A note on the Isomorphism Problem for 
Monomial Digraphs

Aleksandr Kodess  
Department of Mathematics  
University of Rhode Island  
kodess@uri.edu

Felix Lazebnik  
Department of Mathematical Sciences  
University of Delaware  
fellaz@udel.edu

October 2, 2016

Abstract

Let $p$ be a prime $e$ be a positive integer, $q = p^e$, and let $\mathbb{F}_q$ denote the finite field of $q$ elements. Let $m, n$, $1 \leq m, n \leq q - 1$, be integers. The monomial digraph $D = D(q; m, n)$ is defined as follows: the vertex set of $D$ is $\mathbb{F}_q^2$, and $((x_1, x_2), (y_1, y_2))$ is an arc in $D$ if $x_2 + y_2 = x_1^m y_1^n$. In this note we study the question of isomorphism of monomial digraphs $D(q; m_1, n_1)$ and $D(q; m_2, n_2)$. In particular, we find some necessary conditions for it, and some sufficient conditions. We conjecture that one simple sufficient condition is also a necessary one.

1 Introduction

For all terms related to digraphs which are not defined below, see Bang-Jensen and Gutin [1]. In this paper, by a directed graph (or simply digraph) $D$ we mean a pair $(V, A)$, where $V = V(D)$ is the set of vertices and $A = A(D) \subseteq V \times V$ is the set of arcs. For an arc $(u, v)$, the first vertex $u$ is called its tail and the second vertex $v$ is called its head; we also denote such an arc by $u \rightarrow v$. If $(u, v)$ is an arc, we call $v$ an out-neighbor of $u$, and $u$ an in-neighbor of $v$. The number of out-neighbors of $u$ is called the out-degree of $u$, and the number of in-neighbors of $u$ — the in-degree of $u$. For an integer $k \geq 2$, 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 $x_i \in V$ and arcs $a_j \in A$ such that the tail of $a_i$ is $x_i$ and the head of $a_i$ is $x_{i+1}$ for every $i$, $1 \leq i \leq k - 1$. Whenever the labels of the arcs of a walk are not important, we use the notation $x_1 \rightarrow x_2 \rightarrow \cdots \rightarrow x_k$ for the walk, and say
that we have an $x_1x_k$-walk. In a digraph $D$, a vertex $y$ is reachable from a vertex $x$ if there exists a walk from $x$ to $y$ in $D$. 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 $y$. A strong component of a digraph $D$ is a maximal induced subdigraph of $D$ that is strong. If $x$ and $y$ are vertices of a digraph $D$, then the distance from $x$ to $y$ in $D$, denoted $\text{dist}(x, y)$, is the minimum length of an $xy$-walk, if $y$ is reachable from $x$, and otherwise $\text{dist}(x, y) = \infty$. The distance from a set $X$ to a set $Y$ of vertices in $D$ is

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

The diameter of $D$ is defined as $\text{dist}(V, V)$, and it is denoted by $\text{diam}(D)$.

Let $p$ be a prime, $e$ a positive integer, and $q = p^e$. Let $\mathbb{F}_q$ denote the finite field of $q$ elements, and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.

Let $\mathbb{F}_q^2$ denote the Cartesian product $\mathbb{F}_q \times \mathbb{F}_q$, and let $f : \mathbb{F}_q^2 \to \mathbb{F}_q$ be an arbitrary function. We define a digraph $D = D(q; f)$ as follows: $V(D) = \mathbb{F}_q^2$, and there is an arc from a vertex $x = (x_1, x_2)$ to a vertex $y = (y_1, y_2)$ if and only if $x_2 + y_2 = f(x_1, y_1)$.

If $(x, y)$ is an arc in $D$, then $y$ is uniquely determined by $x$ and $y_1$, and $x$ is uniquely determined by $y$ and $x_1$. Hence, each vertex of $D$ has both its in-degree and out-degree equal to $q$.

By Lagrange’s interpolation, $f$ can be uniquely represented by a bivariate polynomial of degree at most $q - 1$ in each of the variables. If $f(x, y) = x^m y^n$, where $m, n$ are integers, $1 \leq m, n \leq q - 1$, we call $D$ a monomial digraph, and denote it by $D(q; m, n)$. Digraph $D(3; 1, 2)$ is depicted in Fig. 1. As for every $a \in \mathbb{F}_q, a^{q^2} = a$, we will also allow ourselves to use the notation $D(q; m, n)$ for $m, n \geq q$. It is clear, that $x \to y$ in $D(q; m, n)$ if and only if $y \to x$ in $D(q; n, m)$. Hence, one digraph is obtained from the other by reversing the direction of every arc. In general, these digraphs are not isomorphic, but if one of them is strong then so is the other and their diameters are equal. Also, if one of them contains a path or cycle, then the other contains a cycle or path of the same length.

