Connectivity of some algebraically defined digraphs

Aleksandr Kodess
Department of Mathematics
University of Rhode Island
Rhode Island, U.S.A.
kodess@uri.edu

Felix Lazebnik*
Department of Mathematical Sciences
University of Delaware
Delaware, U.S.A.
fellaz@udel.edu

Submitted: Feb 20, 2015; Accepted: Aug 16, 2015; Published: Aug 28, 2015
Mathematics Subject Classifications: 05.60, 11T99

Dedicated to the memory of Vasyl Dmytrenko (1961-2013)

Abstract

Let p be a prime, e a positive integer, $q = p^e$, and let $\mathbb{F}_q$ denote the finite field of q elements. Let $f_i \colon \mathbb{F}_q^2 \to \mathbb{F}_q$ be arbitrary functions, where $1 \leqslant i \leqslant l$, i and l are integers. The digraph $D = D(q; \mathbf{f})$, where $\mathbf{f} = (f_1, \dots, f_l) \colon \mathbb{F}_q^2 \to \mathbb{F}_q^l$, is defined as follows. The vertex set of D is $\mathbb{F}_q^{l+1}$. There is an arc from a vertex $\mathbf{x} = (x_1, \dots, x_{l+1})$ to a vertex $\mathbf{y} = (y_1, \dots, y_{l+1})$ if $x_i + y_i = f_{i-1}(x_1, y_1)$ for all i, $2 \leqslant i \leqslant l+1$. In this paper we study the strong connectivity of D and completely describe its strong components. The digraphs D are directed analogues of some algebraically defined graphs, which have been studied extensively and have many applications.

Keywords: Finite fields; Directed graphs; Strong connectivity

1 Introduction and Results

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. The *order* of D is the number of its vertices. For an arc (u, v), the first vertex u is called its *tail* and the second vertex v is called its *head*; we denote such an arc by $u \to v$. For an integer $k \geqslant 2$, a *walk W from x_1 to x_k* in D is an alternating sequence $W = x_1 a_1 x_2 a_2 x_3 \dots x_{k-1} a_{k-1} x_k$ 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, $1 \leqslant i \leqslant k-1$. Whenever the labels of the arcs of a walk are not important, we use the notation $x_1 \to x_2 \to \cdots \to x_k$ for the walk. 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

*Partially supported by NSF grant DMS-1106938-002

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. For all digraph terms not defined in this paper, see Bang-Jensen and Gutin [1].

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 $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. We write $\mathbb{F}_q^n$ to denote the Cartesian product of n copies of $\mathbb{F}_q$. Let $f_i \colon \mathbb{F}_q^2 \to \mathbb{F}_q$ be arbitrary functions, where $1 \leqslant i \leqslant l$, 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. (Throughout all of the paper the bold font is used to distinguish elements of $\mathbb{F}_q^j$, $j \geqslant 2$, from those of $\mathbb{F}_q$, and we simplify the notation $\mathbf{f}((x,y))$ and $f((x,y))$ to $\mathbf{f}(x,y)$ and $f(x,y)$, respectively.) 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 and only if

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

We call the functions f_i, $1 \leqslant i \leqslant l$, the *defining functions* of $D(q; \mathbf{f})$.

If $l = 1$ and $\mathbf{f}(x,y) = f_1(x,y) = x^m y^n$, $1 \leqslant m, n \leqslant q-1$, we call D a *monomial* digraph, and denote it by $D(q; m, n)$.

The digraphs $D(q; \mathbf{f})$ 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 [11] and references therein; for some subsequent work see Viglione [15], Lazebnik and Mubayi [7], Lazebnik and Viglione [10], Lazebnik and Verstraëte [9], Lazebnik and Thomason [8], Dmytrenko, Lazebnik and Viglione [3], Dmytrenko, Lazebnik and Williford [4], Ustimenko [14], Viglione [16], Terlep and Williford [13], Kronenthal [6], Cioabă, Lazebnik and Li [2], and Kodess [5].

We note that $\mathbb{F}_q$ and $\mathbb{F}_q^l$ can be viewed as vector spaces over $\mathbb{F}_p$ of dimensions e and el, respectively. For $X \subseteq \mathbb{F}_q^l$, by $\langle X \rangle$ we denote the span of X over $\mathbb{F}_p$, which is the set of all finite linear combinations of elements of X with coefficients from $\mathbb{F}_p$. For any vector subspace W of $\mathbb{F}_q^l$, $\dim(W)$ denotes the dimension of W over $\mathbb{F}_p$. If $X \subseteq \mathbb{F}_q^l$, let $\mathbf{v} + X = \{\mathbf{v} + \mathbf{x} \colon \mathbf{x} \in X\}$. Finally, let $\mathrm{Im}(\mathbf{f}) = \{(f_1(x,y), \ldots, f_l(x,y)) \colon (x,y) \in \mathbb{F}_q^2\}$ denote the image of function $\mathbf{f}$.

In this paper we study strong connectivity of $D(q; \mathbf{f})$. We mention that by Lagrange's interpolation (see, for example, Lidl, Niederreiter [12]), each f_i can be uniquely represented by a bivariate polynomial of degree at most $q-1$ in each of the variables. We therefore also call functions f_i *defining polynomials*.

