mathbf{d}),
\end{aligned}
$$

and so $(c, \mathbf{d})$ is reachable from $(a, \mathbf{b})$. Hence, $D(q; \mathbf{f})$ is strong. □

At the end of this section we deal with fields of even characteristic $p = 2$. Since Lemma 2.1.1 cannot be applied, we require that $\mathbf{f}$ itself satisfy (2.1), that is, polynomials representing the defining functions $f_i \colon \mathbb{F}_{2^e} \to \mathbb{F}_{2^e}$, $1 \le i \le l$, contain mixed terms only.

Theorem 2.1.7. *Let e be a positive integer, $\mathbf{f} = (f_1, \ldots, f_l)$, $f_i \colon \mathbb{F}_{2^e}^2 \to \mathbb{F}_{2^e}$ for every i, $1 \le i \le l$, $d = \dim\langle \mathrm{Im}(\mathbf{f})\rangle$. Assume that for any $x \in \mathbb{F}_{2^e}$,*

$$\mathbf{f}(x, 0) = \mathbf{f}(0, x) = \mathbf{0}.$$

Then the digraph $D(2^e; \mathbf{f})$ has 2^{le-d} strong components, each of order 2^{e+d}. All strong components are isomorphic.

Proof. By an argument similar to the one used in the proof of Theorem 2.1.3, part (i), the vertex set of the component containing some vertex $(u, \mathbf{v})$ of $D = D(2^e; \mathbf{f})$ is

$$\{(x, \mathbf{v} + \langle \mathrm{Im}\mathbf{f}\rangle) \colon x \in \mathbb{F}_{2^e}\}.$$

From this we find that every strong component of D contains $|\mathbb{F}_{2^e}| \cdot |\langle \mathrm{Im}(\mathbf{f})\rangle| = 2^{e+d}$ vertices, and there are $|\mathbb{F}_{2^e}^l / \langle \mathrm{Im}(\mathbf{f})\rangle| = 2^{le-d}$ strong components. An isomorphism of any two distinct strong components of D is exhibited by an argument similar to the one in the proof of Theorem 2.1.3, part (iii). □

2.2 Connectivity of $D(q; m, n)$

We apply the results of Section 2.1 to digraphs in which the only defining function is a monomial, i.e. to the case when $\mathbf{f}(x, y) = f(x, y) = x^m y^n$, $1 \le m, n \le q - 1$. Obviously Theorem 2.1.3 applies to functions of this type.

The main idea in the analysis of connectivity of the graph $D(q; m, n)$ is finding $\langle \mathrm{Im}(f)\rangle$ depending on the parameters m and n, which is done in Lemmas 2.2.1 and 2.2.2. The key observation here is Lemma 2.2.2 which essentially allows for a reduction to the case $m = n$.

We adopt the following notation throughout this section. In a field with $q = p^e$ elements we define

$$q_i = \frac{q-1}{p^{e_i}-1} = \frac{p^e-1}{p^{e_i}-1} \text{ for any } e_i | e.$$

Let A_k be the set of k-th powers of all elements of the field, $A_k^* = A_k \setminus \{0\}$. Let $A_{m,n}$ denote the set $\{x^m y^n : x, y \in \mathbb{F}_q\}$, $A_{m,n}^* = A_{m,n} \setminus \{0\}$. For any pair of integers m and n with $1 \leq m, n \leq q-1$, let $d = (q-1, m, n)$, the greatest common divisor of $q-1$, m and n.

Lemma 2.2.1. *Let q_s be the largest of the q_i's dividing $(k, q-1)$. Then $\mathbb{F}_{p^{e_s}}$ is the smallest subfield of $\mathbb{F}_q$ in which A_k is contained. Moreover, A_k contains a basis for $\mathbb{F}_{p^{e_s}}$ over $\mathbb{F}_p$. So, in fact, $\langle A_k \rangle = \mathbb{F}_{p^{e_s}}$.*

Proof. By definition, q_s divides k so that $k = tq_s$ for some integer t. Thus for any $x \in \mathbb{F}_q$,

$$x^k = x^{tq_s} = \left(x^{\frac{p^e-1}{p^{e_s}-1}}\right)^t \in \mathbb{F}_{p^{e_s}}$$

by definition of the norm of an element of $\mathbb{F}_q$ over $\mathbb{F}_{p^{e_s}}$. Suppose now that $A_k \subseteq \mathbb{F}_{p^{e_i}} \subsetneqq \mathbb{F}_{p^{e_s}}$ so that $e_i < e_s$. Since A_k^* is a subgroup of $\mathbb{F}_{p^{e_i}}^*$, we have that $|A_k^*|$ divides $|\mathbb{F}_{p^{e_i}}^*|$, that is, $\frac{q-1}{(p^e-1,k)}$ divides $p^{e_i}-1$. Write $p^{e_i}-1 = t \cdot \frac{q-1}{(p^e-1,k)}$ for some integer t so that $(q-1,k) = t \cdot \frac{p^e-1}{p^{e_i}-1} = tq_i$, and a contradiction is obtained as $q_i > q_s$.

Clearly the span of A_k over $\mathbb{F}_p$ is closed under addition and multiplication and so is a subfield of $\mathbb{F}_q$. Since we know A_k is not contained in any subfield of $\mathbb{F}_q$ smaller than $\mathbb{F}_{p^{e_s}}$, it follows that the span is all of $\mathbb{F}_{p^{e_s}}$ and therefore A_k contains a basis of it over $\mathbb{F}_p$. □

Lemma 2.2.2. $A_{m,n} = A_d$.

Proof. It is easy to see $A_{m,n}^* = A_m^* A_n^*$ and so

$$|A_{m,n}^*| = |A_m^* A_n^*| = \frac{|A_m^*||A_n^*|}{|A_m^* \cap A_n^*|}. \tag{2.5}$$

Let $\mathbb{F}_q^*$ be generated by some ξ so that $A_m^* = \langle \xi^{(q-1,m)} \rangle$ and so $|A_m^*| = \frac{q-1}{(q-1,m)}$. Also from elementary algebra (see Proposition 3.2.2) we know that if x is a generator of a finite group, then for any integers m and n, $\langle x^m \rangle \cap \langle x^n \rangle = \langle x^{lcm(m,n)} \rangle$. That is, $A_m^* \cap A_n^* = \langle \xi^l \rangle$, where $l = lcm((m, q-1), (n, q-1))$. We show that $|A_{m,n}^*| = |A_d^*|$, and since in a cyclic group any two subgroups of equal order are equal, that would imply $A_{m,n} = A_d$.

From (2.5) we find

$$\begin{aligned} |A_{m,n}^*| =& \frac{\frac{q-1}{(q-1,(q-1,m))} \cdot \frac{q-1}{(q-1,(q-1,n))}}{\frac{q-1}{(q-1,lcm((q-1,m),(q-1,n)))}} \\ =& \frac{(q-1) \cdot (q-1, lcm((q-1,m),(q-1,n)))}{(q-1,m) \cdot (q-1,n)}. \end{aligned} \tag{2.6}$$

Let M and N be such that $q-1 = M\overline{m} = N\overline{n}$. Let $d = (\overline{m}, \overline{n})$, so that $\overline{m} = dm'$ and $\overline{n} = dn'$ for some integers m' and n' for which $(m', n') = 1$. Then $q-1 = dm'M = dn'N$ and $(q-1)/d = m'M = n'N$. As $(m', n') = 1$, we have $M = n't$ and $N = m't$ for some integer t. This implies that $q - 1 = dm'n't$. For any integer a and b there holds $lcm(a, b) = ab/(a, b)$, we have

$$\begin{aligned} lcm((q-1,m),(q-1,n)) &= lcm(\overline{m},\overline{n}) = lcm(dm', dn') \\ &= \frac{dm'dn'}{(dm', dn')} = \frac{dm'dn'}{d(m', n')} = dm'n'. \end{aligned}$$

Therefore, $(q-1, lcm(\overline{m}, \overline{n})) = dm'n'$. Thus,

$$A_{m,n}^* = \frac{(q-1)dm'n'}{\overline{m}\overline{n}} = \frac{q-1}{d} = \frac{q-1}{(\overline{m},\overline{n})} = \frac{q-1}{(q-1,m,n)}.$$

Since A_d^* is generated by $\xi^{(q-1,d)}$, we have

$$|A_d^*| = \frac{q-1}{(q-1,(q-1,d))} = \frac{q-1}{(q-1,d)} = \frac{q-1}{(q-1,(q-1,m,n))} = \frac{q-1}{(q-1,m,n)}.$$

Hence $|A_{m,n}^*| = |A_d^*|$ and so $A_{m,n} = A_d$. □

Clearly, $\langle \mathrm{Im}(f) \rangle = \langle A_d \rangle$, and the following is a straightforward application of Theorem 2.1.3.

Theorem 2.2.1. *For the graph $D = D(q; m, n)$, let q_s be the largest of the q_i's dividing d. The following statements hold.*

(i) The vertex set of the strong component of D containing some vertex (u, v) is

$$\{(x, v + \mathbb{F}_{p^{e_s}}) \colon x \in \mathbb{F}_q\} \cup \{(x, -v + \mathbb{F}_{p^{e_s}}) \colon x \in \mathbb{F}_q\}; \tag{2.7}$$

in particular, D is strong if and only $e_s = e$, that is, if and only if $q_s = 1$ is the largest of the q_i's dividing d.

(ii) The strong component containing vertex $(0, 0)$ is of order p^{e+e_s}; all other components are of equal order $2p^{e+e_s}$. There are $\frac{p^{e-e_s}+1}{2}$ components.

(iii) All strong components of equal order are isomorphic.

Proof. We apply Theorem 2.1.3 with $\langle \mathrm{Im}(f) \rangle = \langle A_d \rangle = \mathbb{F}_{p^{e_s}}$. Also D is strong if and only if $\mathbb{F}_{p^{e_s}} = \mathbb{F}_q$, that is, if and only if $e_s = e$, which is equivalent to $q_s = 1$. Thus (2.7) is proved. The rest of the statements in the theorem follow directly from Theorem 2.1.3. □

At the end of this section we restate Theorem 2.1.7 for monomial digraphs.

Theorem 2.2.2. *For the graph $D = D(2^e; m, n)$, let q_s be the largest of the q_i's dividing d. Then the vertex set of the strong component of D containing some vertex (u, v) is*

$$\{(x, v + \mathbb{F}_{2^{e_s}}) \colon x \in \mathbb{F}_{2^e}\},$$

G has 2^{e-e_s} strong components with 2^{e+e_s} vertices in each. All components are isomorphic one to another.

2.3 General Remarks about Diameter

Theorem 2.1.3 describes conditions under which the digraph $D(q; \mathbf{f}^*) \cong D(q; \mathbf{f})$ is strong. When considering strong digraphs a natural property to consider is that of diameter. Suppose for a graph $D = D(q; \mathbf{f})$ the conditions guaranteeing that D is strong are satisfied. As D is strong, we know that any vertex of D is reachable from any other arbitrary vertex of D. Let us introduce the following notation: instead of

$(x_1, \ldots, x_{l+1})$ we will write an ordered pair $(x_1, \mathbf{b})$ where $\mathbf{b} = (x_2, \ldots x_{l+1})$. For any walk of length k originating at $(a, \mathbf{b})$ we have

$$\begin{aligned}(a, \mathbf{b}) &\to (x_1, -\mathbf{b} + \mathbf{f}(a, x_1)) \\ &\to (x_2, \mathbf{b} - \mathbf{f}(a, x_1) + \mathbf{f}(x_1, x_2)) \\ &\to \ldots \\ &\to (x_k, \mathbf{f}(x_{k-1}, x_k) - \mathbf{f}(x_{k-2}, x_{k-1}) + \cdots + (-1)^{k-1}\mathbf{f}(a, x_1) + (-1)^k \mathbf{b}), \end{aligned} \tag{2.8}$$

where, by Definition 2.1.1, $\mathbf{f}(x_{k-1}, x_k) - \cdots + (-1)^{k-1}\mathbf{f}(a, x_1)$ is an alternating sum of $\mathbf{f}$ of length k. In order to give an upper bound on the diameter of D one would have to provide an upper bound on k, and find $x_1, x_2, \ldots, x_k \in \mathbb{F}_q$, such that

$$\left\{(x_k, \mathbf{f}(x_{k-1}, x_k) + \cdots + (-1)^{k-1}\mathbf{f}(a, x_1) + (-1)^k \mathbf{b}) \colon x_1, \ldots, x_k \in \mathbb{F}_q\right\} = \mathbb{F}_q^{l+1}. \tag{2.9}$$

While this problem seems hard for a general function $\mathbf{f}$, in Section 2.4 we obtain some results for the case when $l = 1$ and $f(x, y) = x^m y^n$. We also obtain some results on diameter when m, n are fixed and q is large in Section 2.6.

2.4 Diameter of Monomial Digraphs

The following is the well-known Moore bound for the diameter of a general digraph: see [1], p. 101.

Proposition 2.4.1. *Let n, Δ and d be the order, the maximum out-degree and the diameter, respectively, of a strong digraph D. If $\Delta > 1$ and $d > 1$, then*

$$d \geq \lfloor \log_\Delta(n(\Delta - 1) + 1) \rfloor.$$

For $D(q; m, n)$, $\Delta = q$, $n = q^2$, and by Proposition 2.4.1 we obtain

$$\operatorname{diam}(D(q; m, n)) \geq \lfloor \log_q(q^2(q - 1) + 1) \rfloor \geq 2$$

for all q, m, n. The following argument shows that monomial digraphs have diameter at least 3.

Proposition 2.4.2. *If $D = D(q; m, n)$ is strong, then* $\operatorname{diam}(D) \geq 3$ *for any parameters* m, n.

Proof. For any parameters m, n, we count the number of vertices in D that are at distance at most 2 from vertex $(0, 0)$. Clearly $(0, 0)$ is a loop in D, and all other vertices in its out-neighborhood are of them form $N_1^+((0, 0)) = \{(x, 0) \colon x \in \mathbb{F}_q^*\}$. From every one of the vertices in $N_1^+((0, 0))$ there is an arc to $(0, 0)$. Therefore,

$$\left| \bigcup_{x \in \mathbb{F}_q^*} N_1^+((x, 0)) \setminus \{(0, 0)\} \right| \leq (q - 1)^2.$$

Hence, the number of vertices in D which are at distance at most 2 from $(0, 0)$ is at most $1 + q - 1 + (q - 1)^2 = q^2 - (q - 1) < q^2$. Thus, there are vertices in D which are at distance at least 3 from $(0, 0)$, which implies that $\operatorname{diam}(D) \geq 3$. □

In several cases we can say more about the diameter of monomial graphs. Here is one such instance.