The digraphs $D(q; f)$ and $D(q; m, n)$ are directed analogues of some algebraically defined graphs, which have been studied extensively and have many applications: see Lazebnik and Woldar [3], and a recent survey by Lazebnik and Sun [7].

The study of digraphs $D(q; f)$ started with the questions of connectivity and diameter. The questions of strong connectivity of digraphs $D(q; f)$ and $D(q; m, n)$ and descriptions of their components were completely answered by Kodess and Lazebnik [5]. The problem of determining the diameter of a component of $D(q; f)$ for an arbitrary prime power $q$ and an arbitrary $f$ turned out to be rather difficult. A number of results concerning some instances of this problem for strong monomial digraphs were obtained by Kodess, Lazebnik, Smith, and Sporre [6].
Figure 1: The digraph $D(3; 1, 2)$: $x_2 + y_2 = x_1 y_1^2$.

As the order of $D(q; m, n)$ is $q^2$, it is clear that digraphs $D_1 = D(q_1; m_1, n_1)$ and $D_2 = D(q_2; m_2, n_2)$ are isomorphic (denoted as $D_1 \cong D_2$) only if $q_1 = q_2$. Hence, the isomorphism problem for monomial graphs can be stated as follows: find necessary and sufficient conditions on $q, m_1, n_1, m_2, n_2$ such that $D_1 \cong D_2$.

Though we are still unable to solve the problem, all our partial results support the following conjecture.

**Conjecture 1.1.** [Kodess [4]] Let $q$ be a prime power, and let $m_1, n_1, m_2, n_2$ be integers from $\{1, 2, \ldots, q-1\}$. Then $D(q; m_1, n_1) \cong D(q; m_2, n_2)$ if and only if there exists an integer $k$, coprime with $q-1$, such that

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

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

The sufficiency part of the conjecture is easy to demonstrate, and we do it in Section 3 (Theorem 3.1). We verified the necessity of these conditions with a computer for all prime powers $q$, $2 \leq q \leq 97$. In the case $m_1 = m_2 = 1$, the conditions imply $n_1 = n_2$, and we checked that for all odd prime powers $q$, $3 \leq q \leq 509$.

Our interest in the isomorphism problem for monomial digraphs $D(q; m, n)$ and Conjecture 1.1 is two-fold. First, since the isomorphism question for various mathematical objects is a fundamental one. Secondly, due to the existence of a simple isomorphism criterion for similarly constructed bipartite graphs $G(q; m, n)$ (see Theorem 1.1 below) defined as follows. Each partition of the vertex set of $G(q; m, n)$, which are denoted by $P$ and $L$, is a copy of $\mathbb{F}_q^2$, and two vertices $(p_1, p_2) \in P$ and $(l_1, l_2) \in L$ are adjacent if and only if $p_2 + l_2 = p_1 l_1^m$.

From now on, let $q$ always denote a prime power, and let $m, n$ in the notation $D(q; m, n)$ denote integers from $\{1, 2, \ldots, q-1\}$ or positive integers congruent to $m$ and $n$ modulo $q-1$. For any integer $a$, we let $\bar{a}$ denote the greatest common divisor of $a$ and $q-1$. 

3
Theorem 1.1. [Dmytrenko, Lazebnik and Viglione] $G(q; m_1, n_1) \cong G(q; m_2, n_2)$ if and only if $\{m_1, n_1\} = \{m_2, n_2\}$ as multisets.

For every digraph $D(q; f)$, one can define a bipartite graph $G(q; f)$ in the following way. Each partition $X$ and $Y$ of the vertex set of $G(q; f)$ is defined to be a copy of $V(D(q; f))$, and a vertex $x = (x_1, x_2) \in X$ is joined to a vertex $y = (y_1, y_2) \in Y$ in $G(q; f)$ if and only if $x \to y$ in $D(q; f)$. This construction is of special interest to us in view of the following proposition that provides us with the first non-trivial necessary condition for isomorphism of monomial digraphs.

Proposition 1.1. If $D(q; m_1, n_1) \cong D(q; m_2, n_2)$, then $G(q; m_1, n_1) \cong G(q; m_2, n_2)$ and $\{m_1, n_1\} = \{m_2, n_2\}$ as multisets.

