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 \( f_i : \mathbb{F}_q^2 \to \mathbb{F}_q \) be arbitrary functions, where \( 1 \leq i \leq l \), \( i \) and \( l \) are integers. The digraph \( D = D(q; f) \), where \( f = (f_1, \ldots, f_l) : \mathbb{F}_q^2 \to \mathbb{F}_q^l \), is defined as follows. The vertex set of \( D \) is \( \mathbb{F}_q^{l+1} \). There is an arc from a vertex \( x = (x_1, \ldots, x_{l+1}) \) to a vertex \( y = (y_1, \ldots, y_{l+1}) \) if \( x_i + y_i = f_{i-1}(x_1, y_1) \) for all \( i, 2 \leq i \leq l + 1 \). 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 \( k \geq 2 \), a walk \( W \) from \( x_1 \) to \( x_k \) in \( D \) is an alternating sequence \( W = x_1a_1x_2a_2x_3 \cdots x_{k-1}a_{k-1}x_k \) 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 \( x_1 \to x_2 \to \cdots \to x_k \) 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
We call the functions $f$ and $x = (W,D)$ vertices in the electronic journal of combinatorics. We also call functions $q$ and interpolation (see, for example, Lidl, Niederreiter [12]), each $f$ the image of function $X$. As $f$ defining polynomials $i$, $m,n$ and we simplify the notation $f(q)$. The vertex set of $D$ is $F_q$. There is an arc from a vertex $x = (x_1,\ldots,x_{l+1})$ to a vertex $y = (y_1,\ldots,y_{l+1})$ if and only if $x_i + y_i = f_{i-1}(x_1,y_1)$ for all $i$, $2 \leq i \leq l+1$.

We call the functions $f_i$, $1 \leq i \leq l$, the defining functions of $D(q;f)$. If $l = 1$ and $f(x,y) = f_1(x,y) = x^my^n$, $1 \leq m,n \leq q - 1$, we call $D$ a monomial digraph, and denote it by $D(q;m,n)$. 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 [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 $F_q$ and $F_q^l$ can be viewed as vector spaces over $F_p$ of dimensions $e$ and $el$, respectively. For $X \subseteq F_q^l$, by $\langle X \rangle$ we denote the span of $X$ over $F_p$, which is the set of all finite linear combinations of elements of $X$ with coefficients from $F_p$. For any vector subspace $W$ of $F_q^l$, $\dim(W)$ denotes the dimension of $W$ over $F_p$. If $X \subseteq F_q^l$, let $v + X = \{v + x : x \in X\}$. Finally, let $\text{Im}(f) = \{(f_1(x,y),\ldots,f_l(x,y)) : (x,y) \in F^2\}$ denote the image of function $f$.

In this paper we study strong connectivity of $D(q;f)$. 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 $f : F_q^2 \rightarrow F_q^l$, we define $g(t) = f(t,0) - f(0,0)$, $h(t) = f(0,t) - f(0,0)$,

$$
\begin{align*}
\tilde{f}(x,y) &= f(x,y) - g(y) - h(x), \\
f_0(x,y) &= f(x,y) - f(0,0), \quad \text{and} \\
\tilde{f}_0(x,y) &= f_0(x,y) - g(y) - h(x).
\end{align*}
$$

As $g(0) = h(0) = 0$, one can view the coordinate function $g_i$ of $g$ (respectively, $h_i$ of $h$), $i = 1,\ldots,l$, as the sum of all terms of the polynomial $f_i$ containing only indeterminate
Let $\{v_1, v_2, \ldots, v_{l+1}\} \in \mathbb{F}_q^{l+1} = V(D)$ as an ordered pair $(v_1, v) \in \mathbb{F}_q \times \mathbb{F}_q^l$, where $v = (v_2, \ldots, v_{l+1})$.

The main result of this paper is the following theorem, which gives necessary and sufficient conditions for the strong connectivity of $D(q; f)$ and provides a description of its strong components in terms of $\langle \text{Im}(f_0) \rangle$ over $\mathbb{F}_p$.