Proposition 2.4.3. *If* $\overline{m} = 1$ *or* $\overline{n} = 1$, *then* $\operatorname{diam}(D(q; m, n)) \leq 4$. *If* $\overline{m} = \overline{n} = 1$, *then* $\operatorname{diam}(D(q; m, n)) = 3$.

Proof. Let $D = D(q; m, n)$ and $(x, y) \in V(D)$ be arbitrary. We show that there exist directed paths to any vertex of D originating at (x, y) of length at most 3 or 4. It is easy to verify that the 3-rd and 4-th out-neighborhoods of (x, y) are, respectively,

$$N_3^+((x, y)) = \{(x_3, -y + x^m x_1^n - x_1^m x_2^n + x_2^m x_3^n) \colon x_1, x_2, x_3 \in \mathbb{F}_q\},$$

$$N_4^+((x, y)) = \{(x_4, y - x^m x_1^n + x_1^m x_2^n - x_2^m x_3^n - x_3^m x_4^n) \colon x_1, x_2, x_3, x_4 \in \mathbb{F}_q\}.$$

Suppose $\overline{m} = 1$. Then $A_m = \mathbb{F}_q$. If $x = 0$, one may set $x_2 = 1$, $x_3 = 0$, so that

$$N_4^+((0, y)) = \{(x_4, x_1^m + y) \colon x_1, x_4 \in \mathbb{F}_q\} = \mathbb{F}_q^2 = V(D).$$

Likewise, if $x \neq 0$, one sets $x_1 = 0$, $x_3 = 1$, which yields

$$N_4^+((x, y)) = \{(x_4, y - x_2^m - x_4^n) \colon x_2, x_4 \in \mathbb{F}_q\} = \mathbb{F}_q^2 = V(D).$$

Suppose now that $\overline{n} = 1$. If, in addition $x = 0$, one may set $x_1 = 1$, $x_3 = 0$, so that

$$N_4^+((0, y)) = \{(x_4, x_2^n + y) \colon x_2, x_4 \in \mathbb{F}_q\} = \mathbb{F}_q^2 = V(D).$$

If however $x \neq 0$, one sets $x_2 = x_3 = 0$, which yields

$$N_4^+((x, y)) = \{(x_4, y - x^m x_1^n) \colon x_1, x_4 \in \mathbb{F}_q\} = \mathbb{F}_q^2 = V(D).$$

Finally, if $\overline{m} = \overline{n} = 1$, then set $x_2 = 1$ for the case $x = 0$, and $x_2 = 0$ if $x \neq 0$. For these two cases, we have, respectively,

$$N_3^+((0, y)) = \{(x_3, x_3^n - x_1^m - y) \colon x_1, x_3 \in \mathbb{F}_q\} = \mathbb{F}_q^2 = V(D),$$

$$N_3^+((x, y)) = \{(x_3, x^m x_1^n - y) \colon x_1, x_3 \in \mathbb{F}_q\} = \mathbb{F}_q^2 = V(D).$$

□

Later we will see that if the conditions of Proposition 2.4.3 are not satisfied, the diameter of $D(q; m, n)$ can be large.

Note that by Theorem 2.2.1 the graph $D(p; m, n)$ is strong for all m, n, and we have

Theorem 2.4.4. $\operatorname{diam}(D(p; m, n)) \leq 4p - 2$.

Proof. Let $D = D(p; m, n)$ and let (a, b) be an arbitrary vertex in D. We show that there exists a walk of length at most $4p - 3$ from (a, b) to any other vertex (u, v) in D.

From (2.8) with k odd we need to show that the system

$$\begin{cases} u = x_k, \\ v = -b + a^m x_1^n - x_1^m x_2^n + x_2^m x_3^n - \cdots - x_{k-2}^m x_{k-1}^n + x_{k-1}^m x_k^n \end{cases} \tag{2.10}$$

has a solution $x_1, \ldots, x_k \in \mathbb{F}_p$ with $k \leq 4p - 3$. Let v' be the unique integer between 0 and $p-1$ whose image under the canonical homomorphism $\phi \colon \mathbb{Z} \to \mathbb{F}_p$ is $v + b$. We take $k = 4v' + 1$ and set $x_1 = 0$, $x_{4i-2} = x_{4i-1} = 1$, $x_{4i} = x_{4i+1} = 0$ for any i, $1 \leq i \leq v' - 1$, $x_{4v'-2} = x_{4v'-1} = 1$, $x_{4v'} = 0$, $x_{4v'+1} = x_k = u$. Clearly such chosen $(x_1, \ldots, x_k)$ satisfy system (2.10); also $k = 4v' + 1 \leq 4(p-1) + 1 = 4p - 3$. Note that a very similar argument with k even yields an upper bound $\operatorname{diam}(D(p; m, n)) \leq 4p - 2$. □

We finish this section with the following conjecture. It is based on computational data of the diameter of monomial digraphs and has been checked for all prime p, $3 \leq p \leq 41$.

Conjecture 2.4.5. $\operatorname{diam}(D(p;m,n)) \leq 2p-1$ *with equality if and only if* $m = n = p-1$.

2.5 Waring's Problem over Finite Fields

Waring's problem for rings asks the question: Given a positive integer k does there exist a positive integer s such that every element in a given ring can be represented as a sum of at most s k-th powers? This was originally posed in 1770 by Waring for positive integers and answered in the affirmative for integers by Hilbert in 1909. The next obvious question once we know every element can be represented is: What is the least number of summands needed? While these two questions are essentially answered for integers by Small [25], in the finite field setting this second question is far from settled.

Over a finite field $\mathbb{F}_q$, the smallest s (should it exist) such that

$$x_1^k + x_2^k + \cdots + x_s^k = \alpha$$

has a solution in $\mathbb{F}_q^s$ for all $\alpha \in \mathbb{F}_q$ is called *Waring's number*, denoted $\gamma(k,q)$. Similarly we define $\delta(k,q)$ to be the smallest s (should it exist) such that every element of $\mathbb{F}_q$ can be represented as sums or differences of s k-th powers, that is, such that

$$\epsilon_1 x_1^k + \epsilon_2 x_2^k + \cdots + \epsilon_s x_s^k = \alpha$$

is solvable in $\mathbb{F}_q^s$ for all $\alpha \in \mathbb{F}_q$ and all sequences $\{\epsilon_1, \ldots, \epsilon_s\}$, where each ϵ_i is in $\{-1, 1\} \subseteq \mathbb{F}_q$. It is easy to show that $\gamma(k,q) = \gamma(\overline{k},q)$ since the set of k-th powers in $\mathbb{F}_q$ is the same as the set of l-th powers, where $l = \overline{k} = (q-1,k)$. Thus we may assume $k|(q-1)$.

The following theorem gives necessary and sufficient conditions for the existence of $\gamma(k,q)$. It is also plain from this theorem that $\delta(k,q)$ exists if and only if $\gamma(k,q)$ exists. This theorem is essentially a restated version of Lemma 2.2.1.

Theorem 2.5.1. *The following are equivalent for any $q = p^e$ and $k|q-1$:*

(i) *$\gamma(k,q)$ exists, that is, every element of $\mathbb{F}_q$ is a sum of k-th powers.*

(ii) *A_k is not contained in any proper subfield of $\mathbb{F}_q$, that is, A_k contains a set of e linearly independent elements over $\mathbb{F}_p$.*

(iii) *$|A_k^*|$ does not divide $p^j - 1$ for any $j|e$, $j < e$, that is, $\frac{p^e-1}{p^j-1}$ does not divide k for any $j|e$, $j < e$.*

The following inequalities relating $\gamma(k,q)$ and $\delta(k,q)$, for any k, q such that $\gamma(k,q)$ is defined, are obtained in Cipra [7]:

$$\delta(k,q) \le \gamma(k,q) \le 2\lceil 2\log_2\log_2 q\rceil \delta(k,q).$$

Waring's problem is an active area of research in additive combinatorics; see for example papers Bourgain, Chang [4], Bourgain, Glibichuk, Konyagin [5], Cipra, Cochrane, Pinner [8] and Cochrane, Pinner [9]. A number of upper and lower bounds of $\gamma(k,q)$ exists. For a survey of results see [7].

A result from the theory on Waring's number that we will use in the next section provides very small bounds of $\gamma(k,p)$ for p sufficiently large relative to k. These results follow from the classical estimates of Weil [28] and Hua, Vandiver [16]; see [7] for a detailed discussion of them.

Theorem 2.5.2. *For $p > (k-1)^{\frac{2s}{s-1}}$, we have $\gamma(k,p) \le s$. In particular,*

$$\gamma(k,p) \le \begin{cases} 2, & p > k^4, \\ 3, & p > k^3, \\ 1 + \log(k)/|\log(\varepsilon))|, & p > (1+\varepsilon)k^2. \end{cases}$$

Note that as p approaches k^2 this bound tends to infinity. A stronger upper bound, namely,

$$\gamma(k,p) \le \lfloor 32\log k\rfloor + 1 \quad \text{for } p > k^2,$$

was obtained in Dodson [11].

2.6 Bounds on Diameter for Large Prime p

In this section we give a number of applications of Theorem 2.5.2. These results establish upper bounds on the diameter of the monomial digraph $D(p; m, n)$ when p is large relative to m, n.

Proposition 2.6.1. *If* $p > \min\{m^4, n^4\}$, *then* $\operatorname{diam}(D(p; m, n)) \leq 7$.

Proof. By (2.9) we need to show that the system

$$\begin{cases} u &= x_7, \\ v &= -x_1^m x_2^n + x_2^m x_3^n - x_3^m x_4^n + x_4^m x_5^n - x_5^m x_6^n + x_6^m x_7^n + x_1^n, \end{cases}$$

has a solution $(x_1, \ldots, x_7)$ for every pair $(u, v) \in \mathbb{F}_p^2$. If $p > n^4$, set $x_1 = x_4 = 1$, $x_3 = x_6 = 0$, so

$$v = -x_2^n + x_5^n + 1. \tag{2.11}$$

By Theorem 2.5.2, $\gamma(n, p) = 2$, and so (2.11) is solvable for any $v \in \mathbb{F}_p$. Likewise, if $p > m^4$, set $x_1 = x_4 = 0$, $x_3 = x_6 = 1$ so

$$v = x_2^m - x_5^m + u^n \tag{2.12}$$

is solvable for any $u, v \in \mathbb{F}_p$ since in this case $\gamma(m, p) = 2$. □

A similar result can be obtained under less strict conditions.

Proposition 2.6.2. *If* $p > \min\{m^3, n^3\}$, *then* $\operatorname{diam}(D(p; m, n)) \leq 10$.

Proof. Following the pattern of the proof of the previous proposition, in (2.9) with $k = 10$, set $x_1 = x_4 = x_7 = 0$ and $x_3 = x_6 = x_9 = 1$ if $p > m^3$; set $x_1 = x_4 = x_7 = 1$ and $x_3 = x_6 = x_9 = 0$ if $p > n^3$. In the first case we have $v = -x_2^m + x_5^m - x_8^m + u^n$. In the second case we have $v = x_2^n - x_5^n + x_8^n - 1$. Note that in either case $\gamma(3, p) \leq 3$, and so both equations are solvable for any $u, v \in \mathbb{F}_p$. □

By the remark after Theorem 2.5.2, a better bound could not be obtained by an argument of this type, i.e. one cannot obtain a bound for $p > \min\{m^2, n^2\}$ through the same approach.

Proposition 2.6.3. $\operatorname{diam}(D(p;n,n)) \leq 6$ *for* $p > n^4$.

Proof. By (2.9), we need to show that the system

$$\begin{cases} u &= x_6, \\ v &= x_1^n x_2^n - x_2^n x_3^n + x_3^n x_4^n - x_4^n x_5^n + x_5^n x_6^n - x_1^n, \end{cases}$$

has a solution $(x_1, \ldots, x_6)$ for every pair $(u, v) \in \mathbb{F}_p^2$. Setting $x_1 = x_5 = 0$ and $x_3 = 1$, we get $v = -x_2^n + x_4^n$ which is solvable for any $v \in \mathbb{F}_p$, as $\gamma(n,p) = 2$ if $p > n^4$. □

Even though we mostly concentrated on obtaining upper bounds on the diameter of digraphs $D(q;m,n)$, some results from the theory of Waring's problem over finite fields can yield lower bounds for the diameter of these graphs. In fact, there exist monomial digraphs with arbitrarily large diameters.

Theorem 2.6.4 ([8])**.** *Let* $t := \frac{p-1}{k}$ *be the number of* k*-th powers in the multiplicative group of the field* $\mathbb{F}_p^*$*. For* $t = 3, 4$ *or* 6*, there hold the bounds*

$$\sqrt{2k} - 1 \leq \gamma(k,p) \leq 2\sqrt{k}.$$

For instance, if $p = 97$, $t = 3$, $m = n = k = \frac{p-1}{t} = 32$, $\gamma(k,p) = \gamma(32,97) \geq 9$, and by a computer verification we found that $\operatorname{diam}(D(97;32,32)) = 9$.

2.7 Bounds on the Diameter of $D(q;1,n)$

In view of Proposition 2.4.3 it is plain that the following bounds hold for the digraph $D(q;1,n)$:

Proposition 2.7.1. *For any* n, $\operatorname{diam}(D(q;1,n)) \leq 4$. *If, additionally,* $\overline{n} = 1$, *then* $\operatorname{diam}(D(q;1,n)) = 3$.

A stronger result, however, may be obtained using some techniques from algebraic geometry. It turns out that only for a finite number of prime powers q is the diameter of $D(q;1,n)$ actually 4. We apply the Hasse-Weil bound, a major result from the theory of algebraic curves over finite fields, in order to estimate the diameter of the

digraph $D(q;1,n)$. The Hasse-Weil bound provides a bound on the number of points on a curve over a finite field. If the number of points on the curve C of genus g over the finite field $\mathbb{F}_q$ is $\#C(\mathbb{F}_q)$, then

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}. \tag{2.13}$$

For a discussion of this technique and proofs we refer to [15] and [24].

Our main result in this section is the following:

Theorem 2.7.2. *Let p be an odd prime, e be a positive integer, $q = p^e$ and assume that p does not divide n. If $q > n^2(n-1)^2$, then* $\operatorname{diam}(D(q;1,n)) = 3$.

Proof. Let (a,b) be an arbitrary vertex of $D(q;1,n)$. To show that any other vertex (u,v) is reachable from (a,b) via a path of length at most 3, we need to show that the system

$$\begin{cases} u &= x_3, \\ v &= -x_1x_2^3 + x_2x_3^n + ax_1^n - b \end{cases}$$

has a solution. We may set $b = 0$. If $u \neq 0$, then clearly $(x_1,x_2,x_3) = (0, vu^{-n}, u)$ is a solution. If, however, $u = 0$, then the existence of a solution of this system is equivalent to the question of determining whether the function $f\colon \mathbb{F}_q^2 \to \mathbb{F}_q$ given by $f(x_1,x_2) = -x_1x_2^n + ax_1^n$ is surjective for any $a \in \mathbb{F}_q$.