The first part of the statement of Proposition 1.1 can be easily verified (see, e.g., Kodess [4]), and the second part follows from Theorem 1.1. In contrast to the case of the monomial bipartite graphs, this necessary condition of Proposition 1.1 is far from being sufficient for the isomorphism of monomial digraphs.

In the following section we discuss some general properties of the isomorphisms of monomial digraphs. In Section 3 we prove the sufficiency of Conjecture 1.1 and present several necessary conditions on the parameters of isomorphic monomial digraphs. In Section 4 we finish the note with some concluding remarks.

2 Some general properties of isomorphisms of monomial digraphs

Suppose digraphs $D_1 = D(q; m_1, n_1)$ and $D_2 = D(q; m_2, n_2)$ are isomorphic via an isomorphism $\phi: V(D_1) \to V(D_2)$, $(x, y) \mapsto \phi((x, y)) = (\phi_1((x, y)), \phi_2((x, y)))$. Functions $\phi_1$ and $\phi_2$ can be considered as functions of two variables on $\mathbb{F}_q$, and so they can be represented by polynomial functions of two variables. Let $f, g \in \mathbb{F}_q[X, Y]$ be such that the degree of $f$ and the degree of $g$ with respect to each indeterminant is at most $q - 1$, and $\phi((x, y)) = (f(x, y), g(x, y))$.

A polynomial $h \in \mathbb{F}_q[X_1, \ldots, X_n]$ is called a permutation polynomial in $n$ variables on $\mathbb{F}_q$ if the equation $h(x_1, \ldots, x_n) = \alpha$ has exactly $q^{n-1}$ solutions in $\mathbb{F}_q^n$ for each $\alpha \in \mathbb{F}_q$. For $n = 1$, it means that the function on $\mathbb{F}_q$ induced by $h$ is a bijection, and $h$ is this case is called just a permutation polynomial on $\mathbb{F}_q$.

The following theorem describes some properties of the functions induced by the polynomials $f$ and $g$, and imposes a strong restriction on the form of $g$.

Theorem 2.1. Let $q$ be an odd prime power, $D_1 = D(q; m_1, n_1) \cong D_2 = D(q; m_2, n_2)$ with an isomorphism given in the form

$$\phi: V(D_1) \to V(D_2), \quad (x, y) \mapsto (f(x, y), g(x, y))$$

for some $f, g \in \mathbb{F}_q[X, Y]$ of degree at most $q - 1$ in each of the variables. Then the following statements hold.

(i) $f$ and $g$ are permutation polynomials in two variables on $\mathbb{F}_q$. 

4
(ii) If $m_1 \neq n_1$, then $f(x, y) = 0$ if and only if $x = 0$.

(iii) If $m_1 \neq n_1$, then $g$ is a polynomial of indeterminant $Y$ only, and is of the form

$$g(Y) = a_{q-2}Y^{q-2} + a_{q-4}Y^{q-4} + \cdots + a_1Y,$$

where all $a_i \in \mathbb{F}_q$, $i = 1, \ldots, q-2$. Moreover, $g$ is a permutation polynomial on $\mathbb{F}_q$.

Proof. As $\phi$ is a bijection, the system

\[
\begin{align*}
  f(x, y) &= a, \\
  g(x, y) &= b,
\end{align*}
\]

does not have a solution for every pair $(a, b) \in \mathbb{F}_q^2$. Fix an $a$ and let $b$ vary through all of $\mathbb{F}_q$. This gives $q$ distinct solutions $(x_i, y_i)$, $i = 0, \ldots, q-1$, of the system. Note that for every $i$, we have $f(x_i, y_i) = a$, so these are $q$ distinct points at which $f$ takes on the value $a$. Assume that for some $(x^*, y^*)$ distinct from each $(x_i, y_i)$ we have $f(x^*, y^*) = a$. As $g(x_i, y_i)$ runs through all of $\mathbb{F}_q$, we have $g(x^*, y^*) = g(x_i, y_i)$ for some $i$. Then, for this $i$, we have

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

contradicting to the choice of $(x^*, y^*)$. Hence, the equation $f(x, y) = \alpha$ has exactly $q$ solutions for each $\alpha \in \mathbb{F}_q$, and so $f$ is a permutation polynomial in two variables on $\mathbb{F}_q$. The proof of the statement for $g$ is similar. This proves part (i).

Since $\phi$ is an isomorphism, the following two equations

\[
x_2 + y_2 = x_1^{m_1}y_1^{n_1}, \quad (1)
\]

\[
g(x_1, x_2) + g(y_1, y_2) = f(x_1, x_2)^{m_2} \cdot f(y_1, y_2)^{n_2} \quad (2)
\]

are equivalent.