In order to state our results, we need the following notation. For every $\mathbf{f} \colon \mathbb{F}_q^2 \to \mathbb{F}_q^l$, we define

$$\begin{aligned} \mathbf{g}(t) = \mathbf{f}(t,0) - \mathbf{f}(0,0), \quad \mathbf{h}(t) &= \mathbf{f}(0,t) - \mathbf{f}(0,0), \\ \tilde{\mathbf{f}}(x,y) &= \mathbf{f}(x,y) - \mathbf{g}(y) - \mathbf{h}(x), \\ \mathbf{f_0}(x,y) &= \mathbf{f}(x,y) - \mathbf{f}(0,0), \quad \text{and} \\ \tilde{\mathbf{f}}_\mathbf{0}(x,y) &= \mathbf{f_0}(x,y) - \mathbf{g}(y) - \mathbf{h}(x). \end{aligned}$$

As $\mathbf{g}(0) = \mathbf{h}(0) = \mathbf{0}$, one can view the coordinate function g_i of $\mathbf{g}$ (respectively, h_i of $\mathbf{h}$), $i = 1, \ldots, l$, as the sum of all terms of the polynomial f_i containing only indeterminate

x (respectively, y), and having zero constant term. We, however, wish to emphasise that in the definition of $\tilde{\mathbf{f}}(x, y)$, $\mathbf{g}$ is evaluated at y, and $\mathbf{h}$ at x. Also, we will often write a vector $(v_1, v_2, \ldots, v_{l+1}) \in \mathbb{F}_q^{l+1} = V(D)$ as an ordered pair $(v_1, \mathbf{v}) \in \mathbb{F}_q \times \mathbb{F}_q^l$, where $\mathbf{v} = (v_2, \ldots, v_{l+1})$.

The main result of this paper is the following theorem, which gives necessary and sufficient conditions for the strong connectivity of $D(q; \mathbf{f})$ and provides a description of its strong components in terms of $\langle \mathrm{Im}(\tilde{\mathbf{f}}_\mathbf{0}) \rangle$ over $\mathbb{F}_p$.

Theorem 1. *Let $D = D(q; \mathbf{f})$, $D_0 = D(q; \mathbf{f_0})$, $W_0 = \langle \mathrm{Im}(\tilde{\mathbf{f}}_\mathbf{0}) \rangle$ over $\mathbb{F}_p$, and $d = \dim(W_0)$ over $\mathbb{F}_p$. Then the following statements hold.*

(i) If q is odd, then the digraphs D and D_0 are isomorphic. Furthermore, the vertex set of the strong component of D_0 containing a vertex $(u, \mathbf{v})$ is

$$\Big\{(a, \mathbf{v} + \mathbf{h}(a) - \mathbf{g}(u) + W_0)\colon a \in \mathbb{F}_q\Big\} \cup \Big\{(b, -\mathbf{v} + \mathbf{h}(b) + \mathbf{g}(u) + W_0) : b \in \mathbb{F}_q\Big\}$$

$$= \Big\{(a, \pm\mathbf{v} + \mathbf{h}(a) \mp \mathbf{g}(u) + W_0)\Big\}. \tag{1}$$

The vertex set of the strong component of D containing a vertex $(u, \mathbf{v})$ is

$$\Big\{(a, \mathbf{v} + \mathbf{h}(a) - \mathbf{g}(u) + W_0)\colon a \in \mathbb{F}_q\Big\} \cup \Big\{(b, -\mathbf{v} + \mathbf{h}(b) + \mathbf{g}(u) + \mathbf{f}(0,0) + W_0) : b \in \mathbb{F}_q\Big\}. \tag{2}$$

In particular, $D \cong D_0$ is strong if and only if $W_0 = \mathbb{F}_q^l$ or, equivalently, $d = el$.

If q is even, then the strong component of D containing a vertex $(u, \mathbf{v})$ is

$$\Big\{(a, \mathbf{v} + \mathbf{h}(a) + \mathbf{g}(u) + W_0)\colon a \in \mathbb{F}_q\Big\} \cup \Big\{(a, \mathbf{v} + \mathbf{h}(a) + \mathbf{g}(u) + \mathbf{f}(0,0) + W_0)\colon a \in \mathbb{F}_q\Big\} \tag{3}$$

$$= \Big\{(a, \mathbf{v} + \mathbf{h}(a) + \mathbf{g}(u) + W)\colon a \in \mathbb{F}_q\Big\},$$

where $W = W_0 + \langle \{f(0,0)\} \rangle = \langle \mathrm{Im}(\tilde{\mathbf{f}}) \rangle$.

(ii) If q is odd, then $D \cong D_0$ has $(p^{el-d} + 1)/2$ strong components. One of them is of order p^{e+d}. All other $(p^{el-d} - 1)/2$ strong components are isomorphic, and each is of order $2p^{e+d}$.

If q is even, then the number of strong components in D is 2^{el-d}, provided $\mathbf{f}(0,0) \in W_0$, and it is 2^{el-d-1} otherwise. In each case, all strong components are isomorphic, and are of orders 2^{e+d} and 2^{e+d+1}, respectively.