We prove that $f(x,y) = ax^n - xy^n$ is surjective as a function $f\colon \mathbb{F}_q^2 \to \mathbb{F}_q$ for all sufficiently large prime powers q and all $a \in \mathbb{F}_q$. We may assume $a \neq 0$ since the case $a = 0$ is trivial. For an arbitrary $\xi \in \mathbb{F}_q$ consider the equation

$$ax^n - xy^n - \xi = 0. \tag{2.14}$$

The corresponding projective curve is the zero locus of the homogeneous polynomial

$$F(X,Y,Z) = aX^nZ - XY^n - \xi Z^{n+1}.$$

We find

$$\frac{\partial F}{\partial X} = anX^{n-1}Z - Y^n;$$

$$\frac{\partial F}{\partial Y} = -nXY^{n-1};$$
$$\frac{\partial F}{\partial Z} = anX^n - (n+1)\xi Z^n.$$

Looking at the partial derivatives and using the fact that p does not divide n we see that they vanish simultaneously only if $X = Y = Z = 0$, so the curve has no singularities. Furthermore, it has exactly two points on the line at infinity $Z = 0$, namely $[1 : 0 : 0]$ and $[0 : 1 : 0]$.

By the genus-degree formula, the genus of a non-singular plane curve given by a degree k equation is $g = (k-1)(k-2)/2$. Taking $k = n+1$ (our case) we have $g = n(n-1)/2$. Let N_q be the number of $\mathbb{F}_q$-rational points on the curve given by (2.14). Then, by (2.13),

$$|N_q - (q+1)| \leq 2g\sqrt{q}.$$

This gives us a lower bound $N_q \geq q+1-2g\sqrt{q}$ for our curve. Let $N(\xi)$ be the number of solutions (2.14). Counting for the two points at infinity we end up with a lower bound

$$N(\xi) \geq q - 1 - 2g\sqrt{q}.$$

Clearly, $N(\xi) \geq 1$ if $q-1-2g\sqrt{q} > 0$. The latter is true if $q > 4g^2 = (n^2-3n+2)^2$. □

The following table shows the diameters of digraphs $D(q; 1, n)$ for some $q \geq 3$ and certain values of $1 \leq n \leq q-1$. For most of these graphs the diameter is still equal to 3; in all exceptional cases it is equal to 4.

Table 2.1: Diameters of digraphs $D(q;1,n)$ for certain values of n.

(m,n)	q exception	$q \leq$
(1,1)		1000
(1,2)	5	∞
(1,3)	19	2000
(1,4)	9, 17	920
(1,5)		1500
(1,6)	13,19,25,37,73	900
(1,7)	197	2000
(1,8)	17	1000
(1,9)		1000
(1,10)	41	1000
(1,11)	243	1000
(1,12)	17,19,25,37,49,73,97,289,433,577	1000
(1,13)	677	2000
(1,14)	29,197	1000
(1,15)	19,151,181	1000
(1,16)	193	1000
(1,17)		3000
(1,18)	25,37,73,109,163	1000
(1,19)		1000
(1,20)	41,81,101,151	1000
(1,21)	127,197	1000
(1,22)	89	1000
(1,23)		1000
(1,24)	37,49,73,97,109,193,257,289,433,769,1009,1153	1500
(1,25)		1000
(1,26)	53,157	1000
(1,27)	163	1000
(1,28)	113,169,197	1000
(1,29)		1000

(m,n)	q exception	$q \leq$
(1,30)	37,41,61,73,101,121,151,181,271	1000
(1,31)		1000
(1,32)		1000
(1,33)	199,243	1000
(1,34)	137	1000
(1,35)	197	1000
(1,36)	49,73,97,109,163,289	1000
(1,37)		1000
(1,38)		1000
(1,39)		1000
(1,40)	81,101,151,193	1000
(1,210)	271,281,337,361,379,421,491,541,601,631,701,751,757,841,883	1000

2.8 Bounds on the Diameter of $D(p;1,2)$

In this section we consider $D(p;1,2)$ for arbitrary odd primes p. Our main result can be stated as follows.

Theorem 2.8.1. *For odd prime $p \neq 5$,* $\operatorname{diam}(D(p;1,2)) = 3$, *while* $\operatorname{diam}(D(5;1,2)) = 4$.

As was noted earlier, in order to obtain an upper bound on the diameter of a monomial digraph, one has to show that a certain polynomial function in a finite field is surjective or, equivalently, that a certain polynomial equation in a finite field is solvable. This is proved in Lemma 2.8.1 where we apply elementary number-theoretic techniques such as certain properties of Gauss and Jacobi sums. All of the facts and techniques used in this section can be found in Ireland, Rosen [17] and Berndt, Evans, Williams [2].

Lemma 2.8.1. *If $p \geq 7$ is a prime, then the function $f(x,y)\colon \mathbb{F}_p^2 \to \mathbb{F}_p$ given by $f(x,y) = ax^2 - xy^2 \in \mathbb{F}_p[x,y]$ is surjective for any $a \in \mathbb{F}_p$.*

Trivially the statement holds for $a = 0$ and so assume from now on that $a \neq 0$.

Let us restate the lemma in the following equivalent way: if p is an odd prime, $p > 5$, then the equation $f(x, y) = t$ has a solution for every $t \in \mathbb{F}_p$. This latter equation is evidently quadratic with respect to x and so, for a solution to exist, for every $t \in \mathbb{F}_p$ we must have $y^4 + 4at \in \square_p$, where $\square_p$ is the set of all squares in $\mathbb{F}_p$. If $ta^{-1} \in \square_p$, then clearly $(x, y) = (z, 0)$, where $z^2 = ta^{-1}$, is a solution of $f(x, y) = t$. So assume from now that $ta^{-1} \notin \square_p$ and, therefore, $4at \notin \square_p$. Let $n = 4at$. Note that if $q \equiv 1 \pmod 4$, then $-n \notin \square_p$, while if $q \equiv 3 \pmod 4$, then $-n \in \square_p$. Thus we have explained that Lemma 2.8.1 is equivalent to the following

Lemma 2.8.2. *If $5 \neq p \equiv 1 \pmod 4$, for every $n \notin \square_p$ there exists $y \in \mathbb{F}_p$ such that $y^4 \in \square_p + n$. If $p \equiv 3 \pmod 4$, for every nonzero $s \in \square_p$ there exists $y \in \mathbb{F}_p$ such that $y^4 \in \square_p + s$.*

Proof. Note that the case $p \equiv 3 \pmod 4$ is trivial: let r be such that $r^2 = s$. Then if $r \in \square_p$, let u be such that $u^2 = r$ and set $y = u$; if $-r \in \square_p$, let u be such that $u^2 = -r$ and set $y = u$. In both cases $y^4 = 0 + s \in \square_p + s$.

Let us now proceed to the case $p \equiv 1 \pmod 4$. We need to prove that every non-square n can be written as $n = x^4 + y^2$ for some $x, y \in \mathbb{F}_p$. We consider the number $N = N(x^4 + y^2 = c)$ of solutions of this equation and argue it is positive. We have

$$N := N(x^4 + y^2 = c) = \sum_{a+b=c} N(x^4 = a)N(x^2 = b).$$

By Proposition 8.1.5 in [17], $N(x^n = a) = \sum_{\chi^n = \varepsilon} \chi(a)$, where $n|(p-1)$, ε is the trivial character and the sum is over all multiplicative characters of order dividing n. From the proof of this proposition it follows that such characters are ε, χ, χ^2, $\ldots$, χ^{n-1} with $\chi(g) = e^{2\pi i/n}$ for some generator g of $\mathbb{F}_p^*$. Then

$$N = \sum_{a+b=c} \left\{ \sum_{k=0}^{3} \chi^k(a) \sum_{j=0}^{1} \lambda^j(b) \right\},$$

where λ and χ are characters on $\mathbb{F}_p^*$ of order 2 and 4, respectively, so that $\lambda(g) = -1$ and $\chi(g) = i$. Define $a' = ac^{-1}$ and $b' = bc^{-1}$ so that $a' + b' = 1$. Then

$$N = \sum_{a'+b'=1} \left\{ \sum_{k=0}^{3} \chi^k(a'c) \sum_{j=0}^{1} \lambda^j(b'c) \right\} = \sum_{k=0}^{3} \sum_{j=0}^{1} \chi^k(c)\lambda^j(c) J(\chi^k, \lambda^j),$$

where $J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$ is a Jacobi sum. By Theorem 1 on p. 93 in [17], $J(\varepsilon, \varepsilon) = p$ and $J(\chi, \varepsilon) = 0$ for any nontrivial character χ. Thus

$$N = p + \sum_{k=1}^{3} \chi^k(c)\lambda(c) J(\chi^k, \lambda) = p - 1 - \chi(c)\Big\{ J(\chi, \chi^2) - J(\chi^3, \chi^2) \Big\}.$$

The values of these Jacobi sums are also known. We refer to [2] for a complete calculation of them. If $p \equiv 1 \pmod 4$, then $p = a^2 + b^2$ for some integers a and b. If we further require $a, b > 0$, a be odd, b be even, then such a representation is unique. In [2] it is proven that $J(\chi, \chi^2) = a + bi$ and $J(\chi^3, \chi^2) = a - bi$. Hence

$$N = p - 1 - 2\chi(c)bi.$$

Since $c \notin \square_p$, we have $c = g^k$ for some $k \equiv 1, 3 \pmod 4$ and therefore $\chi(c) = \pm i$. Thus

$$N = \begin{cases} p - 1 + 2b, & k \equiv 1 \pmod 4 \\ p - 1 - 2b, & k \equiv 3 \pmod 4 \end{cases}$$

Since $b < \sqrt{p}$, $p \geq 7 > 3 + 2\sqrt{2} > 5$ guarantees $p - 1 - 2b > 0$. This ends our proof. $\square$

We now can prove Theorem 2.8.1.

Proof. Consider an arbitrary vertex (a, b) of $D(p; 1, 2)$, $p > 5$ prime. A walk of length 3 originating at (a, b) will have its final vertex in the set

$$A = \{(z, yz^2 + ax^2 - b - xy^2) \colon x, y, z \in \mathbb{F}_p\}.$$

We show that $A = \mathbb{F}_p^2$, that is, we show that given any vertex $(u, v) \in V(D(p; 1, 2))$, we can find $x, y, z \in \mathbb{F}_p$ such that

$$\begin{cases} u = z, \\ v = yz^2 + ax^2 - b - xy^2. \end{cases}$$

If $u \neq 0$, set $(x, y, z) = (0, u^{-2}(b + v), u)$. If $u \neq 0$, by Lemma 2.8.1, $ax^2 - xy^2$ is a surjective function from $\mathbb{F}_p^2$ to $\mathbb{F}_p$ for every $a \in \mathbb{F}_p$, and so the equation $v = ax^2 - b - xy^2$ has a solution x, y for every $v \in \mathbb{F}_p$. The statement of the theorem now follows from Proposition 2.4.2.

In the graph $D(5; 1, 2)$ the shortest directed path between vertices $(1, 3)$ and $(0, 0)$ is of length 4. Finally, a computation shows that $\text{diam}(D(3; 1, 2)) = 3$. □

Chapter 3

ISOMORPHISMS AND AUTOMORPHISMS OF MONOMIAL DIGRAPHS

A natural question arises when dealing with our algebraically defined digraphs: when are two such digraphs isomorphic? Of course they must be of the same order, so we certainly need the number of defining equations to be the same for each graph. Is there a way to decide this matter by simply looking at some property of the defining functions? In general this seems to be a difficult question. In this chapter we focus on a special case, the case when both digraphs are defined in terms of one function only. We will further specialize by requiring that each function be a nonzero monomial of two variables. In fact, we can restrict our exploration to monic monomials, meaning functions of the form $f(x, y) = x^m y^n$, by noting that an isomorphism from $D(q; x^m y^n)$ to $D(q; ax^m y^n)$ (with $a \in \mathbb{F}_q^*$) is clearly given by $(x, y) \mapsto (x, ay)$.

One way to determine whether two digraphs are isomorphic is to choose a digraph property and show that one digraph satisfies this property while the other does not. In our case we will concentrate on the number of certain subdigraphs in each digraph.

This approach was successfully used in [27] and [10]. In [27], the number of 4-cycles was a graph invariant sufficient to settle the question about isomorphism of bipartite monomial graphs $B\Gamma(q; m, n) := B\Gamma(q; x^m y^n)$ for m, n fixed and q sufficiently large. In [10] this result was strengthened for all q by concentrating on the number of subgraphs isomorphic to the complete bipartite graph $K_{s,t}$, where s and t were chosen depending on m and n. Unfortunately, we have not found a single family of digraphs which would play a similar role for monomial digraphs $D(q; m, n)$. In this chapter we

present some results of our investigation of the isomorphism question, both theoretical and computational ones. The main result of this investigation is the following

Conjecture 3.0.2. *Let q be a prime power. The digraphs $D(q; m_1, n_1)$ and $D(q; m_2, n_2)$ are isomorphic if and only if there exists k, coprime with $q-1$, such that*

$$m_2 \equiv km_1 \mod (q-1),$$

$$n_2 \equiv kn_1 \mod (q-1).$$

3.1 Simple Results on Isomorphisms and Automorphisms

For any integer k, let $\overline{k}$ be the greatest common divisor of k and $q-1$. We start this section from the proof of sufficiency of Conjecture 3.7.1.

Theorem 3.1.1. *Let q be a prime power and k be an integer coprime with $q-1$. Suppose that $1 \leq m_1, n_1, m_2, n_2 \leq q-1$ are integers satisfying the relations*

$$m_1 \equiv km_2 \mod (q-1),$$

$$n_1 \equiv kn_2 \mod (q-1).$$

Then $D(q; m_1, n_1) \cong D(q; m_2, n_2)$.

Proof. Let $(x_1, x_2)(y_1, y_2)$ be an arc in $D(q; m_1, n_1)$ so that $x_2 + y_2 = x_1^{m_1} y_1^{n_1}$. Define the mapping $\phi\colon V(D(q; m_1, n_1)) \to V(D(q; m_2, n_2))$ via the rule

$$\phi\colon (x, y) \mapsto (x^k, y).$$

As k is coprime with $q-1$, ϕ is bijective and we check that ϕ preserves adjacency and non-adjacency. We have

$$\phi((x_1, x_2)) = (x_1^k, x_2),$$

$$\phi((y_1, y_2)) = (y_1^k, y_2),$$

so that

$$x_2 + y_2 = x_1^{m_1} y_1^{n_1} = (x_1^k)^{m_2} (y_1^k)^{n_2}.$$

Hence, $\phi((x_1, x_2))\phi((y_1, y_2)) = (x_1^k, x_2)(y_1^k, y_2)$ is an arc in $D(q; m_2, n_2)$, and ϕ is indeed an isomorphism from $D(q; m_1, n_1)$ to $D(q; m_2, n_2)$. □

The following two corollaries are of interest.