From (1), $y_2 = x_1^{m_1}y_1^{n_1} - x_2$, and substituting this expression for $y_2$ in (2) we have

\[
g(x_1, x_2) + g(y_1, x_1^{m_1}y_1^{n_1} - x_2) = f(x_1, x_2)^{m_2} \cdot f(y_1, x_1^{m_1}y_1^{n_1} - x_2)^{n_2}, \quad (3)
\]

for all $x_1, x_2, y_1 \in \mathbb{F}_q$. Let $(a, b) \in \mathbb{F}_q^2$ be such that $f(a, b) = 0$ (its existence follows from part (i)). Set $(x_1, x_2) = (a, b)$, and set $y_1 = s$. Then (3) yields

\[
g(a, b) + g(s, a^{m_1}s^{n_1} - b) = 0, \quad \text{for all } s \in \mathbb{F}_q. \quad (4)
\]

Likewise from (1), $x_2 = x_1^{m_1}y_1^{n_1} - y_2$. Substituting this expression for $x_2$ in (2), and setting $x_1 = t$ and $(y_1, y_2) = (a, b)$, we obtain

\[
g(t, t^{m_1}a^{n_1} - b) + g(a, b) = 0, \quad \text{for all } t \in \mathbb{F}_q. \quad (5)
\]

5
Hence, (4) and (5) yield
\[ g(s, a^{m_1}s^{n_1} - b) = g(t, a^{n_1}t^{m_1} - b) = -g(a, b), \quad \text{for all } s, t \in \mathbb{F}_q. \]
From part (i), \( g \) is a permutation polynomial in two variables, and we conclude that the set
\[ \{(s, a^{m_1}s^{n_1} - b), (t, a^{n_1}t^{m_1} - b) : s, t \in \mathbb{F}_q \} \]
contains exactly \( q \) elements. As \( (s, a^{m_1}s^{n_1} - b) = (t, a^{n_1}t^{m_1} - b) \) implies \( s = t \), we obtain that \( a^{m_1}t^{n_1} - b = a^{n_1}t^{m_1} - b \) for all \( t \in \mathbb{F}_q \). Since \( m_1 \neq n_1 \), this implies \( a = 0 \) as, otherwise the polynomial \( X^{m_1-n_1} - a^{m_1-n_1} \in \mathbb{F}_q[X] \) of degree \( |m_1-n_1| \leq q-2 \) has \( q \) roots.
Thus, \( f(a, b) = 0 \) implies \( a = 0 \). From part (i), \( f \) is a permutation polynomial in two variables. Let \( \{(a_i, b_i)\}_{i=1}^g \) be the set of \( q \) distinct points at which \( f \) is zero. Then \( a_i = 0 \) for all \( i \), and all \( b_i \) must be distinct. That is, \( f(0, b) = 0 \) for any \( b \in \mathbb{F}_q \). This proves part (ii).

We now turn to the proof of part (iii). We just concluded that \( f(a, b) = 0 \) implies \( a = 0 \). Substituting \( a = 0 \) in (5) we obtain
\[ g(t, -b) = -g(0, b), \quad \text{for all } b, t \in \mathbb{F}_q. \]
Write \( g(X, Y) = Yg_1(X, Y) + \hat{g}(X) \) for some \( g_1 \in \mathbb{F}_q[X, Y] \), and \( \hat{g} \in \mathbb{F}_q[X] \) of degree at most \( q-1 \). Now from (6), we have \( g(x, 0) = \hat{g}(x) = -g(0, 0) \) for every \( x \in \mathbb{F}_q \). Since the degree of \( \hat{g} \) is at most \( q-1 \), it follows that \( \hat{g} \) is a constant polynomial. Also from (6), \( g(0, 0) = \hat{g}(0) = -g(0, 0) \), and, as \( q \) is odd, \( \hat{g} \) is the zero polynomial. Thus \( g(X, Y) = Yg_1(X, Y) \) for some \( g_1 \in \mathbb{F}_q[X, Y] \), where the degree of \( g_1 \) in \( Y \) is at most \( q-2 \).