We note here that for q even the digraphs D and D_0 are generally not isomorphic.

We apply this theorem to monomial digraphs $D(q; m, n)$. For these digraphs we can restate the connectivity results more explicitly.

Theorem 2. *Let $D = D(q; m, n)$ and let $d = (q-1, m, n)$ be the greatest common divisor of $q-1$, m and n. For each positive divisor e_i of e, let $q_i := (q-1)/(p^{e_i}-1)$, and let q_s be the largest of the q_i that divides d. Then the following statements hold.*

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

$$\{(x, v + \mathbb{F}_{p^{e_s}}) \colon\ x \in \mathbb{F}_q\} \cup \{(x, -v + \mathbb{F}_{p^{e_s}}) \colon\ x \in \mathbb{F}_q\}. \tag{4}$$

In particular, D is strong if and only if $q_s = 1$ or, equivalently, $e_s = e$.

(ii) If q is odd, then D has $(p^{e-e_s}+1)/2$ strong components. One of them is of order p^{e+e_s}. All other $(p^{e-e_s}-1)/2$ strong components are all isomorphic and each is of order $2p^{e+e_s}$.

If q is even, then D has 2^{e-e_s} strong components, all isomorphic, and each is of order 2^{e+e_s}.

Our proof of Theorem 1 is presented in Section 2, and the proof of Theorem 2 is in Section 3. In Section 4 we suggest two areas for further investigation.

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

Theorem 1 and our proof below were inspired by the ideas from [15], where the components of similarly defined bipartite simple graphs were described.

We now prove Theorem 1.

Proof. Let q be odd. We first show that $D \cong D_0$. The map $\phi \colon V(D) \to V(D_0)$ given by

$$(x, \mathbf{y}) \mapsto (x, \mathbf{y} - \frac{1}{2}\mathbf{f}(0,0)) \tag{5}$$

is clearly a bijection. We check that ϕ preserves adjacency. Assume that $((x_1, \mathbf{x}_2), (y_1, \mathbf{y}_2))$ is an arc in D, 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

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

and so $(\phi((x_1, \mathbf{x}_2)), \phi((y_1, \mathbf{y}_2)))$ is an arc in D_0. As the above steps are reversible, ϕ preserves non-adjacency as well. Thus, $D(q; \mathbf{f}) \cong D(q; \mathbf{f_0})$.

We now obtain the description (1) of the strong components of D_0, and then explain how the description (2) of the strong components of D follows from (1).

Note that as $\mathbf{f_0}(0,0) = \mathbf{0}$, we have $\mathbf{g}(t) = \mathbf{f_0}(t, 0)$, $\mathbf{h}(t) = \mathbf{f_0}(0, t)$, $\mathbf{g}(0) = \mathbf{h}(0) = \mathbf{0}$, and $\tilde{\mathbf{f}}_\mathbf{0}(x, y) = \mathbf{f_0}(x, y) - \mathbf{g}(y) - \mathbf{h}(x)$.

Let $\tilde{\alpha}_1, \dots, \tilde{\alpha}_d \in \mathrm{Im}(\tilde{\mathbf{f}}_\mathbf{0})$ be a basis for W_0. Now, choose $x_i, y_i \in \mathbb{F}_q$ be such that $\tilde{\mathbf{f}}_\mathbf{0}(x_i, y_i) = \tilde{\alpha}_i$, $1 \leqslant i \leqslant d$.

Let $(u, \mathbf{v})$ be a vertex of D_0. We first show that a vertex $(a, \mathbf{v} + \mathbf{y})$ is reachable from $(u, \mathbf{v})$ if $\mathbf{y} \in \mathbf{h}(a) - \mathbf{g}(u) + W_0$. In order to do this, we write an arbitrary $\mathbf{y} \in \mathbf{h}(a) - \mathbf{g}(u) + W_0$ as

$$\mathbf{y} = \mathbf{h}(a) - \mathbf{g}(u) + (a_1\tilde{\alpha}_1 + \cdots + a_d\tilde{\alpha}_d),$$

for some $a_1, \dots, a_d \in \mathbb{F}_p$, and consider the following directed walk in D_0:

$$\begin{aligned}
(u, \mathbf{v}) &\to (0, -\mathbf{v} + \mathbf{f}_\mathbf{0}(u, 0)) = (0, -\mathbf{v} + \mathbf{g}(u)) \\
&\to (0, \mathbf{v} - \mathbf{g}(u)) && (6) \\
&\to (x_1, -\mathbf{v} + \mathbf{g}(u) + \mathbf{f}_\mathbf{0}(0, x_1)) = (x_1, -\mathbf{v} + \mathbf{g}(u) + \mathbf{h}(x_1)) && (7) \\
&\to (y_1, \mathbf{v} - \mathbf{g}(u) - \mathbf{h}(x_1) + \mathbf{f}_\mathbf{0}(x_1, y_1)) && (8) \\
&\to (0, -\mathbf{v} + \mathbf{g}(u) + \mathbf{h}(x_1) - \mathbf{f}_\mathbf{0}(x_1, y_1) + \mathbf{g}(y_1)) && (9) \\
&= (0, -\mathbf{v} + \mathbf{g}(u) - \tilde{\mathbf{f}}_\mathbf{0}(x_1, y_1)) = (0, -\mathbf{v} + \mathbf{g}(u) - \tilde{\alpha}_1) && (10) \\
&\to (0, \mathbf{v} - \mathbf{g}(u) + \tilde{\alpha}_1)). && (11)
\end{aligned}$$