**Theorem 1.** Let $D = D(q; f)$, $D_0 = D(q; f_0)$, $W_0 = \langle \text{Im}(f_0) \rangle$ 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 $(u, v)$ is

$$\left\{ (a, v + h(a) - g(u) + W_0) : a \in \mathbb{F}_q \right\} \cup \left\{ (b, -v + h(b) + g(u) + W_0) : b \in \mathbb{F}_q \right\} \smallsetminus \left\{ (a, \pm v + h(a) \mp g(u) + W_0) \right\}.$$  

(ii) If $q$ is even, then the strong component of $D$ containing a vertex $(u, v)$ is

$$\left\{ (a, v + h(a) + g(u) + W_0) : a \in \mathbb{F}_q \right\} \cup \left\{ (a, v + h(a) + g(u) + f(0, 0) + W_0) : a \in \mathbb{F}_q \right\} \smallsetminus \left\{ (a, v + h(a) + g(u) + W) : a \in \mathbb{F}_q \right\},$$

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

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

\[
\{(x, v + \mathbb{F}_{p^{e_i}}) : x \in \mathbb{F}_q \} \cup \{(x, -v + \mathbb{F}_{p^{e_i}}) : x \in \mathbb{F}_q \}.
\]

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

If \( q \) is even, then \( D \) has \( 2^{e_i} + e_s \) strong components, all isomorphic, and each is of order \( 2^{e_i} + e_s \).

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 \( D(q; f) \)

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 \( \phi: V(D) \to V(D_0) \) given by

\[
(x, y) \mapsto (x, y - \frac{1}{2} f(0, 0))
\]

is clearly a bijection. We check that \( \phi \) preserves adjacency. Assume that \((x_1, x_2, y_1, y_2)\) is an arc in \( D \), that is, \( x_2 + y_2 = f(x_1, y_1) \). Then, since \( \phi((x_1, x_2)) = (x_1, x_2 - \frac{1}{2} f(0, 0)) \) and \( \phi((y_1, y_2)) = (y_1, y_2 - \frac{1}{2} f(0, 0)) \), we have

\[
(x_2 - \frac{1}{2} f(0, 0) + y_2 - \frac{1}{2} f(0, 0)) = f(x_1, y_1) - f(0, 0) = f_0(x_1, y_1),
\]

and so \( \phi((x_1, x_2)), \phi((y_1, y_2)) \) is an arc in \( D_0 \). As the above steps are reversible, \( \phi \) preserves non-adjacency as well. Thus, \( D(q; f) \cong D_0 \).

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 \( f_0(0, 0) = \mathbf{0} \), we have \( g(t) = f_0(t, 0), h(t) = f_0(0, t), g(0) = h(0) = \mathbf{0} \), and \( \tilde{f}_0(x, y) = f_0(x, y) - g(y) - h(x) \).
Let \( \tilde{\alpha}_i, \ldots, \tilde{\alpha}_d \in \text{Im}(\tilde{f}_0) \) be a basis for \( W_0 \). Now, choose \( x_i, y_i \in \mathbb{F}_q \) be such that \( \tilde{f}_0(x_i, y_i) = \tilde{\alpha}_i, 1 \leq i \leq d \).

Let \((u, v)\) be a vertex of \( D_0 \). We first show that a vertex \((a, v + y)\) is reachable from \((u, v)\) if \( y \in h(a) - g(u) + W_0 \). In order to do this, we write an arbitrary \( y \in h(a) - g(u) + W_0 \) as
\[
y = h(a) - g(u) + (a_1 \tilde{\alpha}_1 + \cdots + a_d \tilde{\alpha}_d),\]
for some \( a_1, \ldots, a_d \in \mathbb{F}_p \), and consider the following directed walk in \( D_0 \):
\[
(u, v) \to (0, -v + f_0(u, 0)) = (0, -v + g(u))
\to (0, v - g(u))
\to (x_1, -v + g(u) + f_0(0, x_1)) = (x_1, -v + g(u) + h(x_1))
\to (y_1, v - g(u) - h(x_1) + f_0(x_1, y_1))
\to (0, -v + g(u) + h(x_1) - f_0(x_1, y_1) + g(y_1))
\to (0, -v + g(u) - f_0(x_1, y_1)) = (0, -v + g(u) - \tilde{\alpha}_1)
\to (0, v - g(u) + \tilde{\alpha}_1).
\]

