A result on polynomials derived via graph theory

Robert S. Coulter
University of Delaware
Newark, Delaware 19716
coulter@udel.edu

Stefaan De Winter
Michigan Technological University
Houghton, Michigan 49931
sgdwint@mtu.edu

Alex Kodess
Farmingdale State College
Farmingdale, New York 11735
alex.kodess@farmingdale.edu

Felix Lazebnik
University of Delaware
Newark, Delaware 19716
fellaz@udel.edu

Math Subject Classification: 05C20, 11T06, 05C60.

Graph theory is a comparatively young mathematical discipline. It is often hard to construct graphs that satisfy certain properties purely combinatorially, i.e., by taking a set of vertices and saying which vertex is connected to which. Often such areas of classical mathematics as number theory, geometry, or algebra are used for this, and the methods from the related areas are used to prove the properties of the obtained graphs. The examples are numerous, and many of them can be found in books and comprehensive survey articles. See, for example, Alon [2]; Babai and Frankl [5]; Biggs [6]; Füredi and Simonovits [12]; Brouwer and Haemers [8], and Alon and Spencer [3]. Here we wish to mention just a few such applications. The probabilistic method was used to prove the existence of certain graphs in Ramsey theory, and explicit constructions for these graphs are still unknown (see [3]). Constructions and analysis of Ramanujan graphs are often based on algebra and number theory. Methods of linear algebra are fundamental for studies of expanders and graphs with high degree of symmetry (see [5] and [8]). Lovász’s proof [20] of a conjecture on the chromatic number of Kneser graphs made use of algebraic topology.

Can the direction be reversed, i.e., can graph theory be used to obtain results in some classical areas of mathematics? Sometimes it can, but the number of such instances is much smaller. See, for example, Swan’s proof of the Amitsur-Levitzki theorem [24], or a counterexample to Borsuk’s conjecture by Kahn and Kalai [14] and related work by Bondarenko [7]. Extremal graph theory was used in probability by Katona [15], and in geometry and potential theory by Turán [25], and Erdős, Meir, Sos, and Turán [11]. For some applications of graph theory to linear algebra, see Doob [10]. A number of applications of graph theory to pure mathematics are mentioned in Lovász, Pyber,
Welsh and Ziegler [21]. The story we wish to share is about one such example. It was discovered entirely not by design.

In order to describe our problem, we need a few preliminaries. Let $p$ be a prime number, and $\mathbb{Z}_p = \{0, 1, 2, \ldots, p - 1\}$ be the set of residue classes of integers modulo $p$, where each class is represented by the unique integer $i$, $0 \leq i \leq p - 1$ belonging to that class. It is known (see for example, Ireland and Rosen [13]) that with respect to modular arithmetic, $\mathbb{Z}_p$ is a field. For instance, in $\mathbb{Z}_7$, $1 + 6 = 0$, $3 \cdot 4 = 5$, and $3^{-1} = 5$ since $3 \cdot 5 = 1$. One can consider polynomials with coefficients from $\mathbb{Z}_p$; let $\mathbb{Z}_p[X]$ denote the set of all of them. Every polynomial $f \in \mathbb{Z}_p[X]$ defines a function on $\mathbb{Z}_p$ when it is evaluated at elements of $\mathbb{Z}_p$. For example, for $f = X^3 - 4X + 6 = X^3 + 3X + 6 \in \mathbb{Z}_7[X]$, $f(0) = 6$, $f(1) = 1^3 + 3 \cdot 1 + 6 = 10 = 3$, and $f(2) = 20 = 6$. Also, $f(3) = 42 = 0$, and we say that $3$ is a root of $f$. Counting or estimating the number of roots of polynomials from $\mathbb{Z}_p[X]$ in $\mathbb{Z}_p$ is a fundamental problem in the area of mathematics called algebraic geometry.

All results in this article hold over any finite field of odd characteristic, but for ease of presentation we will simply use the field $\mathbb{Z}_p$, $p > 2$.

Here is the problem. Recently we were surprised to learn that for any prime $p$, we define the directed graph $D = (V, A)$ is a pair of two sets $V$ and $A \subseteq V \times V$; $V$ is called the set of vertices of $D$, and $A$ is called the set of arcs of $D$. All undefined terms related to digraphs can be found in Bang-Jensen and Gutin [1].