Traveling through vertices whose first coordinates are 0, x_1, y_1, 0, 0, and 0 again (steps 6–11) as many times as needed, one can reach vertex $(0, \mathbf{v} - \mathbf{g}(u) + a_1\tilde{\alpha}_1)$. Continuing a similar walk through vertices whose first coordinates are 0, x_i, y_i, 0, 0, and 0, $2 \leqslant i \leqslant d$, as many times as needed, one can reach vertex $(0, \mathbf{v} - \mathbf{g}(u) + (a_1\tilde{\alpha}_1 + \ldots + a_i\tilde{\alpha}_i))$, and so on, until the vertex $(0, -\mathbf{v} + \mathbf{g}(u) - (a_1\tilde{\alpha}_1 + \cdots + a_d\tilde{\alpha}_d))$ is reached. The vertex $(a, \mathbf{v} + \mathbf{y})$ will be its out-neighbor. Here we indicate just some of the vertices along this path:

$$\begin{aligned}
&\to \ldots \\
&\to (0, \mathbf{v} - \mathbf{g}(u) + a_1\tilde{\alpha}_1) \\
&\to (x_2, -\mathbf{v} + \mathbf{g}(u) - a_1\tilde{\alpha}_1 + \mathbf{h}(x_2)) \\
&\to (y_2, \mathbf{v} - \mathbf{g}(u) + a_1\tilde{\alpha}_1 - \mathbf{h}(x_2) + \mathbf{f}_\mathbf{0}(x_2, y_2)) \\
&\to (0, -\mathbf{v} + \mathbf{g}(u) - a_1\tilde{\alpha}_1 + \mathbf{h}(x_2) - \mathbf{f}_\mathbf{0}(x_2, y_2) + \mathbf{g}(y_2)) \\
&= (0, -\mathbf{v} + \mathbf{g}(u) - a_1\tilde{\alpha}_1 - \tilde{\alpha}_2) \\
&\to (0, \mathbf{v} - \mathbf{g}(u) + a_1\tilde{\alpha}_1 + \tilde{\alpha}_2) \\
&\to \ldots \\
&= (0, -\mathbf{v} + \mathbf{g}(u) - a_1\tilde{\alpha}_1 - a_2\tilde{\alpha}_2) \\
&\to \ldots \\
&= (0, -\mathbf{v} + \mathbf{g}(u) - (a_1\tilde{\alpha}_1 + \cdots + a_d\tilde{\alpha}_d)) \\
&\to (a, \mathbf{v} - \mathbf{g}(u) + \mathbf{h}(a) + (a_1\tilde{\alpha}_1 + \cdots + a_d\tilde{\alpha}_d)) \\
&= (a, \mathbf{v} + \mathbf{y}).
\end{aligned}$$

Hence, $(a, \mathbf{v} + \mathbf{y})$ is reachable from $(u, \mathbf{v})$ for any $a \in \mathbb{F}_q$ and any $\mathbf{y} \in \mathbf{h}(a) - \mathbf{g}(u) + W_0$, as claimed. A slight modification of this argument shows that $(a, -\mathbf{v} + \mathbf{y})$ is reachable from $(u, \mathbf{v})$ for any $\mathbf{y} \in \mathbf{h}(a) + \mathbf{g}(u) + W_0$.

Let us now explain that every vertex of D_0 reachable from $(u, \mathbf{v})$ is in the set

$$\{(a, \pm\mathbf{v} \mp \mathbf{g}(u) + \mathbf{h}(a) + W_0) \colon \ a \in \mathbb{F}_q\}.$$

We will need the following identities on $\mathbb{F}_q$ and $\mathbb{F}_q^2$, respectively, which can be checked easily using the definition of $\tilde{\mathbf{f}}$:

$$\begin{aligned} &\tilde{\mathbf{f}}_{\mathbf{0}}(t,0) = \mathbf{g}(t) - \mathbf{h}(t) = -\tilde{\mathbf{f}}_{\mathbf{0}}(0,t) \ \text{ and} \\ &\mathbf{f}_{\mathbf{0}}(x,y) = \mathbf{g}(x) + \mathbf{h}(y) + \tilde{\mathbf{f}}_{\mathbf{0}}(x,y) - \tilde{\mathbf{f}}_{\mathbf{0}}(0,y) + \tilde{\mathbf{f}}_{\mathbf{0}}(0,x). \end{aligned}$$

The identities immediately imply that for every $t, x, y \in \mathbb{F}_q$,

$$\begin{aligned} &\mathbf{g}(t) - \mathbf{h}(t) \in W_0 \ \text{ and} \\ &\mathbf{f}_{\mathbf{0}}(x,y) = \mathbf{g}(x) + \mathbf{h}(y) + w \ \text{ for some } \ w = w(x,y) \in W_0. \end{aligned}$$