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 \((0, v - g(u) + a_1 \tilde{\alpha}_1)\). Continuing a similar walk through vertices whose first coordinates are \( 0, x_i, y_i, 0, 0, 0, \) and \( 0, 2 \leq i \leq d, \) as many times as needed, one can reach vertex \((0, v - g(u) + (a_1 \tilde{\alpha}_1 + \cdots + a_i \tilde{\alpha}_i))\), and so on, until the vertex \((0, -v + g(u) - (a_1 \tilde{\alpha}_1 + \cdots + a_d \tilde{\alpha}_d))\) is reached. The vertex \((a, v + y)\) will be its out-neighbor. Here we indicate just some of the vertices along this path:
\[
\to \ldots
\to (0, v - g(u) + a_1 \tilde{\alpha}_1)
\to (x_2, -v + g(u) - a_1 \tilde{\alpha}_1 + h(x_2))
\to (y_2, v - g(u) + a_1 \tilde{\alpha}_1 - h(x_2) + f_0(x_2, y_2))
\to (0, -v + g(u) - a_1 \tilde{\alpha}_1 + h(x_2) - f_0(x_2, y_2) + g(y_2))
\to (0, v - g(u) + a_1 \tilde{\alpha}_1 - \tilde{\alpha}_2)
\to (0, v - g(u) + a_1 \tilde{\alpha}_1 + \tilde{\alpha}_2)
\to \ldots
\to (0, v - g(u) - a_1 \tilde{\alpha}_1 - a_2 \tilde{\alpha}_2)
\to \ldots
\to (0, v - g(u) - (a_1 \tilde{\alpha}_1 + \cdots + a_d \tilde{\alpha}_d))
\to (a, v - g(u) + h(a) + (a_1 \tilde{\alpha}_1 + \cdots + a_d \tilde{\alpha}_d))
\to (a, v + y).
\]

Hence, \((a, v + y)\) is reachable from \((u, v)\) for any \( a \in \mathbb{F}_q \) and any \( y \in h(a) - g(u) + W_0 \), as claimed. A slight modification of this argument shows that \((a, -v + y)\) is reachable from \((u, v)\) for any \( y \in h(a) + g(u) + W_0 \).
Let us now explain that every vertex of \( D_0 \) reachable from \((u, v)\) is in the set

\[
\{(a, \pm v \mp g(u) + h(a) + W_0) : a \in \mathbb{F}_q\}.
\]

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 \( \tilde{f} \):

\[
\tilde{f}_0(t, 0) = g(t) - h(t) = -\tilde{f}_0(0, t) \quad \text{and} \quad \tilde{f}_0(x, y) = g(x) + h(y) + \tilde{f}_0(x, y) - \tilde{f}_0(0, y) + \tilde{f}_0(0, x).
\]

The identities immediately imply that for every \( t, x, y \)

\[
\text{Theorem } 1 \text{ for } q \\
\text{odd.}
\]

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

\[
(u, v) = (x_0, v) \to (x_1, \ldots) \to (x_2, \ldots) \to \cdots \to (x_k, v + y) = (a, v + y).
\]

Using the definition of an arc in \( D_0 \), and setting \( f_0(x_i, x_{i+1}) = g(x_i) + h(x_{i+1}) + w_i \), and \( g(x_i) - h(x_i) = w'_i \), with all \( w_i, w'_i \in W_0 \), we obtain:

\[
y = f_0(x_{k-1}, x_k) - f_0(x_{k-2}, x_{k-1}) + \cdots + f_0(x_1, x_2) - f_0(x_0, x_1) = \sum_{i=0}^{k-1} (-1)^{i+1} f_0(x_i, x_{i+1}) = \sum_{i=0}^{k-1} (-1)^{i+1} (g(x_i) + h(x_{i+1}) + w_i) = -g(x_0) + h(x_k) + \sum_{i=1}^{k-1} (-1)^{i-1}(g(x_i) - h(x_i)) + \sum_{i=0}^{k-1} (-1)^{i+1} w_i = -g(x_0) + h(x_k) + \sum_{i=1}^{k-1} (-1)^{i-1} w'_i + \sum_{i=0}^{k-1} (-1)^{i+1} w_i.
\]

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

\[
(u, v) = (x_0, v) \to (x_1, \ldots) \to (x_2, \ldots) \to \cdots \to (x_k, v + y) = (a, -v + y),
\]

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

The digraph \( D_0 \) is strong if and only if \( W_0 = \langle \text{Im}(\tilde{f}_0) \rangle = \mathbb{F}_q^{d} \) or, equivalently, \( d = el \). Hence part (i) of the theorem is proven for \( D_0 \) and \( q \) odd.