Corollary 3.1.2. *If* $\overline{m} = 1$ *and* $mn' \equiv n \mod q-1$, *then* $D(q;m,n) \cong D(q;1,n')$.

Proof. In Theorem 3.1.1, set $m_1 = m$, $n_1 = n$, $m_2 = 1$, $n_2 = n'$. Also set $k = [m^{-1}]_{q-1}$, the inverse of m modulo $q-1$, which exists as $\overline{m} = 1$. The result follows immediately. □

Corollary 3.1.3. *If* $n_1 n_2 \equiv 1 \mod (q-1)$, *then* $D(q;1,n_1) \cong D(q;n_2,1)$.

Proof. As $(q-1)|(n_1 n_2 - 1)$, no prime divisor of $q-1$ divides n_1 and so $\overline{n}_1 = 1$. The result now follows directly from Corollary 3.1.2. □

Proposition 3.1.4. *If* $m+n \equiv 0 \mod (q-1)$, *then* $D(q;m,n) \cong D(q;n,m)$, *and an isomorphism is defined via the rule*

$$(x,y) \mapsto \begin{cases} (x^{-1},y), & \text{if } x \neq 0, \\ (0,y), & \text{if } x = 0. \end{cases}$$

Proof. Let $D = D(q;m,n)$, $D' = D(q;n,m)$, and let $\phi\colon V(D) \to V(D')$ be defined as in the statement of the theorem. Clearly ϕ is a bijection. Let $(x_1,x_2),(y_1,y_2) \in V(D)$ and suppose there is an arc in D from (x_1,x_2) to (y_1,y_2). If $x_1 = 0$ or $y_1 = 0$ then trivially $\phi((x_1,x_2))\phi((y_1,y_2)) \in E(D')$. If $x_1 \neq 0$ and $y_1 \neq 0$, we still have $\phi((x_1,x_2))\phi((y_1,y_2)) \in E(D')$ since

$$x_2 + y_2 = x_1^m y_1^n = x_1^{-n} y_1^{-m} = (x_1^{-1})^n (y_1^{-1})^m.$$

Hence ϕ preserves adjacency and is an isomorphism from $D(q;m,n)$ to $D(q;n,m)$. □

Remark 3.1.5. The converse of Proposition 3.1.4 is not true, i.e. digraphs $D(q;m,n)$ and $D(q;n,m)$ can be isomorphic while $m+n \not\equiv 0 \mod (q-1)$. By Corollary 3.1.3, the digraphs $D(17;1,7)$ and $D(17;7,1)$ are isomorphic, and one isomorphism between them is given by the rule $(x,y) \mapsto (x^7,y)$. By the same corollary, the digraphs $D(9;1,5)$ and $D(9;5,1)$ are also isomorphic, and one isomorphism between them is given by the rule $(x,y) \mapsto (x^5,y)$.

Concerning automorphisms of $D(q;m,n)$ we have the following proposition.

Proposition 3.1.6. *For any $a \in \mathbb{F}_q^*$, the mapping $\phi_a\colon (x,y) \mapsto (ax, a^{m+n}y)$ is an automorphism of $D(q;m,n)$. In particular, the group of automorphisms of $D(q;m,n)$ contains a cyclic subgroup of order $q-1$ generated by ϕ_g, where $\langle g\rangle = \mathbb{F}_q^*$.*

Proof. The mapping ϕ_a is trivially bijective; also if there is an arc from (x_1,x_2) to (y_1,y_2), there is an arc from $\phi_a((x_1,x_2)) = (ax_1, a^{m+n}x_2)$ to $\phi_a((y_1,y_2)) = (ay_1, a^{m+n}y_2)$. Thus ϕ_a preserves adjacency. Clearly $\langle\phi_g\rangle$ is a cyclic group of automorphisms of $D(q;m,n)$. □

3.2 Auxiliary Results and Notation

In the following, (m,n) denotes the greatest common divisor of two integers m and n. By $I_m(a)$, $m \in \mathbb{Z}$, $a \in \mathbb{F}_q$, we denote $\{x \in \mathbb{F}_q\colon x^m = a\}$. We write I_m for $I_m(1)$. Note that $I_0 = \mathbb{F}_q^*$. Let ξ be a generator of the multiplicative group $\mathbb{F}_q^*$ of the finite field $\mathbb{F}_q$. As in Section 2.2, $A_n = \{x^n\colon x \in \mathbb{F}_q\}$, $A_n^* = A_n \setminus \{0\}$.

The following four propositions are well-known elementary results on cyclic groups. See Dummit and Foote [12] for details.

Proposition 3.2.1 ([12], p. 57)**.** *If G is a group, and $x \in G$ of order $o(x) = n$, then $o(x^m) = \frac{n}{(m,n)}$ for any $m \in \mathbb{Z}$.*

Proposition 3.2.2. *If G is a group and $x \in G$, $m,n \in \mathbb{Z}$, then $\langle x^m\rangle \cap \langle x^n\rangle = \langle x^l\rangle$, where $l = lcm(m,n)$.*

Proposition 3.2.3. *$A_m^* \le \mathbb{F}_q^*$ with $A_m^* = \langle\xi^m\rangle = \langle\xi^{\overline{m}}\rangle$ and $|A_m^*| = \dfrac{q-1}{\overline{m}}$.*

Proposition 3.2.4. *$A_m^* \cap A_n^* = \langle\xi^l\rangle = \langle\xi^{\bar{l}}\rangle$, where $l = lcm(m,n)$, and so $|A_m^* \cap A_n^*| = \dfrac{q-1}{\bar{l}}$.*

Proposition 3.2.5. *$|I_m| = \overline{m}$, and*

$$I_m = \langle\xi^{\frac{q-1}{\overline{m}}}\rangle = \{1, \xi^{\frac{q-1}{\overline{m}}}, \xi^{\frac{q-1}{\overline{m}}\cdot 2}, \ldots, \xi^{\frac{q-1}{\overline{m}}\cdot(\overline{m}-1)}\}.$$

Likewise, for any $a \in A_m^*$, $|I_m(a)| = \overline{m}$; moreover, if $x \in I_m(a)$, then

$$I_m(a) = \{x\varepsilon_0, x\varepsilon_1, \ldots, x\varepsilon_{\overline{m}-1}\}, \quad \varepsilon_i = \xi^{\frac{q-1}{\overline{m}}i}, \quad 0 \le i \le \overline{m} - 1.$$

Proof. From Proposition 3.2.3, $\{x^m \colon x \in \mathbb{F}_q\} = \{x^{\overline{m}} \colon x \in \mathbb{F}_q\}$, and so $|I_m| = |I_{\overline{m}}| \le \overline{m}$. Clearly, $\xi^{\frac{q-1}{\overline{m}} \cdot i} \in I_m$ for i, $1 \le i \le \overline{m} - 1$, and all these are distinct. Hence

$$|I_m| = \overline{m}, \text{ and } I_m = \langle \xi^{\frac{q-1}{\overline{m}}} \rangle.$$

The same argument can be applied to prove the rest of the proposition. □

Proposition 3.2.6. *We have*

$$|I_m \cap I_n| = (q-1, m, n) = (\overline{m}, \overline{n}).$$

Proof. Let M and N be such that $q - 1 = M\overline{m} = N\overline{n}$. Let $d = (\overline{m}, \overline{n})$, so that $\overline{m} = dm'$ and $\overline{n} = dn'$ for some integers m' and n' for which $(m', n') = 1$. Then $q-1 = dm'M = dn'N$ and $(q-1)/d = m'M = n'N$. As $(m', n') = 1$, we have $M = n't$ and $N = m't$ for some integer t. This implies that $q - 1 = dm'n't$. Thus,

$$\frac{q-1}{\overline{m}} = n't, \quad \frac{q-1}{\overline{n}} = m't.$$

This yields

$$lcm(\frac{q-1}{\bar{m}}, \frac{q-1}{\bar{n}}) = lcm(n't, m't) = \frac{n'tm't}{(n't, m't)} = m'n't.$$

Hence,

$$|I_m \cap I_n| = |\langle \xi^{\frac{q-1}{\bar{m}}} \rangle \cap \langle \xi^{\frac{q-1}{\bar{n}}} \rangle| = |\langle \xi^{lcm(\frac{q-1}{\bar{m}}, \frac{q-1}{\bar{n}})} \rangle|$$

$$= \frac{q-1}{(q-1, lcm(\frac{q-1}{\bar{m}}, \frac{q-1}{\bar{n}}))} = \frac{q-1}{(q-1, m'n't)} = \frac{q-1}{m'n't} = \frac{dm'n't}{m'n't} = d.$$

□

Proposition 3.2.7. *The number of elements α in $\mathbb{F}_q^*$ for which the system of equations $x^m = x^n = \alpha$ has a solution is*

$$\frac{\overline{m-n}}{|I_{m-n} \cap I_n|}.$$

Proof. If for some $x \in \mathbb{F}_q^*$, $x^m = x^n$, then $x^{m-n} = 1$ and $x \in I_{m-n}$. Let ϕ be a homomorphism defined on I_{m-n} via $x \mapsto x^n$. Then

$$\ker \phi = \{x \in I_{m-n} \colon x^n = 1\} = I_{m-n} \cap I_n.$$

By the first isomorphism theorem,

$$|\{\alpha \in \mathbb{F}_q^* | \, \exists x \in \mathbb{F}_q^* \colon x^m = x^n = \alpha\}| = \frac{|I_{m-n}|}{|\ker \phi|} = \frac{\overline{m-n}}{|I_{m-n} \cap I_n|}.$$

□

Proposition 3.2.8. *For any given $\alpha \in \mathbb{F}_q^*$, the set $\{x \in \mathbb{F}_q \colon x^m = x^n = \alpha\}$ is either empty or contains $|I_m \cap I_n| = (\overline{m}, \overline{n})$ elements. That is, for any $\alpha \in \mathbb{F}_q^*$,*

$$|I_m(\alpha) \cap I_n(\alpha)| \in \{(\overline{m}, \overline{n}), 0\}.$$

Proof. If there exists $x \in \mathbb{F}_q$ such that $x^m = x^n = \alpha$, then any other element y of the field with the same property satisfies $\left(\frac{y}{x}\right)^m = \left(\frac{y}{x}\right)^n = 1$. Choose any such x and $t \in I_m \cap I_n$ and set $y = tx$. □

3.3 Number of Small Cycles

In this section we give formulas for the number of cycles of length 1 (loops), 2 and 3, and some formulas for the number of cycles of length 4.

Proposition 3.3.1. *The digraph $D(q; m, n)$ has q loops for any q and any m, n.*

Proof. Suppose first that q is odd. If (x, y) is adjacent to itself, then $y = 2^{-1}x^{m+n}$. Hence any vertex of the form $(x, 2^{-1}x^{m+n})$, $x \in \mathbb{F}_q$, is a loop. If q is even, then the only vertices that have loops on them are those of the form $(0, y)$, $y \in \mathbb{F}_q$. □

Proposition 3.3.2. *If q is odd, then the number of 2-cycles in the digraph $D(q; m, n)$ is given by*

$$\frac{1}{2}q(q-1)(2 + \overline{m-n}).$$

Proof. Counting the number of 2-cycles in $D(q;m,n)$ is equivalent to counting the number of solutions of the system

$$\begin{cases} x_2 + y_2 = x_1^m y_1^n, \\ x_2 + y_2 = x_1^n y_1^m \end{cases} \tag{3.1}$$

subject to constraint $(x_1, x_2) \neq (y_1, y_2)$. If $x_1 y_1 = 0$ consider three cases: 1) if $x_1 = 0$ and $y_1 \neq 0$, then y_1 can be choses in $q-1$ ways, x_2 in q ways and we obtain a solution corresponding to the 2-cycle of the form $(0, x_2) \to (y_1, -x_2)$ (or its reverse). There are $q(q-1)$ of them; 2) if $x_1 \neq 0$, $y_1 = 0$, then the same counting argument applies; 3) if $x_1 = y_1 = 0$, then x_2 can be chosen to be any element of $\mathbb{F}_q^*$, and $y_2 = -x_2$. Overall we have

$$q(q-1) + q(q-1) + q - 1 = (2q+1)(q-1)$$

solutions for which $x_1 y_1 = 0$.

If $x_1 y_1 \neq 0$, then (3.1) yields $(x_1 y_1^{-1})^{m-n} = 1$. Let $z = x_1 y_1^{-1}$. The equation $z^{m-n} = 1$ has precisely $d := \overline{m-n}$ solutions z, $z \in I_{m-n}$. If $z = 1$, then $x_1 = y_1$, and there are $q-1$ choices for their common value. One then chooses x_2 in $q-1$ ways such that $y_2 \neq x_2$ is determined uniquely. Thus we obtain $(q-1)^2$ solutions in the case $z = 1$. If $z \neq 1$, choose $y_1 \in \mathbb{F}_q^*$ in $q-1$ ways, $x_2 \in \mathbb{F}_q$ in q ways, and then y_2 is determined uniquely. Thus for every $z \in I_m \setminus \{1\}$, there are $q(q-1)$ solutions.

Overall there are

$$(q-1)(2q+1) + (q-1)^2 + q(d-1)(q-1) = q(q-1)(2+d)$$

solutions of (3.1). The total number is half of this quantity as vertices (x_1, x_2) and (y_1, y_2) can be swapped. □

Proposition 3.3.3. *If q is odd, the number of 3-cycles in the digraph $D(q;m,n)$ is given by*

$$\frac{1}{3} q(q-1)(q-2) + (q-1)(q - \overline{m-n} - 1).$$

Proof. Suppose that three vertices (x_1, x_2), (y_1, y_2) and (z_1, z_2) form a 3-cycle in $D(q, m, n)$. Then

$$\begin{cases} x_2 = 2^{-1}(x_1^m y_1^n + z_1^m x_1^n - y_1^m z_1^n), \\ y_2 = 2^{-1}(x_1^m y_1^n + y_1^m z_1^n - z_1^m x_1^n), \\ z_2 = 2^{-1}(y_1^m z_1^n + z_1^m x_1^n - x_1^m y_1^n), \end{cases} \tag{3.2}$$

so that the choice of the first coordinates x_1, y_1 and z_1 uniquely determines the second coordinates x_2, y_2 and z_2.

If the first three coordinates are distinct, then there are $q(q-1)(q-2)$ ways to choose an ordered triple (x_1, y_1, z_1).