Using (6) again, we find that
\[ g_1(t, -b) = g_1(0, b), \quad \text{for all } b \in \mathbb{F}_q^*, t \in \mathbb{F}_q. \]
Write \( g_1(X, Y) = Xh_1(X, Y) + h_2(Y) \), where \( h_1 \in \mathbb{F}_q[X, Y], h_2 \in \mathbb{F}_q[Y] \). By (7), for all \( t \in \mathbb{F}_q \) and all \( b \in \mathbb{F}_q^* \) we have
\[ g_1(t, -b) = th_1(t, -b) + h_2(-b) = g_1(0, b) = h_2(b). \]
For \( t = 0 \), it implies that \( h_2(b) = h_2(-b) \) for all \( b \in \mathbb{F}_q^* \), and since \( q \) is odd, and the degree of \( h_2 \) is at most \( q-2 \), we have \( h_2(Y) = \sum_{i=0}^{(q-3)/2} \tilde{a}_i Y^{2i} \) for some \( \tilde{a}_i \in \mathbb{F}_q \), \( 0 \leq i \leq (q-3)/2 \). From (8), it now follows that for every \( t \in \mathbb{F}_q \) and every \( b \in \mathbb{F}_q^* \), \( th_1(t, -b) = 0 \), and so \( h_1(t, -b) = 0 \) for all \( b, t \in \mathbb{F}_q^* \). Write \( h_1(X, Y) \) as
\[ h_1(X, Y) = c_{q-2}(Y)X^{q-2} + c_{q-3}(Y)X^{q-3} + \cdots + c_1(Y)X + c_0(Y), \]
where all \( c_i \in \mathbb{F}_q[Y] \) are of degree at most \( q-2 \). For any fixed \( b \in \mathbb{F}_q^* \), the polynomial \( h_1(-b, Y) \) of degree at most \( q-2 \) has \( q-1 \) roots. Hence, \( c_i(-b) = 0 \).
for all $i$, $0 \leq i \leq q-2$, and so all $c_i(Y)$ are zero polynomials. Thus, $h_1(X, Y)$ is zero polynomial. Therefore,

$$g(X, Y) = Yg_1(X, Y) = Y(Xh_1(X, Y) + h_2(Y)) = Yh_2(Y) = \sum_{i=0}^{(q-3)/2} \tilde{a}_{2i}Y^{2i+1}.$$ 

Set $a_{i+1} = \tilde{a}_{2i}$ for all $i$, $0 \leq i \leq (q-3)/2$, so

$$g(Y) = a_{q-2}Y^{q-2} + a_{q-4}Y^{q-4} + \cdots + a_1Y.$$ 

(9)

Every permutation polynomial in two variables, which is actually a polynomial of one variable, has to be a permutation polynomial. By part (i), and by the last expression for $g$ as $g(Y)$, we obtain that $g$ is a permutation polynomial. This ends the proof of part (iii), and of the theorem.

\[\square\]

3 Conditions on the parameters of isomorphic monomial digraphs

We begin with the proof of the sufficiency part of Conjecture 1.1.

**Theorem 3.1.** Suppose there exists an integer $k$ such that $\overline{k} = 1$ and

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

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

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

**Proof.** Define the mapping $\phi: V(D(q; m_2, n_2)) \to V(D(q; m_1, n_1))$ via the rule

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

As $\overline{k} = 1$, $\phi$ is bijective and we check that $\phi$ preserves adjacency and non-adjacency. Let $(x_1, x_2) \rightarrow (y_1, y_2)$ in $D(q; m_2, n_2)$. Then $x_2 + y_2 = x_1^{m_2}y_1^{n_2}$. We have

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

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

and

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

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 $D(q; m_1, n_1)$, and $\phi$ is indeed an isomorphism from $D(q; m_2, n_2)$ to $D(q; m_1, n_1)$.

\[\square\]

**Corollary 3.1.** The following statements hold.

(i) If $\overline{m} = 1$, then $D(q; m, n) \cong D(q; 1, n')$, for some integer $n'$ such that $mn' \equiv n \mod (q-1)$. 

7
(ii) If \( mn \equiv 1 \mod (q - 1) \), then \( D(q; m, 1) \cong D(q; 1, n) \), and \( D(q; m, n) \cong D(q; 1, n^2) \cong D(q; m^2, 1) \).

(iii) If \( m + n \equiv 0 \mod (q - 1) \), then \( D(q; m, n) \cong D(q; n, m) \).

(iv) If \( D(q; m_1, n_1) \cong D(q; m_2, n_2) \) and \( m_1 = n_1 \), then \( m_2 = n_2 \), and \( \overline{m_1} = \overline{m_2} \).

(v) If \( \overline{m} = \overline{n} \), then \( D(q; m, m) \cong D(q; n, n) \).