Consider a path with k arcs, where $k > 0$ and even, from $(u, \mathbf{v})$ to $(a, \mathbf{v} + \mathbf{y})$:

$$(u, \mathbf{v}) = (x_0, \mathbf{v}) \to (x_1, \ldots) \to (x_2, \ldots) \to \cdots \to (x_k, \mathbf{v} + \mathbf{y}) = (a, \mathbf{v} + \mathbf{y}).$$

Using the definition of an arc in D_0, and setting $\mathbf{f}_{\mathbf{0}}(x_i, x_{i+1}) = \mathbf{g}(x_i) + \mathbf{h}(x_{i+1}) + w_i$, and $\mathbf{g}(x_i) - \mathbf{h}(x_i) = w_i'$, with all $w_i, w_i' \in W_0$, we obtain:

$$\begin{aligned} \mathbf{y} &= \mathbf{f}_{\mathbf{0}}(x_{k-1}, x_k) - \mathbf{f}_{\mathbf{0}}(x_{k-2}, x_{k-1}) + \cdots + \mathbf{f}_{\mathbf{0}}(x_1, x_2) - \mathbf{f}_{\mathbf{0}}(x_0, x_1) \\ &= \sum_{i=0}^{k-1} (-1)^{i+1} \mathbf{f}_{\mathbf{0}}(x_i, x_{i+1}) = \sum_{i=0}^{k-1} (-1)^{i+1} (\mathbf{g}(x_i) + \mathbf{h}(x_{i+1}) + w_i) \\ &= -\mathbf{g}(x_0) + \mathbf{h}(x_k) + \sum_{i=1}^{k-1} (-1)^{i-1} (\mathbf{g}(x_i) - \mathbf{h}(x_i)) + \sum_{i=0}^{k-1} (-1)^{i+1} w_i \\ &= -\mathbf{g}(x_0) + \mathbf{h}(x_k) + \sum_{i=1}^{k-1} (-1)^{i-1} w_i' + \sum_{i=0}^{k-1} (-1)^{i+1} w_i. \end{aligned}$$

Hence, $\mathbf{y} \in -\mathbf{g}(x_0) + \mathbf{h}(x_k) + W_0$. Similarly, for any path

$$(u, \mathbf{v}) = (x_0, \mathbf{v}) \to (x_1, \ldots) \to (x_2, \ldots) \to \cdots \to (x_k, \mathbf{v} + \mathbf{y}) = (a, -\mathbf{v} + \mathbf{y}),$$

with k arcs, where k is odd and at least 1, we obtain $\mathbf{y} \in \mathbf{g}(x_0) + \mathbf{h}(x_k) + W_0$.

The digraph D_0 is strong if and only if $W_0 = \langle \mathrm{Im}(\tilde{\mathbf{f}}_{\mathbf{0}}) \rangle = \mathbb{F}_q^l$ or, equivalently, $d = el$. Hence part (i) of the theorem is proven for D_0 and q odd.

Let $(u, \mathbf{v})$ be an arbitrary vertex of a strong component of D. The image of this vertex under the isomorphism ϕ, defined in (5), is $(u, \mathbf{v} - \frac{1}{2}\mathbf{f}(0,0))$, which belongs to the strong component of D_0 whose description is given by (1) with $\mathbf{v}$ replaced by $\mathbf{v} - \frac{1}{2}\mathbf{f}(0,0)$. Applying the inverse of ϕ to each vertex of this component of D_0 immediately yields the description of the component of D given by (2). This establishes the validity of part (i) of Theorem 1 for q odd.

For q even we first apply an argument similar to the one we used above for establishing components of D_0 for q odd. As $p = 2$, the argument becomes much shorter, and we obtain (3). Then we note that if

$$(u, \mathbf{v}) = (x_0, \mathbf{v}) \to (x_1, \dots) \to (x_2, \dots) \to \dots \to (x_k, \mathbf{v} + \mathbf{y})$$

is a path in D, then

$$\mathbf{y} = \sum_{i=0}^{k-1} \mathbf{f_0}(x_i, x_{i+1}) + \delta \cdot \mathbf{f}(0, 0),$$

where $\delta = 1$ if k is odd, and $\delta = 0$ if k is even.

For (ii), we first recall that any two cosets of W_0 in $\mathbb{F}_p^{kl}$ are disjoint or coincide. It is clear that for q odd, the cosets (1) coincide if and only if $\mathbf{v} \in \mathbf{g}(u) + W_0$. The vertex set of this strong component is $\{(a, \mathbf{h}(a) + W_0) \colon a \in \mathbb{F}_q\}$, which shows that this is the unique component of such type. As $|W_0| = p^d$, the component contains $q \cdot p^d = p^{e+d}$ vertices. In all other cases the cosets are disjoint, and their union is of order $2qp^d = 2p^{e+d}$. Therefore the number of strong components of D_0, which is isomorphic to D, is

$$\frac{|V(D)| - p^{e+d}}{2p^{e+d}} + 1 = \frac{p^{e(l+1)} - p^{e+d}}{2p^{e+d}} + 1 = \frac{p^{el-d} + 1}{2}.$$

For q even, our count follows the same ideas as for q odd, and the formulas giving the number of strongly connected components and the order of each component follow from (3).