Suppose that, say, $x_1 = y_1 \neq z_1$. Then clearly $x_1 \neq 0$, since otherwise $x_2 = y_2$ and $x_1 = y_1$, and the two vertices are not distinct. The same argument shows that $z_1 \neq 0$. Since $x_1 = y_1$, we have to ensure that $x_2 \neq y_2$, that is, that $(x_1 z_1^{-1})^{m-n} \neq 1$. This implies $x_1 z_1^{-1} \notin I_{m-n} \cup \{0\}$. One may choose $z_1 \in \mathbb{F}_q^*$ in $q-1$ ways, and a value for $x_1 z_1^{-1}$ in $(q-(d+1))$ ways, $d = \overline{m-n}$, so that the number of solutions of this type is $(q-1)(q-d-1)$. The other two cases, $x_1 = z_1 \neq y_1$ and $y_1 = z_1 \neq x_1$ are dealt with similarly.

If (x_1, x_2), (y_1, y_2) and (z_1, z_2) are a solution of (3.2), then any permutation of order 3 on these vertices results in the same 3-cycle. Hence the number of 3-cycles of $D(q; m, n)$ is as claimed. □

Counting the number of 4-cycles in the general graph $D(q; m, n)$ seems to be a hard problem. We count it only in certain particular cases.

Proposition 3.3.4. *If q is odd, the number of 4-cycles in the digraph $D(q; q-1, q-1)$ is given by*

$$\frac{1}{4}(q-1)(q-2)\{q(q-3) + (q-1)^2(q+2)\}.$$

Proof. Assume vertices (a_1, a_2), (b_1, b_2), (c_1, c_2) and (d_1, d_2) are the four consecutive vertices of a 4-cycle in $D = D(q; q-1, q-1)$. This translates into the following system of equations:

$$\begin{cases} a_2 + b_2 = (a_1 b_1)^{q-1}, \\ b_2 + c_2 = (b_1 c_1)^{q-1}, \\ c_2 + d_2 = (c_1 d_1)^{q-1}, \\ d_2 + a_2 = (d_1 a_1)^{q-1}. \end{cases} \tag{3.3}$$

Assume first that none of a_1, b_1, c_1 or d_1 is 0. Then the right-hand sides above are trivially 1's, and the system has a 1-parameter solution

$$(a_2, b_2, c_2, d_2) = (a_2, 1 - a_2, a_2, 1 - a_2).$$

If $a_2 = 2^{-1}$ and so $a_2 = 1 - a_2$, then we must have a_1, b_1, c_1 and d_1 all distinct. If, however, $a_2 \neq 2^{-1}$, then it is enough to require $a_1 \neq c_1$ and $b_1 \neq c_1$. There are

$$\frac{1}{4}\{1 \cdot (q-1)(q-2)(q-3)(q-4) + (q-1)(q-1)^2(q-2)^2\}$$

cycles of this type where division by 4 corresponds to counting unordered 4-tuples.

If some two of the first coordinates a_1, b_1, c_1 or d_1 equal 0, it is easy to see that system (3.3) has no solutions. So suppose now that $a_1 = 0$, but the other three first coordinates b_1, c_1 and d_1 are nonzero. System (3.3) again has a 1-parameter solution

$$(a_2, b_2, c_2, d_2) = (a_2, -a_2, 1 + a_2, -a_2).$$

If $a_2 = -2^{-1}$ and so $1 + a_2 = -a_2$, then we require that b_1, c_1 and d_1 all be distinct. If, however, $a_2 \neq -2^{-1}$, then we only require that $b_1 \neq d_1$. There are

$$4 \cdot \frac{1}{4}\{1 \cdot (q-1)(q-2)(q-3) + (q-1)(q-1)(q-1)(q-2)\}$$

cycles of this type. Division by 4 corresponds to counting only unordered 4-tuples while multiplication by 4 accounts for 4 possible choices for a zero first coordinate. Taken together the number of 4-cycles in $D(q; q-1, q-1)$ is

$$\frac{1}{4}(q-1)(q-2)\{q(q-3) + (q-1)^2(q+2)\}.$$

□

Proposition 3.3.5. *If $\overline{m} = 1$, then $D(q; m, m)$ has no 4-cycles.*

Proof. Assume vertices (a_1, a_2), (b_1, b_2), (c_1, c_2) and (d_1, d_2) are the four consecutive vertices of a 4-cycle in $D = D(q; m, m)$. This translates into the following system of equations:

$$\begin{cases} a_2 + b_2 = (a_1 b_1)^m, \\ b_2 + c_2 = (b_1 c_1)^m, \\ c_2 + d_2 = (c_1 d_1)^m, \\ d_2 + a_2 = (d_1 a_1)^m. \end{cases} \tag{3.4}$$

This system only has solutions if $(a_1^m - c_1^m)(b_1^m - d_1^m) = 0$. If, say $a_1^m = c_1^m$, then $\overline{m} = 1$ implies that $a_1 = c_1$. But then $a_2 = c_2$. Likewise, if $b_1^m = d_1^m$, then $b_1 = d_1$ and $b_2 = d_2$. Hence system (3.4) has no solutions satisfying the restriction that (a_1, a_2), (b_1, b_2), (c_1, c_2) and (d_1, d_2) be distinct. □

3.4 Looped Paths in $D(q; 1, n)$

For any positive integer k we define a *looped path of length k* to be a directed path of length k in which every vertex is adjacent to itself.

Although we could not find an explicit formula for the number of looped paths of length k in $D(q; 1, n)$, we have a simple way of computing them based on the number of roots of a certain polynomial equation, which can be easily done by a computer. It gives us a convenient invariant for verifying isomorphism between digraphs $D(q; 1, n)$ and $D(q; 1, n')$ by a computer. It was used together with other invariants to arrive at Conjecture 3.7.1. Another feature of this invariant is that it gives a graph theory approach of proving that certain polynomials over finite fields have equal number of roots.

Let (a, x) be the tail and (b, y) be the head of a looped path of length 1 in $D(q; 1, n)$. Since there is a loop on each of these vertices, $x = \frac{1}{2}a^{n+1}$, $y = \frac{1}{2}b^{n+1}$, and

$a^{n+1}+b^{n+1}=2ab^n$. Clearly $a \neq b$, and none of them is zero. It follows that $\frac{a}{b}$ is a root of the equation

$$t^{n+1}-2t+1=0 \tag{3.5}$$

different from 1.

Let $F(n)$ be the number of roots of this equation different from 1, so $0 \leq F(n) \leq n$. It follows that the digraph $D(q;1,n)$ has $(q-1)F(n)$ looped paths of length 1, as the choice of a root of (3.5) and a choice of a determine b uniquely.

Assume now that $(a, \frac{1}{2}a^{n+1})$, $(b, \frac{1}{2}b^{n+1})$ and $(c, \frac{1}{2}c^{n+1})$ are three distinct consecutive vertices of a looped path of length 2. Then

$$\begin{cases} a^{n+1}+b^{n+1}=2ab^n, \\ b^{n+1}+c^{n+1}=2bc^n, \end{cases}$$

where $abc \neq 0$ and a, b and c are all distinct. It follows from this system that the ratios $\frac{a}{b}$ and $\frac{b}{c}$ are both roots of (3.5) different from 1.

Suppose both $\frac{a}{b}$ and $\frac{b}{c}$ are equal to the same root t different from 1. Clearly, $a \neq b$ and $b \neq c$. We claim that $a \neq c$, for otherwise it follows that $t^2=1$. Clearly, $t=-1$ is not a root of (3.5), and if $t=1$, it follows that $a=b=c$. This case yields $(q-1)F(n)$ looped paths of length 2.

Suppose $\frac{a}{b}=t_1 \neq t_2=\frac{b}{c}$, where t_1 and t_2 are roots of (3.5) with $t_1, t_2 \neq 1$. We again need to ensure that $a \neq c$. If $a=c$, then $t_1t_2=1$. As $t_1^{n+1}-2t_1+1=0$ and $t_1^{-(n+1)}-2t_1^{-1}+1=0$, it follows that $t_1^{n-1}=1$, and so $t_1^2-2t_1+1=0$, or $t_1=1$. Therefore $a \neq c$ and this case yields $F(n)(F(n)-1)(q-1)$ looped paths of length 2. Hence there are $F(n)^2(q-1)$ of them in $D(q;1,n)$.

The following proposition gives additional information about the roots of (3.5).

Proposition 3.4.1. *The polynomial $T(t)=t^{n+1}-2t+1$ has no multiple root over any finite field $\mathbb{F}_q$ for $n>1$.*

Proof. We verify that T and its formal derivative $T'(t) = (n+1)t^n - 2$ are coprime, that is, that (T, T') is a constant polynomial. Assume by contradiction that (T, T') is of degree at least 1. If $p|(n+1)$, the result follows immediately. Otherwise note that

$$(n+1)T(n) - tT'(t) = -2nt + n + 1.$$

If $p|n$ then the result follows immediately. Otherwise (T, T') is of degree 1 and has $\frac{n+1}{2n}$ as its root. This implies that $T'(\frac{n+1}{2n}) = 0$ or, equivalently,

$$\frac{(n+1)^{n+1}}{(2n)^n} = 2. \tag{3.6}$$

Let $r(n) = \frac{(n+1)^{n+1}}{(2n)^n} - 2$. Clearly $r(1) = 0$. It is easy to check that

$$r'(n) = \frac{(n+1)^{n+1}(\ln(n+1) - \ln n - \ln 2)}{(2n)^n} < 0$$

for $n > 1$. Thus $T'(\frac{n+1}{2n}) \neq 0$ for $n > 1$, and a contradiction is obtained. □

We tried to count the number of looped paths of length 1 and 2 in digraphs $D(q; 1, n)$ in order to prove Conjecture 3.7.1 in the case $m_1 = m_2 = 1$. The idea looked promising especially in light of Proposition 3.1.2. Numerous computer verifications however showed that these invariants cannot distinguish digraphs $D(q; 1, n_1)$ and $D(q; 1, n_2)$ when $n_1 n_2 \equiv 1 \mod (q-1)$ which we conjecture are never isomorphic unless $n_1 = n_2$. Indeed, the following proposition explains why the two invariants are not discriminating enough.

Proposition 3.4.2. *If $n_1 \cdot n_2 \equiv 1 \mod (q-1)$, the equations*

$$t^{n_1+1} - 2t + 1 = 0, \tag{3.7}$$

$$t^{n_2+1} - 2t + 1 = 0,$$

have equal number of roots in $\mathbb{F}_q$.

Proof. This proof is due S. De Winter [29]. Define the sets S_{n_1} and S_{n_2} as follows:

$$S_{n_1} := \{x \in \mathbb{F}_q \colon f(x) = x^{n_1+1} - 2x + 1 = 0\},$$

$$S_{n_2} := \{x \in \mathbb{F}_q \colon f(x) = x^{n_2+1} - 2x + 1 = 0\}.$$

We prove that S_{n_1} and S_{n_2} have the same cardinality.

As $q-1 | n_1 n_2 - 1$, it follows that no prime divisor of $q-1$ divides n_1 or n_2, hence $(q-1, n_1) = (q-1, n_2) = 1$. This implies that the mappings

$$\mu_i \colon \mathbb{F}_q^* \to \mathbb{F}_q^*,\ x \mapsto x^{-i},\ i = n_1, n_2$$

are bijections. It is easy to verify that for any $z \in S_{n_1}$, $z^{n_1+1} g(z^{-n_1}) = 0$, and so $g(z^{-n_1}) = 0$. Consequently μ_{n_1}, when restricted to S_{n_1}, is an injective map from S_{n_1} into S_{n_2}. In exactly the same way μ_{n_2}, when restricted to S_{n_2}, is an injective map from S_{n_2} into S_{n_1}. Hence we have established a bijection between S_{n_1} and S_{n_2}, proving both sets have the same cardinality. □

We now give a graph-theoretic proof of Proposition 3.4.2.

Proof. By Proposition 3.1.3, the digraphs $D(q; 1, n_1)$ and $D(q; n_2, 1)$ are isomorphic. Recall that the converse of a digraph H is a digraph obtained by reversing the directions of all arcs in H. Let us denote H^c the converse of any digraph H. Let H be a subdigraph of $D(q; 1, n_1)$ isomorphic to a looped path of length 1. Note that $D(q; 1, n_2)$ can be obtained from $D(q; n_2, 1)$ by reversing the directions of all arcs, that is, the two digraphs are the converses of each other. Thus, the number of subdigraphs in $D(q; 1, n_2)$ isomorphic to H equals the number of subdigraphs in $D(q; n_2, 1)$ isomorphic to H^c. Trivially, $H \cong H^c$. Hence, $D(q; 1, n_2)$ and $D(q; n_2, 1)$ have equal number of subdigraphs isomorphic to H, which is equal to the number of subdigraphs in $D(q; 1, n_1)$ isomorphic to H. By an argument above, a digraph $D(q; 1, n)$ has $(q-1)F(n)$ subdigraphs isomorphic to H. Thus, $F(n_1) = F(n_2)$, and the corresponding equations have equally many roots. □

3.5 Number of $K_{2,2}$'s in $D(q; m, n)$

As was discussed at the beginning of this chapter, one idea to determine whether two given digraphs $D(q; m_1, n_1)$ and $D(q; m_2, n_2)$ are isomorphic could be to count the

number of certain subdigraphs in these two digraphs. In particular, of special interest are such subdigraphs of $D(q;m,n)$ whose number can be expressed explicitly as a function of its parameters m,n. We believe that this can be done for any subdigraph of $D(q;m,n)$ isomorphic to a complete bipartite graph $K_{s,t}$ in which all arcs are directed from the vertices of the partition of size s to the vertices of the partition of size t. Let us denote this digraph by $\overrightarrow{K}_{s,t}$. We remind the reader that for two undirected bipartite monomial graphs $B\Gamma(q;m,n)$ and $B\Gamma(q;m',n')$ considered in [27] and [10], it was possible to determine $s,t\geq 2$ such that the equality of the number of copies of $K_{s,t}$ in these graphs completely determined whether they were isomorphic. There it was possible since these numbers were computed explicitly. Unfortunately, we are unable to compute the number of copies of $\overrightarrow{K}_{s,t}$ in monomial digraphs $D(q;m,n)$ for $s,t>2$. Below we present the computation for the number of copies of $\overrightarrow{K}_{2,2}$ in $D(q;m,n)$, the only case we have succeeded so far. This computation was useful in determining non-isomorphisms of some pairs of monomial digraphs.

Throughout this section, for any two integers m and n, by (m,n) we denote the greatest common divisor of m and n.

Let $\mathbf{x}=(x_1,x_2)$, $\mathbf{y}=(y_1,y_2)$, $\mathbf{z}=(z_1,z_2)$, $\mathbf{w}=(w_1,w_2)$, be the vertices of any subdigraph of $D(q;m,n)$ isomorphic to $\overrightarrow{K}_{22}$ such that

$$\deg^+(\mathbf{x})=\deg^+(\mathbf{y})=\deg^-(\mathbf{z})=\deg^-(\mathbf{w})=2.$$

Throughout this section this digraph will be denoted by $\overrightarrow{K}_{2,2}$.