Proof. Part (i) is straightforward. As \( \overline{m} = 1 \), there exists an integer \( k \) such that \( k \equiv 1 \mod (q - 1) \), and \( m' \equiv km \mod (q - 1) \). By Theorem 3.1, \( D(q; m, n) \cong D(q; 1, n') \).

For part (ii), \( mn \equiv 1 \mod (q - 1) \) is equivalent to \( \overline{m} = \overline{n} = 1 \), and the conclusion follows directly from Theorem 3.1 by taking \( k = \) equal mod or \( n \).

For part (iii), we need to show that \( D(q; m, -m) \cong D(q; -m, m) \). As \( -1 = 1 \), the statement follows from Theorem 3.1.

Let us prove part (iv). If \( m_1 = n_1 \), then for every arc of \( D_1 \), the opposite arc is also an arc of \( D_1 \). As \( D_1 \cong D_2 \), for every arc of \( D_2 \), the opposite arc is also an arc of \( D_2 \). Consider an arc of \( D_2 \) of the form \( (a, b) \rightarrow (1, a^{m_2} - b) \). Then \( D_2 \) contains the opposite arc \( (1, a^{m_2} - b) \rightarrow (a, b) \) only if \( a^{m_2} = a^{m_2} \). Taking \( a \) to be a primitive element of \( \mathbb{F}_q \), we obtain \( m_2 = n_2 \). Then the equality \( \overline{m_1} = \overline{m_2} \) follows from Proposition 1.1.

For part (v), let \( m_1 = n_1 = m \) and \( m_2 = n_2 = n \). The following lemma appeared in Viglione [9] (the proof can also be found in [3]).

**Lemma 3.1.** Let \( m, n, \) and \( l \) be integers with gcd\((m, l) = \) gcd\((n, l) \). Then there exists an integer \( k \), coprime with \( l \), such that \( mk \equiv n \mod l \).

Setting \( l = q - 1 \) in the statement of the lemma, and using \( \overline{m} = \overline{n} \), we obtain that the conditions of Theorem 3.1 are met. Hence, \( D(q; m, m) \cong D(q; n, n) \).

The following statement provides some information on the automorphism groups of monomial digraphs. The proof is trivial, and we omit it.

**Proposition 3.1.** For any \( c \in \mathbb{F}_q^* \), the mapping \( \psi_c: (x, y) \mapsto (cx, cm+n y) \) 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 \( \psi_g \), where \( \langle g \rangle = \mathbb{F}_q^* \).

It is well known that \( \mathbb{F}_q^* \), viewed as a multiplicative group, is a cyclic group of order \( q - 1 \). For any integer \( n \), let

\[
A_n = \{ x^n : x \in \mathbb{F}_q^* \}, \quad I_n = \{ x \in \mathbb{F}_q^* : x^n = 1 \}.
\]

By standard theory of cyclic groups, \( |A_n| = (q - 1)/\pi \), and \( |I_n| = \pi \). For any integers \( a \) and \( b \), let \( (a, b) \) denote their greatest common divisor. We recall the following basic fact: if the order \( o(x) \) of an element \( x \) of a finite group \( G \) is \( n \), then \( o(x^m) = n/(m, n) \). We also use the following two statements: the number of elements \( y \) in \( \mathbb{F}_q^* \) for which the system of equations \( x^m = y, x^n = y \) in \( x \) has
a solution is $m - n / (m - n, n)$, and for any such $y$, the number of solutions is $(m, n)$.

In the following theorem we collect some independent necessary conditions on the parameters of isomorphic monomial digraphs.

**Theorem 3.2.** Let $D_1 = D(q; m_1, n_1)$, $D_2 = D(q; m_2, n_2)$ and $D_1 \cong D_2$, where $q$ is an odd prime power. Then

(i) $\overline{m_1} = \overline{m_2}$ and $\overline{n_1} = \overline{n_2}$.

(ii) $m_1 + n_1 = m_2 + n_2$.

(iii) $m_1 - n_1 = m_2 - n_2$.

Moreover, the conditions (i) – (iii) are independent in the sense that no two of them imply the remaining one.

**Proof.** For (i), by Proposition 1.1, we have $\{m_1, n_1\} = \{m_2, n_2\}$ as multisets. Therefore, in order to prove both equalities in (i), it is sufficient to prove only one of them. We will show that $\overline{m_1} = \overline{m_2}$.