The digraph $D$ of Figure 1(a) has vertex set $V = \{a, b, c, d\}$ and arc set $A = \{(a, b), (a, c), (b, b), (b, c), (c, a), (d, a), (d, c)\}$. Arc $(b, b)$ is called a loop, and we say that vertex $b$ has a loop on it. Given a digraph $D = (V, A)$, a digraph $H = (V_1, A_1)$ is called a subdigraph of $D$ if $V_1 \subseteq V$ and $A_1 \subseteq A$ (see Figure 1(b)).

![Figure 1](image-url) Digraph $D$ and its subdigraph $H$.

We shall be interested in a certain type of digraphs. For any positive prime $p$, and any positive integers $m, n$, we define the directed graph $D(p; m, n) = (V, A)$, with vertex set $V = \mathbb{F}_p \times \mathbb{F}_p$ and arc set $A$ as follows: the ordered pair of vertices $((x_1, x_2), (y_1, y_2))$ is an arc if

$$x_2 + y_2 = x_1^m y_1^n.$$
We call \( D(p; m, n) \) a monomial digraph. It is known (and often referred to as Fermat’s little theorem), that \( x^p = x \) for any \( x \in \mathbb{F}_p \). It is therefore sufficient to restrict integers \( m \) and \( n \) in the definition of \( D(p; m, n) \) to the set \( \{1, \ldots, p - 1\} \). We thus have \((p - 1)^2\) digraphs \( D(p; m, n) \) for every prime \( p \).

The digraphs \( D(p; m, n) \) are directed analogues (see Kodess [16], Kodess and Lazebnik [17]) of particular cases of a well studied class of algebraically defined undirected graphs having many applications, see surveys by Lazebnik and Woldar [18] and Lazebnik, Sun, and Wang [19].

Figure 2 shows \( D(3; 1, 2) \). Note that \((2, 2), (1, 0)\) is an arc, since according to the adjacency condition above, \( 2 + 0 = 2^1 \cdot 1^2 \) in \( \mathbb{F}_3 \); \((1, 0), (2, 2)\) is not an arc, since \( 0 + 2 \neq 1^1 \cdot 2^2 \) in \( \mathbb{F}_3 \); and vertex \((1, 2)\) has a loop on it since, \( 2 + 1 = 1 \cdot 1^2 \) in \( \mathbb{F}_3 \).

![Figure 2](image-url)

**Figure 2** The digraph \( D(3; 1, 2): x_2 + y_2 = x_1 y_1^2 \).

As all these \((p - 1)^2\) digraphs \( D(p; m, n) \) share the same vertex set, one cannot help wondering if they are actually different. For instance, it is not hard to see that \( D(3; 1, 2) \) and \( D(3; 2, 1) \) can be obtained one from the other by reversing the orientation of every arc, but not by relabeling the vertices! The reason for this will become more clear later.

A very thorough and tedious inspection or any modern computer would reveal that the digraphs \( D(5; 1, 2) \) and \( D(5; 3, 2) \), both having 25 vertices, are in fact not much different: one can be obtained from the other by relabeling the vertices in a certain way.

We would like to make this discussion a little more formal.

Central to many areas of mathematics is the concept of isomorphism. It is defined for such ubiquitous and important objects as vector spaces, groups, fields and graphs, to name just a few. Informally, two objects are called isomorphic if they are not fundamentally different in their structure; that is, one of them can be obtained from the other by renaming or relabeling the elements while preserving the internal structure. Formally, we call digraphs \( D_1 \) and \( D_2 \) isomorphic and write \( D_1 \cong D_2 \) if there is a bijective function \( f \) from the vertex set \( V(D_1) \) of \( D_1 \) to the vertex set \( V(D_2) \) of \( D_2 \) such that for any two vertices \( u, v \in V(D_1) \), \((u, v)\) is an arc in \( D_1 \) if and only if \((f(u), f(v))\) is an arc in \( D_2 \). That is, \( f \) preserves adjacency and non-adjacency mapping vertices of \( D_1 \) to those of \( D_2 \). Such a mapping \( f \) is called an isomorphism from \( D_1 \) to \( D_2 \). To illustrate this idea we refer to Figure 3.