Theorem 3.5.1. *In the graph $D(q;m,n)$, q odd, the number of subdigraphs isomorphic to $\overrightarrow{K}_{2,2}$ (with a particular orientation of arcs described above) is given by*

$$\frac{1}{4|I_{m-n}\cap I_n|}(q-1)\times \tag{3.8}$$

$$\Big\{q^3|I_{m-n}\cap I_n|\Big(|I_m|+|I_n|-2\Big)+q^2|I_{m-n}\cap I_n|\Big(1-|I_m||I_n|\Big)+q|I_{m-n}\cap I_n|\Big(9+|I_m|(|I_n|-5)-5|I_n|\Big)$$

$$+2|I_{m-n}\cap I_n|\Big(-3+2|I_m||I_n|+|I_m\cap I_n|+|I_m\cap I_n|+2|I_{m-n}|[-2+|I_m|+|I_n|-|I_m||I_n|+|I_m\cap I_n|]\Big)$$

$$-4|I_m \cap I_n||I_{m-n}|\Big(-2+|I_m|+|I_n|-|I_m||I_n|+|I_m \cap I_n|\Big)\Big\}.$$

Proof. If $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$ and $\mathbf{w}$ are as above, then

$$\begin{cases} x_2+z_2 &= x_1^m z_1^n, \\ x_2+w_2 &= x_1^m w_1^n, \\ y_2+z_2 &= y_1^m z_1^n, \\ y_2+w_2 &= y_1^m w_1^n, \end{cases} \tag{3.9}$$

and also $x_1 \neq y_1$ and $z_1 \neq w_1$. It is easy to check that this system has a solution if and only if

$$x_1^m = y_1^m \text{ or } z_1^n = w_1^n. \tag{3.10}$$

From this system we find the second coordinates x_2, y_2 and z_2 expressed through the free parameter w_2:

$$\begin{cases} x_2 &= x_1^m w_1^n - w_2, \\ y_2 &= -x_1^m z_1^n + x_1^m w_1^n + y_1^m z_1^n - w_2, \\ z_2 &= x_1^m z_1^n - x_1^m w_1^n + w_2. \end{cases} \tag{3.11}$$

Note that the first coordinates are either all distinct, or exactly three of them are equal, or there are exactly two equal pairs among them. Clearly all of the first coordinates could not be equal. We treat the three possible cases separately.

A. *The first coordinates x_1, y_1, z_1 and w_1 are all distinct.*

In this case the second coordiantes can assume any values in $\mathbb{F}_q$ provided that they satisfy system (3.11). We therefore count the number of ordered 4-tuples that could be the first coordinates of the 4 vertices of a subdigraph of $D(q;m,n)$ isomorphic to $\overrightarrow{K}_{22}$.

We further subdivide condition (3.10) in the following subcases and give the number α of the 4 first ordered coordinates in each of them.

Case 1. $x_1^m = y_1^m$, $z_1^n \neq w_1^n$.

If $z_1 \neq 0$ consider the following subcases.

Case 1.1. $x_1^n = y_1^n = z_1^n$.

$\alpha = (q-1)(|I_m \cap I_n| - 1)(|I_n| - 2)(q - |I_n|)$.

Case 1.2. $x_1^n \neq y_1^n$, $x_1^n = z_1^n$.

$\alpha = (q-1)(|I_m| - |I_m \cap I_n|)(|I_n| - 1)(q - |I_n| - 1)$.

Case 1.3. $x_1^n \neq y_1^n$, $y_1^n = z_1^n$.

$\alpha = (q-1)(|I_m| - |I_m \cap I_n|)(|I_n| - 1)(q - |I_n| - 1)$.

Case 1.4. $x_1^n \neq y_1^n$, $x_1^n \neq z_1^n$, $y_1^n \neq z_1^n$.

$\alpha = (q-1)(|I_m| - |I_m \cap I_n|)(q - 1 - 2|I_n|)(q - |I_n| - 2)$.

Case 1.5. $x_1^n = y_1^n \neq z_1^n$.

$\alpha = (q-1)(|I_m \cap I_n| - 1)(q - 1 - |I_n|)(q - |I_n| - 2)$.

If $z_1 = 0$, then we have $\alpha = (q-1)(|I_m| - 1)(q-3)$.

Case 2. $x_1^m \neq y_1^n$, $z_1^n = w_1^n$.

This case is symmetric to the previous through the bijection

$$(m, n, x, y, z, w) \to (n, m, z, w, x, y).$$

Case 3. $x_1^m = y_1^m$, $z_1^n = w_1^n$.

Case 3.1. $x_1^n = y_1^n = z_1^n = w_1^n$.

$\alpha = (q-1)(|I_m \cap I_n| - 1)(|I_n| - 2)(|I_n| - 3)$.

Case 3.2. $x_1^n = y_1^n \neq z_1^n = w_1^n$.

$\alpha = (q-1)(|I_m \cap I_n| - 1)(q - 1 - |I_n|)(|I_n| - 1)$.

Case 3.3. $x_1^n \neq y_1^n$, $x_1^n = z_1^n = w_1^n$.

$\alpha = (q-1)(|I_m| - |I_m \cap I_n|)(|I_n| - 1)(|I_n| - 2)$.

Case 3.4. $x_1^n \neq y_1^n$, $y_1^n = z_1^n = w_1^n$.

$\alpha = (q-1)(|I_m| - |I_m \cap I_n|)(|I_n| - 1)(|I_n| - 2)$.

Case 3.5. $x_1^n \neq y_1^n$, $x_1^n \neq z_1^n$, $y_1^n \neq w_1^n$.

$\alpha = (q-1)(|I_m| - |I_m \cap I_n|)(q - 1 - 2|I_n|)(|I_n| - 1)$.

Since the free parameter w_2 in (3.11) can be chosen to be any element of $\mathbb{F}_q$, and the first coordinates were counted as an ordered 4-tuple, the overall number of subdigraphs of $D(q;m,n)$ isomorphic to $\overrightarrow{K}_{22}$ in case **A** is given by

$$\frac{1}{4}q(q-1)\Big\{q^2(|I_m|+|I_n|-2)-q\Big(|I_m|(|I_n|+4)+4|I_n|-9\Big)+|I_m|+|I_n|+5|I_m||I_n|-2|I_m\cap I_n|-5\Big\}. \tag{3.12}$$

B. *There are exactly three distinct first coordinates among x_1, y_1, z_1 and w_1.*

Without loss of generality let us assume that $x_1 = z_1$ and $y_1 \neq w_1$. We will have to ensure that $x_2 \neq z_2$ for otherwise $\mathbf{x} = \mathbf{z}$.

Condition (3.10) yields three possible subcases:

Case 1. $x_1^m = y_1^m$, $x_1^n \neq w_1^n$.

By (3.11), condition $x_2 \neq z_2$ translates in this case to $w_2 \neq x_1^m(w_1^n - \frac{1}{2}x_1^n)$. That is, there is only one forbidden value for the free parameter w_2.

We further subdivide condition (3.10) in the following subcases and give the number α of the 4 first ordered coordinataes in each of them.

Case 1.1 $x_1^n = y_1^n \neq w_1^n$

$\alpha = (q-1)(|I_m \cap I_n| - 1)(q - |I_n|)$.

Case 1.2 $x_1^n \neq y_1^n$, $y_1^n = w_1^n$

$\alpha = (q-1)(|I_m| - |I_m \cap I_n|)(q - |I_n|)$.

Case 1.3 $x_1^n \neq y_1^n$, $y_1^n \neq w_1^n$

$\alpha = (q-1)(|I_m| - |I_m \cap I_n|)(q - 2|I_n|)$.

Therefore the number of digraphs in **Case 1** is

$$(q-1)^2\Big\{(|I_m|-1)(q-|I_n|-1)+|I_m\cap I_n|-1\Big\}. \tag{3.13}$$

Case 2. $x_1^m \neq y_1^m$, $x_1^n = w_1^n$.

This case is symmetric to the previous through the bijection

$$(m,n,x_1,y_1,w_1) \to (n,m,x_1,w_1,y_1).$$

The only forbidden values for the free parameter w_2 is $\frac{1}{2}x_1^{m+n}$. So we have the following number of graphs:

$$(q-1)^2\Big\{(|I_n|-1)(q-|I_m|-1)+|I_m\cap I_n|-1\Big\}. \tag{3.14}$$

Case 3. $x_1^m = y_1^m$, $x_1^n = w_1^n$.

In this case we have $x_2 = z_2$ if and only if $w_2 = \frac{1}{2}x_1^{m+n}$, and so there is only one forbidden value for w_2.

Case 3.1. $x_1^m = x_1^n$.

Let $a = x_1^m = x_1^n$. By Proposition 3.2.7, there are

$$\frac{\overline{m-n}}{|I_{m-n}\cap I_n|}$$

$a \in \mathbb{F}_q$ for which the equation $a = x_1^m = x_1^n$ is solvable. Fix any such a and consider the following subcases:

Case 3.1.1. $x_1 \in I_m(a)\cap I_n(a)$, $y_1 \in I_m(a)\setminus I_n(a)$, $w_1 \in I_n(a)\setminus I_m(a)$.

Choose x_1 in $|I_m\cap I_n|$ ways; y_1 in $|I_m|-|I_m\cap I_n|$ ways; w_1 in $|I_n|-|I_m\cap I_n|$ ways.

Case 3.1.2. $x_1 \in I_m(a)\cap I_n(a)$, $y_1 \in I_m(a)\setminus I_n(a)$, $w_1 \in I_n(a)\cap I_m(a)$.

Choose x_1 in $|I_m\cap I_n|$ ways; y_1 in $|I_m|-|I_m\cap I_n|$ ways; w_1 in $|I_m\cap I_n|-1$ ways.

Case 3.1.3. $x_1 \in I_m(a)\cap I_n(a)$, $y_1 \in I_m(a)\cap I_n(a)$, $w_1 \in I_n(a)\setminus I_m(a)$.

Choose x_1 in $|I_m\cap I_n|$ ways; y_1 in $|I_m\cap I_n|-1$ ways; w_1 in $|I_n|-|I_m\cap I_n|$ ways.

Case 3.1.4. $x_1, y_1, w_1 \in I_m(a)\cap I_n(a)$.

Choose x_1, y_1 and w_1 in $(|I_m\cap I_n|)(|I_m\cap I_n|-1)(|I_m\cap I_n|-2)$ ways.

Case 3.2. $x_1^m \neq x_1^n$.

Choose $x_1 \in \mathbb{F}_q^*\setminus I_{m-n}$ in $q-1-|I_{m-n}|$ ways. As $x_1 \neq 0$, we may set $r = \frac{y_1}{x_1}$ and $s = \frac{w_1}{x_1}$. Clearly the choices of r and s determine y_1 and w_1, respectively, uniquely once x_1 is chosen. Consider the following subcases. We have $r \in I_m\setminus\{1\}$ and $s \in I_n\setminus\{1\}$ and need to ensure that $r \neq s$ since otherwise $y_1 = w_1$.

Case 3.2.1. $r \in I_m\setminus I_n$, $s \in I_n\setminus I_m$.

The pair (r,s) can be chosen in $(|I_m|-|I_m\cap I_n|)(|I_n|-|I_m\cap I_n|)$ ways.

Case 3.2.2. $r \in I_m \cap I_n$, $s \in I_n \setminus I_m$.

The pair (r, s) can be chosen in $(|I_m \cap I_n| - 1)(|I_n| - |I_m \cap I_n|)$ ways.

Case 3.2.3. $r \in I_m \setminus I_n$, $s \in I_n \cap I_m$.

The pair (r, s) can be chosen in $(|I_m| - |I_m \cap I_n|)(|I_m \cap I_n| - 1)$ ways.

Case 3.2.4. $r, s \in I_m \cap I_n$.

The pair (r, s) can be chosen in $(|I_m \cap I_n| - 1)(|I_m \cap I_n| - 2)$.

Overall, in Case **3** the number of subdigraphs we have is

$$(q-1)\left\{\frac{\overline{m-n}}{|I_{m-n}\cap I_n|}|I_m\cap I_n|+q-1-|I_{m-n}|\right\}\Big[(|I_m|-|I_m\cap I_n|)(|I_n|-1)+(|I_m\cap I_n|-1)(|I_n|-2)\Big]. \tag{3.15}$$

C. *There are exactly two distinct first coordinates among* x_1, y_1, z_1 *and* w_1.

Let us assume that $x_1 = z_1$ and $y_1 = w_1$. Since $x_1 = z_1$ and $y_1 = w_1$, we must ensure that $x_2 \neq z_2$ and $y_2 \neq w_2$. By relations (3.11),

$$\begin{aligned} x_2 = z_2 &\Leftrightarrow x_1^m w_1^n - w_2 = x_1^m z_1^n - x_1^m w_1^n + w_2 \\ &\Leftrightarrow w_2 = x_1^m y_1^n - \frac{1}{2} x_1^m x_1^n. \end{aligned}$$

Similarly,

$$\begin{aligned} y_2 = w_2 &\Leftrightarrow -x_1^m z_1^n + x_1^m w_1^n + y_1^m z_1^n - w_2 = w_2 \\ &\Leftrightarrow w_2 = \frac{1}{2}(-x_1^m x_1^n + x_1^m y_1^n + y_1^m x_1^n). \end{aligned}$$

We now find conditions under which these values are equal. After simple algebra we conclude that

$$x_1^m y_1^n - \frac{1}{2} x_1^m x_1^n = \frac{1}{2}(-x_1^m x_1^n + x_1^m y_1^n + y_1^m x_1^n)$$

if and only if

$$x_1^m y_1^n = y_1^m x_1^n. \tag{3.16}$$

Case 1. $x_1^m = y_1^m$, $x_1^n \neq y_1^n$.

In this case condition (3.16) is not satisfied, and there are two forbidden values for w_2.

Since $x_1 \neq y_1$, we have $x_1 \neq 0$, $y_1 \neq 0$. As $(x_1 y_1^{-1})^m = 1$ and $(x_1 y_1^{-1})^n \neq 1$, we have that $x_1 y_1^{-1} \in I_m$ and $x_1 y_1^{-1} \notin I_n$. Thus, $x_1 y_1^{-1} \in I_m \setminus I_n$. Recall that by Proposition 3.2.5, $I_m = \overline{m}$. We have $|I_m \setminus I_n| = |I_m| - |I_m \cap I_n|$ choices for $x_1 y_1^{-1}$. We can choose y_1 in $(q-1)$ ways and $x_1 y_1^{-1}$ in $|I_m \setminus I_n|$ ways; x_1 is then determined uniquely.