For the isomorphism of strong components of the same order, let q be odd, and let D_1 and D_2 be two distinct strong components of D_0 each of order $2p^{e+d}$. Then there exist $(u_1, \mathbf{v}_1), (u_2, \mathbf{v}_2) \in V(D_0)$ with $\mathbf{v}_1 \notin \mathbf{g}(u_1) + W_0$ and $\mathbf{v}_2 \notin \mathbf{g}(u_2) + W_0$ such that $V(D_1) = \{(a, \mathbf{v}_1 + \mathbf{h}(a) - \mathbf{g}(u_1) + W_0) \colon a \in \mathbb{F}_q\}$ and $V(D_2) = \{(a, \mathbf{v}_2 + \mathbf{h}(a) - \mathbf{g}(u_2) + W_0) \colon a \in \mathbb{F}_q\}$.

Consider a map $\psi : V(D_1) \to V(D_2)$ defined by

$$(a, \pm\mathbf{v}_1 + \mathbf{h}(a) \mp \mathbf{g}(u_1) + \mathbf{y}) \mapsto (a, \pm\mathbf{v}_2 + \mathbf{h}(a) \mp \mathbf{g}(u_2) + \mathbf{y}),$$

for any $a \in \mathbb{F}_q$ and any $\mathbf{y} \in W_0$. Clearly, ψ is a bijection. Consider an arc (α, β) in D_1. If $\alpha = (a, \mathbf{v}_1 + \mathbf{h}(a) - \mathbf{g}(u_1) + \mathbf{y})$, then $\beta = (b, -\mathbf{v}_1 - \mathbf{h}(a) + \mathbf{g}(u_1) - \mathbf{y} + \mathbf{f_0}(a, b))$ for some $b \in \mathbb{F}_q$. Let us check that $(\psi(\alpha), \psi(\beta))$ is an arc in D_2. In order to find an expression for the second coordinate of $\psi(\beta)$, we first rewrite the second coordinate of β as $-\mathbf{v}_1 + \mathbf{h}(a) + \mathbf{g}(u_1) + \mathbf{y}'$, where $\mathbf{y}' \in W_0$. In order to do this, we use the definition of $\tilde{\mathbf{f}}_\mathbf{0}$ and the obvious equality $\mathbf{g}(b) - \mathbf{h}(b) = \tilde{\mathbf{f}}_\mathbf{0}(b, 0) \in W_0$. So we have:

$$\begin{aligned}
&- \mathbf{v}_1 - \mathbf{h}(a) + \mathbf{g}(u_1) - \mathbf{y} + \mathbf{f}(a, b) \\
=& - \mathbf{v}_1 - \mathbf{h}(a) + \mathbf{g}(u_1) - \mathbf{y} + \tilde{\mathbf{f}}_\mathbf{0}(a, b) + \mathbf{g}(b) + \mathbf{h}(a) \\
=& - \mathbf{v}_1 + \mathbf{h}(b) + \mathbf{g}(u_1) + (\mathbf{g}(b) - \mathbf{h}(b)) - \mathbf{y} + \tilde{\mathbf{f}}_\mathbf{0}(a, b) \\
=& - \mathbf{v}_1 + \mathbf{h}(b) + \mathbf{g}(u_1) + \mathbf{y}',
\end{aligned}$$

where $\mathbf{y}' = (\mathbf{g}(b) - \mathbf{h}(b)) - \mathbf{y} + \tilde{\mathbf{f}}_{\mathbf{0}}(a,b) \in W_0$. Now it is clear that $\psi(\alpha) = (a, \mathbf{v}_2 + \mathbf{h}(a) - \mathbf{g}(u_2) + \mathbf{y})$ and $\psi(\beta) = (b, -\mathbf{v}_2 + \mathbf{h}(b) + \mathbf{g}(u_2) + \mathbf{y}')$ are the tail and the head of an arc in D_2. Hence ψ is an isomorphism of digraphs D_1 and D_2.

An argument for the isomorphism of all strong components for q even is absolutely similar. This ends the proof of the theorem. $\square$

We illustrate Theorem 1 by the following example.

Example 3. Let $p \geqslant 3$ be prime, $q = p^2$, and $\mathbb{F}_q \cong \mathbb{F}_p(\xi)$, where ξ is a primitive element in $\mathbb{F}_q$. Let us define $f\colon \mathbb{F}_q^2 \to \mathbb{F}_q$ by the following table:

$y \backslash x$	0	1	$x \neq 0,1$
0	0	ξ	1
1	ξ	2ξ	ξ
$y \neq 0,1$	2	ξ	0

.

As 1 and ξ are values of f, $\langle \mathrm{Im}(f) \rangle = \mathbb{F}_q^2$. Nevertheless, $D(q;f)$ is not strong as we show below.