Let $\phi : D_1 \to D_2$ be an isomorphism. It follows from Theorem 2.1 that $\phi((0, 0)) = (0, 0)$. As $(1, 0)$ is an out-neighbor of $(0, 0)$ in $D_1$, $\phi((1, 0))$ is an out-neighbor of $(0, 0)$ in $D_2$, distinct from $(0, 0)$. The adjacency equation in $D_2$ implies that $\phi((1, 0)) = (c, 0)$, for some $c \in F_q^*$. By Proposition 3.1, composing $\phi$ with $\psi_c^{-1}$, we obtain an isomorphism $\phi_1 : D_1 \to D_2$, such that $(0, 0) \mapsto (0, 0)$ and $(1, 0) \mapsto (1, 0)$. Let $f$ and $g$ be the polynomials described in Theorem 2.1 so that $\phi_1((a, b)) = (f(a, b), g(b))$ for every $(a, b) \in V(D_1)$.

The out-neighbors of the vertex $(1, 0)$ distinct from $(0, 0)$ in $D_1$ and in $D_2$ have the form $(x, x^{n_1})$ and $(x, x^{n_2})$, respectively, for every $x \in F_q^*$. As $\phi_1$ maps $(0, 0)$ to $(0, 0)$ and $(1, 0)$ to $(1, 0)$, we obtain that for every $x \in F_q^*$ there exists a unique $y \in F_q^*$ such that $\phi_1(f(x, x^{n_1})) = (y, y^{n_2})$. As $g$ is a permutation polynomial on $F_q$, and $g(0) = 0$, we obtain that $g(A_{n_1}) = A_{n_2}$, and so $|A_{n_1}| = |A_{n_2}|$. As $|A_{n_1}| = (q - 1)/\overline{m_1}$, $i = 1, 2$, we obtain $\overline{m_1} = \overline{m_2}$. This ends the proof of (i).

For (ii), we count the number of distinct nonzero second coordinates of the vertices of $D = D(q; m, n)$ which have a loop on them. As $q$ is odd, there exists a loop on a vertex $(x, y)$ of $D$ if and only if

$$(x, y) \mapsto (x, y) \iff 2y = x^{m+n} \iff y = \frac{1}{2}x^{m+n} \iff (x, y) = (x, \frac{1}{2}x^{m+n}).$$

Therefore, the number of distinct nonzero second coordinates of the vertices of $D$ which have a loop on them is

$$|A_{m+n}| = \frac{q - 1}{m + n}.$$

Now, if $\phi : D_1 \to D_2$ is an isomorphism, then $\phi$ maps the set of loops of $D_1$ to the set of loops of $D_2$ bijectively. As $\phi((0, 0)) = (0, 0)$, and both $D_1$ and $D_2$
Thus there are \( |A_{m_1+n_1}| = |A_{m_2+n_2}| \). Hence, \( m_1 + m_1 = m_2 + n_2 \), and part (ii) is now proved.

For (iii), we compute the number of 2-cycles in \( D = D(q; m, n) \), which we denote by \( c_2 = c_2(q; m, n) \). If \( (x_1, x_2) \rightarrow (y_1, y_2) \rightarrow (x_1, x_2) \) is a 2-cycle in \( D \), then

\[
x_2 + y_2 = x_1^m y_1^n = x_1^n y_1^m, \quad (x_1, x_2) \neq (y_1, y_2).
\]

To compute \( c_2 \), we count the number of solutions \((x_1, x_2, y_1, y_2) \in \mathbb{F}_q^4 \) of this system.

There are \( q(q-1) \) solutions if \( x_1 = 0 \) and \( y_1 \neq 0 \), and the same number if \( x_1 \neq 0 \) and \( y_1 = 0 \). If \( x_1 = y_1 = 0 \), then \( x_2 = -y_2 \) can be chosen in \( q-1 \) ways.

Thus there are

\[
q(q-1) + q(q-1) + (q-1) = 2q(q-1) + (q-1) = (2q + 1)(q-1)
\]

solutions with \( x_1 y_1 = 0 \).

If \( x_1 y_1 \neq 0 \), then \( x_1 y_1 = 1 \). If \( x_1 = y_1 \), then choose \( x_2 \) such that \( x_2 \neq \frac{1}{2} x_1^{m+n} \) in \( q-1 \) ways, so the value of \( y_2 \) is determined uniquely and is different from \( x_2 \). This case yields \( (q-1)^2 \) solutions. If \( x_1 \neq y_1 \), \( x_1 \) can be chosen in \( q-1 \) ways, and \( y_1 \) in \( |I_{m-n}| - 1 = m-n - 1 \) ways, and \( x_2 \) in \( q \) ways.