Let \((u, v)\) be an arbitrary vertex of a strong component of \( D \). The image of this vertex under the isomorphism \( \phi \), defined in (5), is \((u, v - \frac{1}{2}f(0, 0))\), which belongs to the strong component of \( D_0 \) whose description is given by (1) with \( v \) replaced by \( v - \frac{1}{2}f(0, 0) \). Applying the inverse of \( \phi \) 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 

\[(u, v) = (x_0, v) \to (x_1, \ldots) \to (x_2, \ldots) \to \cdots \to (x_k, v + y)\]

is a path in \( D \), then

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

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

\[
\frac{|V(D)| - p^{d+1}}{2p^{d+1}} + 1 = \frac{p^{d+1} - p^{d+1}}{2p^{d+1}} + 1 = \frac{p^{d+1} + 1}{2}.
\]

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 \( 2p^{d+1} \). Then there exist \((u_1, v_1), (u_2, v_2) \in V(D_0) \) with \( v_1 \not\in g(u_1) + W_0 \) and \( v_2 \not\in g(u_2) + W_0 \) such that \( V(D_1) = \{(a, v_1 + h(a) - g(u_1) + W_0) : a \in \mathbb{F}_q\} \) and \( V(D_2) = \{(a, v_2 + h(a) - g(u_2) + W_0) : a \in \mathbb{F}_q\} \).

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

\[(a, \pm v_1 + h(a) \mp g(u_1) + y) \mapsto (a, \pm v_2 + h(a) \mp g(u_2) + y),\]

for any \( a \in \mathbb{F}_q \) and any \( y \in W_0 \). Clearly, \( \psi \) is a bijection. Consider an arc \((\alpha, \beta)\) in \( D_1 \). If \( \alpha = (a, v_1 + h(a) - g(u_1) + y) \), then \( \beta = (b, -v_1 - h(a) + g(u_1) - y + f_0(a, b)) \) 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 \( \beta \) as \(-v_1 + h(a) + g(u_1) + y', \) where \( y' \in W_0 \). In order to do this, we use the definition of \( f_0 \)

and the obvious equality \( g(b) - h(b) = f_0(b, 0) \in W_0 \). So we have:

\[-v_1 - h(a) + g(u_1) - y + f(a, b) \]
\[= -v_1 - h(a) + g(u_1) - y + \tilde{f}_0(a, b) + g(b) + h(a) \]
\[= -v_1 + h(b) + g(u_1) + (g(b) - h(b)) - y + \tilde{f}_0(a, b) \]
\[= -v_1 + h(b) + g(u_1) + y', \]
where \( y' = (g(b) - h(b)) - y + \tilde{f}_0(a, b) \in W_0 \). Now it is clear that \( \psi(\alpha) = (a, v_2 + h(a) - g(u_2) + y) \) and \( \psi(\beta) = (b, -v_2 + h(b) + g(u_2) + y') \) are the tail and the head of an arc in \( D_2 \). Hence \( \psi \) 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 \( p \geq 3 \) be prime, \( q = p^2 \), and \( \mathbb{F}_q \cong \mathbb{F}_p(\xi) \), where \( \xi \) is a primitive element in \( \mathbb{F}_q \). Let us define \( f: \mathbb{F}_2^2 \rightarrow \mathbb{F}_p \) by the following table:

\[
\begin{array}{c|c|c|c}
  x & 0 & 1 & x \neq 0, 1 \\
  \hline
  y & 0 & \xi & 1 \\
  1 & \xi & 2\xi & \xi \\
  y \neq 0, 1 & 2 & \xi & 0
\end{array}
\]

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

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

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

The function \( \tilde{f}_0(x, y) = \tilde{f}(x, y) = f(x, y) - f(y, 0) - f(0, x) \) can be represented by the table

\[
\begin{array}{c|c|c|c}
  x & 0 & 1 & x \neq 0, 1 \\
  \hline
  y & 0 & 0 & -1 \\
  1 & 0 & 0 & -2 \\
  y \neq 0, 1 & 1 & -1 & -3
\end{array}
\]