In this example, since $l = 1$, the function $\mathbf{f} = f$. Since $f(0,0) = 0$, $f_0 = f$, and

$$\mathbf{g}(t) = g(t) = f(t,0) = \begin{cases} 0, & t = 0, \\ \xi, & t = 1, \\ 1, & \text{otherwise} \end{cases}, \quad \mathbf{h}(t) = h(t) = f(0,t) = \begin{cases} 0, & t = 0, \\ \xi, & t = 1, \\ 2, & \text{otherwise} \end{cases}.$$

The function $\tilde{\mathbf{f}}_{\mathbf{0}}(x,y) = \tilde{f}(x,y) = f(x,y) - f(y,0) - f(0,x)$ can be represented by the table

$y \backslash x$	0	1	$x \neq 0,1$
0	0	0	-1
1	0	0	-2
$y \neq 0,1$	1	-1	-3

,

and so $\langle \mathrm{Im}(\tilde{f}_0) \rangle = \mathbb{F}_p \neq \langle \mathrm{Im}(f) \rangle = \mathbb{F}_{p^2}$.

As $l = 1$, $e = 2$, and $d = 1$, $D(q;f)$ has $(p^{le-d} + 1)/2 = (p+1)/2$ strong components. For $p = 5$, there are three of them. If $\mathbb{F}_{25} = \mathbb{F}_5[\xi]$, where ξ is a root of $X^2 + 4X + 2 \in \mathbb{F}_5[X]$, these components can be presented as:

$$\{(a, h(a) + \mathbb{F}_5)\colon a \in \mathbb{F}_{25}\},$$
$$\{(a, h(a) - \xi + \mathbb{F}_5)\colon a \in \mathbb{F}_{25}\} \cup \{(b, h(b) + \xi + \mathbb{F}_5)\colon b \in \mathbb{F}_{25}\},$$
$$\{(a, h(a) + 2\xi + \mathbb{F}_5)\colon a \in \mathbb{F}_{25}\} \cup \{(b, h(b) - 2\xi + \mathbb{F}_5)\colon b \in \mathbb{F}_{25}\}.$$

3 Connectivity of $D(q, m, n)$

The goal of this section is to prove Theorem 2.

For any $t \geqslant 2$ and integers $a_1, \ldots, a_t$, not all zero, let $(a_1, \ldots, a_t)$ (respectively $[a_1, \ldots, a_t]$) denote the greatest common divisor (respectively, the least common multiple) of these numbers. Moreover, for an integer a, let $\overline{a} = (q-1, a)$. Let $< \xi >= \mathbb{F}_q^*$, i.e., ξ is a generator of the cyclic group $\mathbb{F}_q^*$. (Note the difference between $< \cdot >$ and $\langle \cdot \rangle$ in our notation.) Suppose $A_k = \{x^k : x \in \mathbb{F}_q^*\}$, $k \geqslant 1$. It is well known (and easy to show) that $A_k =< \xi^{\overline{k}} >$ and $|A_k| = (q-1)/\overline{k}$.

We recall that for each positive divisor e_i of e, $q_i = (q-1)/(p^{e_i} - 1)$.

Lemma 4. *Let q_s be the largest of the q_i dividing $\overline{k}$. Then $\mathbb{F}_{p^{e_s}}$ is the smallest subfield of $\mathbb{F}_q$ in which A_k is contained. Moreover, $\langle A_k \rangle = \mathbb{F}_{p^{e_s}}$.*

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

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

as $x^{(p^e-1)/(p^{e_s}-1)}$ is the norm of x over $\mathbb{F}_{p^{e_s}}$ and hence is in $\mathbb{F}_{p^{e_s}}$. Suppose now that $A_k \subseteq \mathbb{F}_{p^{e_i}}$, where $e_i < e_s$. 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, $(q-1)/\overline{k}$ divides $p^{e_i} - 1$. Then $\overline{k} = r \cdot (q-1)/(p^{e_i} - 1) = rq_i$ for some integer r. Hence, q_i divides $\overline{k}$, and a contradiction is obtained as $q_i > q_s$. This proves that $\langle A_k \rangle$ is a subfield of $\mathbb{F}_{p^{e_s}}$ not contained in any smaller subfield of $\mathbb{F}_q$. Thus $\langle A_k \rangle = \mathbb{F}_{p^{e_s}}$. $\square$

Let $A_{m,n} = \{x^m y^n \colon x, y \in \mathbb{F}_q^*\}$, $m, n \geqslant 1$. Then, obviously, $A_{m,n}$ is a subgroup of $\mathbb{F}_q^*$, and $A_{m,n} = A_m A_n$ – the product of subgroups A_m and A_n.

Lemma 5. *Let $d = (q-1, m, n)$. Then $A_{m,n} = A_d$.*

Proof. As A_m and A_n are subgroups of $\mathbb{F}_q^*$, we have

$$|A_{m,n}| = |A_m A_n| = \frac{|A_m||A_n|}{|A_m \cap A_n|}. \tag{12}$$

It is well known (and easy to show) that if x is a generator of a cyclic group, then for any integers a and b, $< x^a > \cap < x^b >=< x^{[a,b]} >$. Therefore, $A_m \cap A_n =< \xi^{[\overline{m}, \overline{n}]} >$ and $|A_m \cap A_n| = (q-1)/\overline{[\overline{m}, \overline{n}]}$.