We have therefore

$$\frac{1}{2!}\Big(|I_m| - |I_m \cap I_n|\Big)(q-1)(q-2) \tag{3.17}$$

corresponding subdigraphs. Note that division by 2! corresponds to a choice of x_1 and y_1 as an unordered pair.

Case 2. $x_1^m \neq y_1^m$, $x_1^n = y_1^n$.

This case is symmetric to the previous and we therefore have

$$\frac{1}{2!}\Big(|I_n| - |I_m \cap I_n|\Big)(q-1)(q-2) \tag{3.18}$$

corresponding subdigraphs.

Case 3. $x_1^m = y_1^m$, $x_1^n = y_1^n$.

We have that $x_1 y_1^{-1} \in I_m$ and $x_1 y_1^{-1} \in I_n$ and so $x_1 y_1^{-1} \in I_m \cap I_n$. Note that $1 \in I_m \cap I_n$ but if $x_1 y_1^{-1} = 1$, then $x_1 = y_1$. Thus $x_1 y_1^{-1}$ can be chosen in $|I_m \cap I_n| - 1$ ways, y_1 in $q-1$ ways; x_1 is then determined uniquely. Note that in this case condition (3.16) is always satisfied meaning that there is only one forbidden value for w_2.

We have therefore

$$\frac{1}{2!}\Big(|I_m \cap I_n| - 1\Big)(q-1)(q-1) \tag{3.19}$$

corresponding subdigraphs.

Summing the expressions in (3.17), (3.18) and (3.19) we obtain the total number of subgraphs of this type:

$$\frac{1}{2!}(q-1)\Big\{(q-2)\Big[|I_m| + |I_n| - |I_m \cap I_n| - 1\Big] + |I_m \cap I_n| - 1\Big\}. \tag{3.20}$$

Summing the expressions in (3.12), (3.13), (3.14), (3.15) and (3.20), we obtain, after simplification, formula (3.8). □

3.6 Reduction to the Bipartite Case

In Section 1.3 we mentioned undirected bipartite graphs $B\Gamma_n$ which were introduced in [21]. In case when there is only one incidence function which can be represented by a monomial $x^m y^n$ we denote this graph by $B\Gamma(q; m, n)$. In [10] an isomorphism criterion for $B\Gamma(q; m, n)$ was proven: two graphs $B\Gamma(q; m_1, n_1)$ and $B\Gamma(q; m_2, n_2)$ are isomorphic if and only $\{\overline{m}_1, \overline{n}_1\} = \{\overline{m}_2, \overline{n}_2\}$ as multisets.

Our goal is to prove the following theorem. Together with the aforementioned result it will give us necessary conditions on the pairs (m, n), (m', n') for which monomial digraphs are isomorphic.

Theorem 3.6.1. *If $D(q; m, n) \cong D(q; m', n')$, then $B\Gamma(q; m, n) \cong B\Gamma(q; m', n')$.*

We use the following construction to obtain a bipartite undirected graph $B\Gamma$ from a digraph D. For $V = V(D)$ we consider two copies, namely, V_1 and V_2, such that $x \in V$ corresponds to $x_1 \in V_1$ and $x_2 \in V_2$. Consider a bipartite undirected graph $B\Gamma$ with V_1 and V_2 being its vertex partitions and the edges defined as follows: For every arc $(u, v) \in A(D)$, we create an edge $\{u_1, v_2\} \in E(B\Gamma)$ and no other edges in $B\Gamma$ are created. Note that this construction is 'well-defined' in the sense that the information about the direction of arcs is retained, and there is a natural bijection between $A(D)$ and $E(B\Gamma)$.

We now prove Theorem 3.6.1.

Proof. Let ϕ be an isomorphism from $D = D(q; m, n)$ to $D' = D'(q; m', n')$ mapping vertex v to vertex v'. Let $B\Gamma = B\Gamma(q; m, n)$ and $B\Gamma' = B\Gamma'(q; m', n')$. Let $V = V(D)$, $V' = V(D')$, and let $V(B\Gamma) = V_1 \cup V_2$ and $V(B\Gamma') = V_1' \cup V_2'$ be the corresponding partitions of the vertex sets. Let $\{u_1, v_2\} \in E(B\Gamma)$ so that $(u, v) \in A(D)$. Let $(u', v') = (\phi(u), \phi(v)) \in A(D')$, and so $\{u_1', v_2'\} \in E(B\Gamma')$. Let $\psi \colon V(B\Gamma) \to V(B\Gamma')$ map a_1 to a_1' and b_2 to b_2' for every $a_1 \in V_1$ and every $b_2 \in V_2$. Trivially ψ is an isomorphism from $B\Gamma$ to $B\Gamma'$. □

3.7 Partial Proof of Conjecture 3.7.1 for $p > 2$

In Section 3.1 we proved the sufficiency of Conjecture 3.7.1. Although we believe that the converse of Theorem 3.1.1 is true, we are only able to prove it under some restrictions.

Suppose we are given two monomial digraphs $D_1 = D(p; m_1, n_1)$ and $D_2 = D(p; m_2, n_2)$ which are isomorphic. An isomorpism ϕ from D_1 to D_2 can be written in a general form

$$\phi\colon (x, y) \mapsto (f(x, y), g(x, y)), \tag{3.21}$$

where $f, g\colon \mathbb{F}_q^2 \to \mathbb{F}_q$. It is well-known (see for example Lidl, Niederreiter [22]) that any such function can be expressed as a polynomial, so $f, g \in \mathbb{F}_p[x, y]$. In each of these polynomials the degree of both x and y is at most $p - 1$.

The central idea of the proof we present below is to show that both f and g are monomials in x and y, respectively. Unfortunately, we were unable to prove this in a general setting (when both f and g are polynomials in x and y), and so we will additionally assume that there exists an isomorphism ϕ from D_1 to D_2 in which f depends on x only. No additional restrictions on g are imposed.

Theorem 3.7.1. *Let $q = p > 2$ be prime and $1 \leq m_1, n_1, m_2, n_2 \leq p - 1$ be integers. Suppose that $D_1 = D(p; m_1, n_1) \cong D_2 = D(p; m_2, n_2)$. Assume moreover that there exists an isomorphism $\phi\colon V(D_1) \to V(D_2)$ of the form (3.21) in which f depends on x only. If $m_1 \neq n_1$ or $m_2 \neq n_2$, then there exists an integer k, coprime with $p - 1$, such that*

$$m_1 \equiv km_2 \mod (p - 1),$$

$$n_1 \equiv kn_2 \mod (p - 1).$$

Proof. Without loss of generality assume that $m_1 \neq n_1$.

To retain some generality we will present our arguments for the case when f depends on both x and y and use the restriction that f depends on x only when needed.

The isomorphism ϕ is defined by $f \in \mathbb{F}_p[x,y]$ and $g \in \mathbb{F}_p[x,y]$ such that the equations

$$x_2 + y_2 = x_1^{m_1} y_1^{n_1}, \tag{3.22}$$

$$g(x_1,x_2) + g(y_1,y_2) = f(x_1,x_2)^{m_2} \cdot f(y_1,y_2)^{n_2} \tag{3.23}$$

are equivalent. We stop to note the following:

Proposition 3.7.2. *If f and g are defined as in (3.21), then for every $(a,b) \in \mathbb{F}_p^2$ there are precisely p pairs $(x,y) \in \mathbb{F}_p^2$ such that $f(x,y) = a$, $g(x,y) = b$. In other words, both f and g take on each of their values at exactly p distinct points.*

Proof. As $\phi(x,y)$ is a bijection on $\mathbb{F}_p^2$, the system

$$\begin{cases} f(x,y) &= a, \\ g(x,y) &= b, \end{cases}$$

must have a solution for every pair $(a,b) \in \mathbb{F}_p^2$. Fix a certain a and let b vary through all of $\mathbb{F}_p$. That way we can find p distinct solutions (x_i,y_i), $i = 0,\ldots,p-1$. Note that for every i we have $f(x_i,y_i) = a$, so that these are p distinct points at which f takes on some arbitrary value a. Assume that for some (x^*,y^*) different from each of the (x_i,y_i)'s we have $f(x^*,y^*) = a$. As $g(x_i,y_i)$ runs through all of $\mathbb{F}_p$, we must have $g(x^*,y^*) = g(x_i,y_i)$ for some i. Fix this i and consider

$$\phi(x^*,y^*) = \Big(f(x^*,y^*), g(x^*,y^*)\Big) = \Big(f(x_i,y_i), g(x_i,y_i)\Big) = \phi(x_i,y_i),$$

contradicting to the choice of (x^*,y^*). □

From (3.22) it follows that $y_2 = x_1^{m_1} y_1^{n_1} - x_2$. Substituting this into (3.23) we get

$$g(x_1,x_2) + g(y_1, x_1^{m_1} y_1^{n_1} - x_2) = f(x_1,x_2)^{m_2} \cdot f(y_1, x_1^{m_1} y_1^{n_1} - x_2)^{n_2}. \tag{3.24}$$

This latter equation must be satisfied for all arbitrary x_1, x_2 and y_1. Now let $(x_1, x_2) = (a, b)$, where (a, b) is some point for which $f(a, b) = 0$, and take $y_1 = t$. Then (3.24) yields

$$g(a, b) + g(t, a^{m_1} t^{n_1} - b) = 0, \quad \forall t \in \mathbb{F}_p. \tag{3.25}$$

On the other hand, from (3.22) $x_2 = x_1^{m_1} y_1^{n_1} - y_2$. Similarly, taking $x_1 = t$, $(y_1, y_2) = (a, b)$ in (3.24) we get

$$g(a, b) + g(t, t^{m_1} a^{n_1} - b) = 0, \quad \forall t \in \mathbb{F}_q. \tag{3.26}$$

Hence, (3.25) and (3.26) yield

$$g(t, a^{m_1} t^{n_1} - b) = g(t, a^{n_1} t^{m_1} - b) = -g(a, b), \quad \forall t \in \mathbb{F}_p.$$

By Proposition 3.7.2, we conclude that letting t run through all of $\mathbb{F}_p$, the set

$$\{(t, a^{m_1} t^{n_1} - b), (t, a^{n_1} t^{m_1} - b)\}$$

has only p elements. Hence, $a^{m_1} t^{n_1} - b = a^{n_1} t^{m_1} - b$ for all $t \in \mathbb{F}_p$. Since $m_1 \neq n_1$, this implies $a = 0$. We use this observation to state the following:

Proposition 3.7.3. *If ϕ is an isomorphism between $D(p; m_1, n_1)$ and $D(p; m_2, n_2)$ defined as in (3.21), then $f(a, b) = 0$ if and only if $a = 0$. Thus, $f(x, y) = x f_1(x, y)$ for some $f_1 \in \mathbb{F}_p[x, y]$ with $\deg_x f_1 \leq p - 2$.*

Proof. We already showed that $f(a, b) = 0$ implies $a = 0$. Also, we know that f takes its value 0 at p points. Hence, b must run through all of $\mathbb{F}_p$. □

Proposition 3.7.4. *$g(t, -b) = -g(0, b)$ for all t and all b in $\mathbb{F}_p$.*

Proposition 3.7.5. *$g(x, y) = y g_1(x, y)$.*

Proof. Write $g(x, y) = y g_1(x, y) + \hat{g}(x)$. By Proposition 3.7.4, taking $y = 0$, we obtain $g(x, 0) = \hat{g}(x) = -g(0, 0)$ for every x. Assuming that the degree of $\hat{g}(x)$ is at most $p - 1$, we conclude that $\hat{g}(x)$ is a constant polynomial. Also, taking both x and y to be 0, by the above claim we get that $g(0, 0) = 0$. The result follows. □

Proposition 3.7.6. *$g_1(t,-b) = g_1(0,b)$ for every t and every $b \neq 0$.*

Proof. Substitute $g(x,y) = yg_1(x,y)$ in the expression for $g(t,-b)$ in Proposition 3.7.4:

$$g(t,-b) = -bg_1(t,-b), \quad -g(0,b) = -bg_1(0,b).$$

It follows that $b[g_1(t,-b)-g_1(0,b)] = 0$. If $b \neq 0$, the claimed result follows immediately. □

Proposition 3.7.7. *$g(x,y) = a_0y + a_2y^3 + \cdots + a_{p-3}y^{p-2}$.*

Proof. Write $g_1(x,y) = xh_1(x,y) + h_2(y)$ for some polynomials h_1 and h_2. Now for all t and all $b \neq 0$ we have

$$g_1(t,-b) = th_1(t,-b) + h_2(-b) = g_1(0,b) = h_2(b).$$

Fixing $t = 0$ and varying $b \in \mathbb{F}_q^*$ we conclude that $h_2(b) = h_2(-b)$ for all $b \neq 0$. Since $deg(h_2) \leq p-2$, it follows that $h_2(y) = \sum_{i=0}^{(p-3)/2} a_{2i}y^{2i}$ for some constants a_i. In other words, $h_2(y)$ may only contain those terms with even powers of y.

On the other hand we know that for every t and every $b \neq 0$, $th_1(t,-b) = 0$. Assume from now on that $t \neq 0$. Then, $h_1(t,-b) = 0$ for all $t, b \neq 0$. Write $h_1(x,y)$ as

$$h_1 = h_1(x,y) = c_{p-2}(y)x^{p-2} + c_{p-3}(y)x^{p-3} + \cdots + c_1(y)x + c_0(y),$$

where these $c_i(y)$ are polynomials of y of degree at most $p-2$. Substituting $x \in \mathbb{F}_q^*$ we obtain a linear system

$$\begin{pmatrix} 1^{p-2} & 1^{p-3} & \cdots & 1^1 & 1^0 \\ 2^{p-2} & 2^{p-3} & \cdots & 2^1 & 2^0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ (p-1)^{p-2} & (p-1)^{p-3} & \cdots & (p-1)^1 & (p-1)^0 \end{pmatrix} \cdot \begin{pmatrix} c_{p-2}(y) \\ c_{p-2}(y) \\ \vdots \\ c_0(y) \end{pmatrix} = 0.$$

This is a Vandermonde type system and none of the entries are 0. So it follows that $c_i(y) = 0$ for any i. Also, since $deg(c_i) \leq p-2$ (which eliminates the possibility that $c_i(y) = y^{p-1} - 1$), $c_i(y) = 0$ for any i and any y. Thus, $h_1(x,y) = 0$ for all $(x,y) \in \mathbb{F}_q^2$. □

From the proof it follows that

$$g(x,y) = a_0 y + a_2 y^3 + \cdots + a_{p-3} y^{p-2},$$

where the coefficients a_i's were defined by $h_2(y)$ above.