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

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

\[
\{(a, h(a) + \mathbb{F}_5) : a \in \mathbb{F}_{25}\},
\]

\[
\{(a, h(a) - \xi + \mathbb{F}_5) : a \in \mathbb{F}_{25}\} \cup \{(b, h(b) + \xi + \mathbb{F}_5) : b \in \mathbb{F}_{25}\},
\]

\[
\{(a, h(a) + 2\xi + \mathbb{F}_5) : a \in \mathbb{F}_{25}\} \cup \{(b, h(b) - 2\xi + \mathbb{F}_5) : b \in \mathbb{F}_{25}\}.
\]
3 Connectivity of \( D(q, m, n) \)

The goal of this section is to prove Theorem 2.

For any \( t \geq 2 \) 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 \( < \xi > \equiv F_q \), i.e., \( \xi \) is a generator of the cyclic group \( F_q^* \). (Note the difference between \( < \cdot > \) and \( \langle \cdot \rangle \) in our notation.) Suppose \( A_k = \{ x^k : x \in F_q^* \} \), \( k \geq 1 \). It is well known (and easy to show) that \( A_k = < \xi^k > \) and \( |A_k| = (q - 1)/k \).

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 \( k \). Then \( F_{p^{e_s}} \) is the smallest subfield of \( F_q \) in which \( A_k \) is contained. Moreover, \( \langle A_k \rangle = F_{p^{e_s}} \).

Proof. By definition of \( k \), \( q_s \) divides \( k \), so \( k = t q_s \) for some integer \( t \). Thus for any \( x \in F_q \),
\[
x^k = x^{t q_s} = \left( x^{(p^{e_s} - 1)} \right)^t \in F_{p^{e_s}},
\]
as \( x^{(p^{e_s} - 1)/(p^{e_i} - 1)} \) is the norm of \( x \) over \( F_{p^{e_s}} \) and hence is in \( F_{p^{e_i}} \). Suppose now that \( A_k \subseteq F_{p^{e_i}} \), where \( e_i < e_s \). Since \( A_k \) is a subgroup of \( F_{p^{e_i}} \), we have that \( |A_k| \) divides \( |F_{p^{e_i}}| \), that is, \( (q - 1)/k \) divides \( p^{e_i} - 1 \). Then \( k = r \cdot (q - 1)/(p^{e_i} - 1) = r q_i \) for some integer \( r \). Hence, \( q_i \) divides \( k \), and a contradiction is obtained as \( q_i > q_s \). This proves that \( \langle A_k \rangle \) is a subfield of \( F_{p^{e_i}} \) not contained in any smaller subfield of \( F_q \). Thus \( \langle A_k \rangle = F_{p^{e_i}} \). \( \square \)

Let \( A_{m,n} = \{ x^m y^n : x, y \in F_q^* \} \), \( m, n > 1 \). Then, obviously, \( A_{m,n} \) is a subgroup of \( F_q^* \), 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 \( F_q^* \), we have
\[
|A_{m,n}| = |A_m A_n| = \frac{|A_m||A_n|}{|A_m \cap A_n|}.
\]
(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, \( A_m \cap A_n = < \xi^{[m,n]} > \) and
\[
|A_m \cap A_n| = \frac{(q - 1)/[m, n]}{(q - 1)/[\overline{m}, \overline{n}]}.
\]

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

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

Hence, \( \left[ \frac{m}{n}, \frac{n}{m} \right] = (q - 1, \left[ \frac{m}{n}, \frac{n}{m} \right]) = (dm'n't, dm'n') = dm'n' \), and

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

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

We are ready to prove Theorem 2.

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

\[
\langle \text{Im}(\tilde{f}_0) \rangle = \langle \text{Im}(f) \rangle = \langle \text{Im}(x^my^n) \rangle = \langle A_{m,n} \rangle = \langle A_d \rangle = \mathbb{F}_{p^e},
\]

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

Part (i) follows immediately from applying Theorem 1 with \( W = \mathbb{F}_{p^e}, g = h = 0 \). Also, \( D \) is strong if and only if \( \mathbb{F}_{p^e} = \mathbb{F}_q \), 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. \( \square \)

### 4 Open problems

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

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

**Problem 2.** Study the connectivity of graphs \( D(\mathbb{F}; f) \), where \( f: \mathbb{F}^2 \to \mathbb{F}^l \), 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