We wish to 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 (12) we find

$$|A_{m,n}| = \frac{(q-1)/\overline{m} \cdot (q-1)/\overline{n}}{(q-1)/\overline{[\overline{m}, \overline{n}]}} = \frac{(q-1) \cdot \overline{[\overline{m}, \overline{n}]}}{\overline{m} \cdot \overline{n}}. \tag{13}$$

We wish to simplify the last fraction in (13). Let M and N be such that $q-1 = M\overline{m} = N\overline{n}$. As $d = (q-1, m, n) = (\overline{m}, \overline{n})$, we have $\overline{m} = dm'$ and $\overline{n} = dn'$ for some co-prime integers

m' and n'. 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 integers a and b, both nonzero, it holds that $[a, b] = ab/(a, b)$. Therefore, we have

$$[\overline{m}, \overline{n}] = [dm', dn'] = \frac{dm'dn'}{(dm', dn')} = \frac{dm'dn'}{d(m', n')} = dm'n'.$$

Hence, $\overline{[\overline{m}, \overline{n}]} = (q-1, [\overline{m}, \overline{n}]) = (dm'n't, dm'n') = dm'n'$, and

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

Since $\overline{d} = (q-1, d) = d$ and $|A_d| = (q-1)/\overline{d}$, we have $|A_{m,n}| = |A_d|$ and so $A_{m,n} = A_d$. □

We are ready to prove Theorem 2.

Proof. For $D = D(q; m, n)$, we have

$$\langle \mathrm{Im}(\tilde{\mathbf{f}}_{\mathbf{0}}) \rangle = \langle \mathrm{Im}(f) \rangle = \langle \mathrm{Im}(x^m y^n) \rangle = \langle A_{m,n} \rangle = \langle A_d \rangle = \mathbb{F}_{p^{e_s}},$$

where the last two equalities are due to Lemma 5 and Lemma 4.

Part (i) follows immediately from applying Theorem 1 with $W = \mathbb{F}_{p^{e_s}}$, $\mathbf{g} = \mathbf{h} = 0$. 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 $q_s = 1$.

The other statements of Theorem 2 follow directly from the corresponding parts of Theorem 1. □

4 Open problems

We would like to conclude this paper with two suggestions for further investigation.

Problem 1. Suppose the digraphs $D(q; \mathbf{f})$ and $D(q; m, n)$ are strong. What are their diameters?

Problem 2. Study the connectivity of graphs $D(\mathbb{F}; \mathbf{f})$, where $\mathbf{f} \colon \mathbb{F}^2 \to \mathbb{F}^l$, and $\mathbb{F}$ is a finite extension of the field $\mathbb{Q}$ of rational numbers.

Acknowledgement

The authors are thankful to the anonymous referees whose thoughtful comments improved the paper; to Jason Williford for pointing to a mistake in the original version of Theorem 1; and to William Kinnersley for carefully reading the paper and pointing to a number of small errors.

References

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

[2] S.M. Cioabă, F. Lazebnik and W. Li, On the Spectrum of Wenger Graphs, *J. Combin. Theory Ser. B* 107: (2014), 132–139.

[3] V. Dmytrenko, F. Lazebnik and R. Viglione, An Isomorphism Criterion for Monomial Graphs, *J. Graph Theory* 48 (2005), 322–328.

[4] V. Dmytrenko, F. Lazebnik and J. Williford, On monomial graphs of girth eight. *Finite Fields Appl.* 13 (2007), 828–842.

[5] A. Kodess, Properties of some algebraically defined digraphs, Doctoral Thesis, University of Delaware, 2014.

[6] B.G. Kronenthal, Monomial graphs and generalized quadrangles, *Finite Fields Appl.* 18 (2012), 674–684.

[7] F. Lazebnik, D. Mubayi, New lower bounds for Ramsey numbers of graphs and hypergraphs, *Adv. Appl. Math.* 8 (3/4) (2002), 544–559.

[8] F. Lazebnik, A. Thomason, Orthomorphisms and the construction of projective planes, *Math. Comput.* 73 (247) (2004), 1547–1557.

[9] F. Lazebnik, J. Verstraëte, On hypergraphs of girth five, *Electron. J. Combin.* 10 (2003), #R25, 1–15.

[10] F. Lazebnik, R. Viglione, An infinite series of regular edge- but not vertex-transitive graphs, *J. Graph Theory* 41 (2002), 249–258.

[11] 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.

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

[13] T.A. Terlep, J. Williford, Graphs from Generalized Kac-Moody Algebras, *SIAM J. Discrete Math.* 26 no. 3 (2012), 1112–1120.

[14] V.A. Ustimenko, On the extremal regular directed graphs without commutative diagrams and their applications in coding theory and cryptography, *Albanian J. Math.* 1 (01/2007), 283–295.

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

[16] R. Viglione, On the Diameter of Wenger Graphs, *Acta Appl. Math.* 104 (2) (11/2008), 173–176.