The two digraphs on the left, \( D_1 \) and \( D_2 \), are isomorphic because the mapping defined as \( f(1) = a, f(2) = b, f(3) = c, f(4) = d \), is clearly a bijection; and it is a routine verification to check that \( f \) preserves adjacency and non-adjacency. For instance,
(a) Two isomorphic digraphs.
(b) Two non-isomorphic digraphs.

Figure 3 The concept of isomorphism of digraphs.

(2, 3) is an arc in $D_1$, and its image $(f(2), f(3)) = (b, c)$ is an arc in $D_2$, whereas $(1, 3)$ and its image $(f(1), f(3)) = (a, c)$ are not arcs in $D_1$ and $D_2$, respectively.

The reader should be convinced that not only arcs but all digraph-theoretic properties (that is, those independent of the actual labeling of the vertices) are shared by two isomorphic digraphs. For example, if $g$ is an isomorphism from a digraph $H_1$ to a digraph $H_2$, then every vertex $x$ of $H_1$ and the vertex $g(x)$ of $H_2$ have the same number of in-going arcs, and the same number of out-going arcs. This observation helps establishing the fact that the two digraphs on the right in Figure 3, $D_1$ and $D_3$, are not isomorphic: in $D_3$ vertex $a$ has two out-going arcs, whereas $D_1$ has no vertex with this property. Other properties shared by isomorphic (di)graphs include the number of (directed) cycles of a given length, the total number of (directed) cycles, the number of (strong) components, etc. Note that simply reversing the orientation of every arc in a digraph may or may not produce a digraph isomorphic to the original one. See Figure 4.

(a) Reversing the arcs produces an isomorphic digraph.
(b) Reversing the arcs produces a non-isomorphic digraph.

Figure 4 Reversing the arcs of a digraph.

Suppose one has a large set of digraphs and wants to find all its members with a particular property. Every member of the set can be considered and checked for having the property, but, as isomorphic digraphs possess the property simultaneously, it is sufficient to check only one of them. So only one member of a class of isomorphic digraphs can be considered. Therefore, if one has an efficient way for establishing isomorphism of digraphs from the set, the original set of digraphs can be replaced by a smaller subset of it (and often much smaller) consisting of one “representative” of each class of isomorphic graphs, and the property can be checked only for digraphs from this subset. This approach becomes even more efficient when we wish to check multiple properties for digraphs from the original set. Once its members are “sorted for isomorphism”, every property can be checked for only one representative of each
isomorphic class. Unfortunately, establishing isomorphism between digraphs is often not easy.

Asking whether two objects are isomorphic and searching for effective computational tools for answering this question has been the subject of a number of highly publicized mathematical endeavors in the 20th century. The reader may have heard of the Classification of Finite Simple Groups problem that seeks to give a complete list of such groups up to isomorphism; see expositions by Solomon [22, 23]. Another example is the Graph Isomorphism Problem which is concerned with finding fast algorithms for determining whether two finite graphs are isomorphic. For recent progress on this problem, see Babai [4].

The question of isomorphism of two monomial digraphs \( D_1 = D(p; m_1, n_1) \) and \( D_2 = D(p; m_2, n_2) \) is open, and it is this question that originally motivated us. In an attempt to answer this question one would seek necessary and sufficient conditions on the parameters \( m_1, n_1, m_2, n_2 \) under which the two digraphs \( D_1 \) and \( D_2 \) are isomorphic. One idea to attack this problem is to look at various subdigraphs of \( D_1 \) and \( D_2 \).

Let \( X \) and \( Y \) be arbitrary digraphs, and let \( N(X, Y) \) denote the number of subdigraphs of \( X \) each of which is isomorphic to \( Y \). In trying to decide whether two given digraphs \( X_1 \) and \( X_2 \) are isomorphic one could hope to find a “test digraph” \( Y \) such that \( N(X_1, Y) = N(X_2, Y) \) if and only if \( X_1 \cong X_2 \). This approach was successful in the case of a certain class of undirected graphs, see Dmytrenko, Lazebnik, and Viglione [9]. In attempting to replicate this success for the class of monomial digraphs, we were led to consider the digraph \( K \) of Figure 5. We must admit at this point that \( K \) was not a good test digraph: much to our regret, we discovered a great many pairs of non-isomorphic monomial digraphs \( D_1 \) and \( D_2 \) containing the same number of (isomorphic) copies of \( K \). Counting \( N(D(p; m, n), K) \), however, led to the result on the number of roots of certain polynomials over finite fields that we have already mentioned. Let us present our solution.