Hence, in total there are

\[
(2q + 1)(q-1) + q(q-1)(m-n-1) = q(q-1)(2 + m-n)
\]

solutions to (10). As vertices \((x_1, x_2) \) and \((y_1, y_2) \) can we swapped in this count, the number of 2-cycles is half of this:

\[
c_2(q; m, n) = \frac{1}{2} q(q-1)(2 + m-n).
\]

If \( D_1 \) and \( D_2 \) are isomorphic, they have the same number of 2-cycles, and \( c_2(q; m_1, n_1) = c_2(q; m_2, n_2) \) yields \( m_1 - n_1 = m_2 - n_2 \), ending the proof of part (iii).

We now show that conditions (i), (ii), and (iii) are independent. Let \( q = 11 \). Then \((m_1, n_1) = (1, 1) \) and \((m_2, n_2) = (1, 3) \) satisfy (i) and (ii), but not (iii); \((m_1, n_1) = (1, 2) \) and \((m_2, n_2) = (1, 4) \) satisfy (i) and (iii), but not (ii); \((m_1, n_1) = (1, 2) \) and \((m_2, n_2) = (1, 10) \) satisfy (ii) and (iii), but not (i).

**Remark 1.** The conditions of Theorem 3.2 do not imply those of Conjecture 1.1. For instance, let \( m_1 = n_2 = 1, n_1 = 4, n_2 = 12 \) with \( q = 17 \). It is known that the digraphs \( D(17; 1, 4) \) and \( D(17; 1, 12) \) are not isomorphic, however \( m_1 = m_2 = 1, n_1 = n_2 = 4, m_1 + n_1 = m_2 + n_2 = 1 \), and \( m_1 - n_1 = m_2 - n_2 = 1 \).

10
4 Concluding remarks

Let \( N(D, H) \) denote the number of isomorphic copies of digraph \( H \) in digraph \( D \). One can attempt to solve the isomorphism problem by finding a “test digraph” \( H \) such that \( N(D_1, H) = N(D_2, H) \) if and only if \( D_1 \cong D_2 \). Similarly, one can try to resolve the problem by finding a “test family” of digraphs \( \mathcal{H} \) satisfying \( N(D_1, H) = N(D_2, H) \) for all \( H \in \mathcal{H} \) if only if \( D_1 \cong D_2 \). This approach was successful in the case of the aforementioned undirected class of graphs \( G(q; m, n) \) \([9, 3]\). It is worth noting that \( K_{2,2} \) (same as 4-cycle) was a good “test graph” in that case: for fixed \( m, n \) and sufficiently large \( q \), the equality of numbers of 4-cycles in \( G(q; m_1, n_1) \) and \( G(q; m_2, n_2) \) implied the isomorphism of the graphs. In order to obtain the result for all \( q \), the number of copies of other \( K_{s,t} \)-subgraphs had to be counted. This approach however fails for monomial digraphs \( D(q; m, n) \) when the “test digraphs” are strong directed cycles: for every odd prime power \( q \), the digraphs \( D_1 = D(q; 2\frac{q-1}{2}, q-1) \) and \( D_2 = D(q; q-1, 2\frac{q-1}{2}) \) are not isomorphic by Theorem 3.2 but have equal number of strong directed cycles of any lengths, since every arc \( x \to y \) in \( D_1 \) corresponds to the arc \( y \to x \) in \( D_2 \). It can also be shown that conditions of Theorem 3.2 imply that \( D(q; m_1, n_1) \) and \( D(q; m_2, n_2) \) have equal number of copies isomorphic to \( K_{2,2} \) with all arcs directed from one partition to the other, and so this digraph cannot be a “test digraph” either.

So far we were unable to find a good “test family” to replicate the success with monomial bipartite graphs for monomial digraphs. One difficulty is that counting \( N(D, H) \) in monomial digraphs is much harder, even for small digraphs \( H \). Another difficulty was with finding good candidates for \( H \), even after utilizing all necessary conditions and extensive experiments with computer.

On the other hand, understanding the equality of \( N(D_1, K) = N(D_2, K) \) in monomial digraphs \( D_1 \) and \( D_2 \) for digraph \( K \) of Fig. 2 (see above), led to a “digraph-theoretic proof” that the numbers of solutions of certain polynomial equations over finite fields were equal, and the latter was not clear to us at first from just algebraic considerations (see Coulter, De Winter, Kodess, and Lazebnik [2]).

Acknowledgments

This work was partially supported by a grant from the Simons Foundation (#426092, Felix Lazebnik).

References


Figure 2: The digraph $K$.  