We now have that for all x_1, y_1, x_2,

$$g(x_2) + g(-x_2 + x_1^{m_1} y_1^{n_1}) = x_1^{m_2} y_1^{n_2} f_1(x_1, x_2)^{m_2} f_1(y_1, -x_2 + x_1^{m_1} y_1^{n_1})^{n_2}.$$

Using the fact that f, and therefore f_1, depends on x only, we rewrite the last equation as

$$g(x_2) + g(-x_2 + x_1^{m_1} y_1^{n_1}) = x_1^{m_2} y_1^{n_2} f_1(x_1)^{m_2} f_1(y_1,)^{n_2}.$$

Set $x_2 = x$, $x_1 = y_1 = 1$. Then

$$g(x) + g(1-x) = C, \quad \forall x,$$

where $C \in \mathbb{F}_p$ is a constant. For any r, $1 \leq r \leq p-2$, the coefficient of x^k, for any integer k, in $(1-x)^r$ is $(-1)^k \binom{r}{k}$. By $[x^k]$ we denote the coefficient of x^k in the expansion of $g(x) + g(1-x)$. We equate all $[x^k]$ to 0 for $k > 0$ even:

$$[x^2] = a_2 \binom{3}{2} + \cdots + a_{p-3} \binom{p-2}{2} = 0,$$

$$[x^4] = a_4 \binom{5}{4} + \cdots + a_{p-3} \binom{p-2}{4} = 0,$$

$$\cdots$$

$$[x^{p-5}] = a_{p-5} \binom{p-4}{p-5} + a_{p-3} \binom{p-2}{p-5} = 0,$$

$$[x^{p-3}] = a_{p-3} \binom{p-2}{p-3} = 0.$$

It follows that $a_2 = a_4 = \cdots = a_{p-5} = a_{p-3} = 0$, and so $g(y) = a_0 y$ for some $a_0 \neq 0$. Therefore

$$g(x_2) + g(-x_2 + x_1^m y_1^{n_1}) = a_0 x_1^{m_1} y_1^{n_1}.$$

Hence,

$$0 \neq a_0 = x^{m_2 - m_1} y^{n_2 - n_1} f_1(x)^{m_2} f_1(y)^{n_2}, \quad \forall x \neq 0, \forall y \neq 0. \tag{3.27}$$

It follows from (3.27) that for any $x \in \mathbb{F}_p^*$,

$$x^{m_2-m_1} f_1(x)^{m_2} = c \neq 0 \quad \text{and} \quad x^{n_2-n_1} f_1(x)^{n_2} = c_2 \neq 0. \tag{3.28}$$

If $m_1 = m_2$ and $n_1 = n_2$, then the proof is complete, and so we may assume, without loss of generality, that $m_1 \neq m_2$. Set

$$d = \begin{cases} m_2 - m_1 & \text{if } m_2 > m_1, \\ p - 1 - (m_1 - m_2) & \text{if } m_2 < m_1. \end{cases}$$

Then $d > 0$, and by (3.28), $x^d f_1(x)^{m_2} = c \neq 0$ for all $x \neq 0$. It can now be easily seen that, as a polynomial, $x^d f_1(x)^{m_2}$ induces the same function on $\mathbb{F}_p$ as cx^{p-1}. Consequently, we have the polynomial identity $x^d f_1(x)^{m_2} \equiv cx^{p-1} \bmod (x^p - x)$. Note that if the reduction of $f_1(x)^{m_2}$ by modulo $x^p - x$ has at least two terms, then so will the reduction of $x^d f_1(x)^{m_2}$. Hence, the reduction of $f_1(x)^{m_2}$ is a monomial which implies that f_1 has a zero constant term. The proof that f_1 is a monomial can now be done by induction on its degree.

Let $f_1(x) = b_0 x^l$ for some integer l, $1 \leq l \leq p-2$ and $b_0 \in \mathbb{F}_p^*$. It follows from (3.27) that

$$x^{m_2-m_1+lm_2} = K_1,$$

$$x^{n_2-n_1+ln_2} = K_2$$

for some constants $K_1, K_2 \in \mathbb{F}_p^*$, and any $x \in \mathbb{F}_p^*$. From this we conclude that

$$\begin{cases} m_2 - m_1 + lm_2 \equiv 0 \mod (p-1), \\ n_2 - n_1 + ln_2 \equiv 0 \mod (p-1). \end{cases}$$

Taking $k = l + 1$ we note that $f(x) = b_0 x^k$, and so we have $\overline{k} = 1$. The proof is now complete. □

Chapter 4

CONCLUSIONS

The question of connectivity of $D(q;\mathbf{f})$ is now settled for prime powers q in case when $\mathbf{g}=\mathbf{h}$, where, for all $x\in\mathbb{F}_q$, $\mathbf{g}(x)=\mathbf{f}(x,0)-\mathbf{f}(0,0)$ and $\mathbf{h}(x)=\mathbf{f}(0,x)-\mathbf{f}(0,0)$. By Lemma 2.1.1, in this case we only need to study strong connectivity of $D(q;\mathbf{f}^*)$, where, for all $x,y\in\mathbb{F}_q$, $\mathbf{f}^*(x,y)=\mathbf{f}(x,y)-\mathbf{g}(x)-\mathbf{h}(y)-\mathbf{f}(0,0)$. Theorem 2.1.3, which heavily uses the fact that $\mathbf{f}^*(x,0)=\mathbf{f}^*(0,x)\,(=\mathbf{0})$ for any $x\in\mathbb{F}_q$, gives a complete description of strong components of $D(q;\mathbf{f}^*)$ and the number of them. The case $\mathbf{g}\neq\mathbf{h}$ was only solved (see Theorem 2.1.5) for $q=p$ prime. In the general case of $\mathbf{g}\neq\mathbf{h}$ and q primer power, one cannot argue that $D(q;\mathbf{f})\cong D(q;\mathbf{f}^*)$. We believe that the question of strong connectivity of this case is related to the properties of functions $\mathbf{g}$ and $\mathbf{h}$. In the general case, however, we prove that if $\mathbf{f}$ has linked alternating sums of even lengths that span $\mathbb{F}_q^l$, then $D(q;\mathbf{f})$ is strong (Theorem 2.1.6).

Some bounds on the diameter of monomial digraphs $D(q;m,n)$ were obtained in Section 2.6. All of them follow from small absolute bounds on the Waring's number $\gamma(k,p)$, given in Theorem 2.5.2. It would be interesting to further investigate what other results on diameter of $D(q;m,n)$ one can get using methods of additive combinatorics.

In Chapter 3, we addressed the question of classifying monomial digraphs $D(q;m,n)$ into isomorphism classes. Our main idea was to find a suitable set of digraph invariants as functions on the parameters q, m and n. Unfortunately no such set of invariants was found, but further investigation in this direction may be continued. Our computational experiments prompted Conjecture 3.7.1, which we prove under certain restriction in Section 3.7. One such restriction was the assumption that if an isomorphism $\phi\colon V(D(p;m_1,n_1))\to V(D(p;m_2,n_2))$ maps a vertex (x,y) to a vertex $(f(x,y),g(x,y))$, where $f,g\in\mathbb{F}_p[x,y]$, then, in fact, f depends on x only. It would be

interesting to see if this restriction can be lifted. It would be interesting as well to see if the technical condition that $m_1 \neq n_1$ or $m_2 \neq n_2$, used in the proof of the conjecture, can be avoided.

BIBLIOGRAPHY

[1] J. Bang-Jensen, G. Gutin, *Digraphs: Theory, Algorithms and Applications*, Springer 2009.

[2] B.C. Berndt, R.J. Evans, K.S. Williams, *Gauss and Jacobi sums*, Willey 1998.

[3] J.A. Bondy, M. Simonovits, Cycles of even length in graphs, *J. Combin. Theory Ser. B*, 16 (1974), 97–105.

[4] J. Bourgain, M.-C. Chang, A Gauss sum estimate in arbitrary finite fields, *C. R. Math. Acad. Sci. Paris*, Ser. I 342 (2006), 643–646.

[5] J. Bourgain, A. Glibichuk, and S. Konyagin, Estimates for the number of sums and products and for exponential sums in fields of prime order, *J. London Math. Soc.* 73 (2006), 380–398.

[6] B. Bukh, Z. Jiang, A bound on the number of edges in graphs without an even cycle, arXiv:1403.1601.

[7] J. Cipra, Waring's number in finite fields, Doctoral Thesis, Kansas State University, 2010.

[8] J. Cipra, T. Cochrane, C. Pinner, Heilbronn's conjecture on Waring's number (mod p), *J. Number Theory* 125 (2007), 289–297.

[9] T. Cochrane, C. Pinner, Sum-product estimates applied to Waring's problem mod p, *Integers* 8 (2008), A46.

[10] V. Dmytrenko, F. Lazebnik, R. Viglione, An isomorphism criterion for monomial graphs, *J. Graph Theory* 48 (2005), 322–328.

[11] M.M. Dodson, On Waring's problem in GF[p], *Acta Arith.* 19 (1971), 147–173.

[12] D. Dummit, R. Foote, *Abstract Algebra*, 3rd ed., John Wiley & Sons, Inc., 2004.

[13] A. Ghoulia-Houri, Diametre maximal d'un graphe fortement connexe, *C. R. Math. Acad. Sci. Paris*, 250:254–256, 1960.

[14] M.K. Goldberg, The diameter of a strongly connected graph, *Dokl. Akad. Nauk SSSR*, 170:767–769, 1966.

[15] R. Hartshorne, *Algebraic Geometry*, Springer, 1977.

[16] L.K. Hua, H.S. Vandiver, Characters over certain types of rings with applications to the theory of equations in a finite field, *Proc. Natl. Acad. Sci. U.S.A.* 35 (1949), 94–99.

[17] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag New York Inc., 1990.

[18] F. Lazebnik, D. Mubayi, New lower bounds for Ramsey numbers of graphs and hypergraphs, *Adv. in Appl. Math.* Vol. 28, No. 3/4, (2002), 544–559.

[19] F. Lazebnik, V.A. Ustimenko, Explicit construction of graphs with an arbitrary large girth and of large size, *Discrete Appl. Math.* 60 (1995), 275–284.

[20] F. Lazebnik, V.A. Ustimenko, A.J. Woldar, A new series of dense graphs of high girth, *Bull. Amer. Math. Soc.* 32 (1) (1995), 73–79.

[21] F. Lazebnik, A.J. Woldar, General properties of some families of graphs defined by systems of equations, *J. Graph Theory* 38 (2) (2001), 65–86.

[22] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 2, Cambridge University Press, 1997.

[23] O. Pikhurko, A note on the Turán function of even cycles, *Proc. Amer. Math. Soc.*, 140(11):3687–3692, 2012.

[24] J.G. Semple, L. Roth, *Introduction to algebraic geometry*, Oxford, 1949.

[25] C. Small, Waring's number mod n, *Amer. Math. Monthly* 84 (1)(1977), 12–25.

[26] J. Verstraëte, On arithmetic progressions of cycle lengths in graphs, *Combin. Probab. Comput.*, 9(4):369–373, 2000.

[27] R. Viglione, Properties of some algebraically defined graphs, Doctoral Thesis, University of Delaware, 2002.

[28] A. Weil, Number of solutions of equations in finite fields, *Bull. Amer. Math. Soc.* 55 (1949), 497–508.

[29] S. De Winter, *private communication*, 2014.

Appendix

SOME SAGE AND MAGMA CODE

Here we present some basic programs used in `sage` and `Magma` to build and explore the algebraically defined digraphs presented in the thesis. The following program is the basic code for constructing the digraphs. It is self-explanatory. This particular program constructs the digraph $D(25;\mathbf{f})$, where $\mathbf{f} = (f_1, f_2)\colon \mathbb{F}_{25}^2 \to \mathbb{F}_{25}^2$, and $f_1(x,y) = xy^2$, $f_2(x,y) = x^3y^4$.

```
#*********************************************************
#This is the basic code to build the algebraically defined
#digraph over a finite field with incidence functions f2,...,fn.
#*********************************************************

#Field characteristic
p = 5
e = 2
#Field order
q = p^e
#Construct finite field of order 25 wtih primitive element xi
F.<xi> = GF(q)
#Assign parameters for functions f_i(x,y) = x^m * y^n
m1 = 1
n1 = 2
m2 = 3
n2 = 4
#Construct the vertex set
V = [(x,y,z) for x in F for y in F for z in F]
#Construct the digraph
D = DiGraph([V, lambda x,y: x[1] + y[1] == (x[0])^m1 * (y[0])^n1 and\
                            x[2] + y[2] == (x[0])^m2 * (y[0])^n2\
           ])
```

Computer system sage has a variety of tools to work with both undirected and directed graphs. The following command returns the number of strong component of a digraph D :

```
#*********************************************************
#Number of strong components of a digraph D
#*********************************************************

len(D.strongly_connected_components())
```

The following command returns the component containing some vertex (x, y, z) of D.

```
#*********************************************************
#Return component containing vertex (x,y,z) of D
#*********************************************************

D.strongly_connected_component_containing_vertex((x,y,z))
```

The following command returns the diameter of a digraph D.

```
#*********************************************************
#Return diameter of D
#*********************************************************

D.diameter()
```

The following code constructs a digraph $D(121; f)$, where f is a random polynomial in $\mathbb{F}_{121}[x, y]$ of degree at most 5 having 7 terms.

```
#*********************************************************
#Construct a digraph $D(121;f)$, where f is a random
#polynomial in \F_{121}[x,y].
#*********************************************************

p = 11
e = 2
q = p^e
#Construct finite field of order 121 wtih primitive element xi
F.<xi> = GF(q)
#Construct vertex set
V = [(x,y) for x in F for y in F]
#Construct bivariate polynomial ring with indeterminants x and y
```

```
R.<x,y> = PolynomialRing(F)
#Construct random polynomial of degree at most 5 with 7 terms requested
f = R.random_element(degree = 5, terms = 7)
#Construct D(121;f)
D = DiGraph([V, lambda x,y: x[1] + y[1] == f(x[0],y[0]) ])
```

We also show how to construct monomial digraphs in Magma. The following code constructs digraphs $D(149; 9, 11)$ and $D(149; 67, 73)$ and tests them for isomorphism.

```
//*********************************************************
//Construct digraphs D(149;9,11) and D(149;67,73)
//and test them for isomorphism
//*********************************************************

q := 149;
//Finite field
F := FiniteField(q);
//Vertex set
V := {[x,y] : x,y in F};
//one graph
m1 := 9;
n1 := 11;
D1 := Digraph< V | { [x,y] : x,y in V | x[2] + y[2] \
                  eq ((x[1])^m1)*((y[1])^n1) } : SparseRep := true>;
//another graph
m2 := 67;
n2 := 73;
D2 := Digraph< V | { [x,y] : x,y in V | x[2] + y[2] \
                  eq ((x[1])^m2)*((y[1])^n2) } : SparseRep := true>;

IsIsomorphic(D1,D2);
```