**Theorem.** For any odd prime \( p \) and any natural numbers \( m \) and \( n \) satisfying \( mn \equiv 1 \mod (p - 1) \), the trinomials \( X^{m+1} - 2X + 1 \) and \( X^{n+1} - 2X + 1 \) have the same number of distinct roots in \( \mathbb{F}_p \).

**Proof.** Set \( D_m = D(p; 1, m) \), \( D_n = D(p; 1, n) \) and \( D'_n = D(p; n, 1) \). We first argue that \( D_m \) and \( D'_n \) are isomorphic, and as such, contain the same number of isomorphic copies of \( K \) shown in Figure 5.

As \( mn \equiv 1 \mod (p - 1) \) implies \( n \cdot m - t \cdot (p - 1) = 1 \) for some integer \( t \), we conclude that \( \gcd(m, p - 1) = 1 \).

We now recall that the multiplicative group \( \mathbb{F}_p^* \) of \( \mathbb{F}_p \) is cyclic of order \( p - 1 \). This implies by elementary theory of cyclic groups that \( x \mapsto x^m \) is a permutation (bijective function) on \( \mathbb{F}_p \). Also for any integers \( k, l \) and any \( x \in \mathbb{F}_p \), \( k \equiv l \mod (p - 1) \) implies \( x^k = x^l \). Proofs of these facts can be found in [13].

Consider the mapping \( \psi : V(D_m) \to V(D'_n) \) defined by \( \psi((x, y)) = (x^m, y) \). We verify that \( \psi \) satisfies the definition of digraph isomorphism discussed above. Clearly

\[
\psi(\alpha) = \beta
\]

**Figure 5** The digraph \( K \).
Then its image \((\psi((x_1, x_2)), \psi((y_1, y_2)))\) is an arc in \(D'_n\), since
\[
x_2 + y_2 = x_1^m y_1^m.
\]
Similarly, we show that \(\psi\) preserves non-adjacency: if \(( (x_1, x_2), (y_1, y_2))\) is not an arc in \(D_m\), then
\[
x_2 + y_2 \neq x_1^m y_1^m,
\]
and so \((\psi((x_1, x_2)), \psi((y_1, y_2)))\) is not an arc in \(D'_n\). This implies by definition that \(D_m\) and \(D'_n\) are isomorphic. Hence, \(N(D_m, Y) = \hat{N}(D'_n, Y)\) for any digraph \(Y\). In particular, \(N(D_m, K) = N(D'_n, K)\).

Now let \(H^c\) denote the converse of digraph \(H\), that is, the digraph obtained from \(H\) by reversing all its arcs. Obviously, for any digraph \(D\), \(N(D, H) = N(D^c, H^c)\), and also \((H^c)^c = H\). Observe that \(D'_n\) is simply \(D_n\) with all arcs reversed, that is \(D'_n = D_n^c\). Thus \(D_n^c\) and \((D_n^c)^c = D_n\) are equal. Since \(K^c \cong K\), we have
\[
N(D_m, K) = N(D'_n, K) = N(D_n^c, K^c) = N(D_n^c, K) = N(D_n, K).
\]
Note that we did not assume that \(D_m\) and \(D_n\) were isomorphic! Actually we conjecture that they never are unless \(m = n\).

We now show that the number of isomorphic copies of \(K\) in a digraph \(D_n\) can be expressed as the number of distinct roots of a polynomial of degree \(n + 1\) in the field \(\mathbb{F}_p\).

Suppose \(K\) is a subgraph of \(D_n = D(p; 1, n)\), and let \(\alpha = (u, s)\) and \(\beta = (v, t)\) be vertices of \(K\). From the relations defining the three arcs of \(K\), we have
\[
s + s = u \cdot u^n, \quad t + t = v \cdot v^n, \quad \text{and} \quad s + t = uv^n.
\]
Note that since \(p\) is odd, \(2 \in \mathbb{F}_p\) is invertible. Hence, we obtain
\[
s = \frac{1}{2} u^{n+1}, \quad t = \frac{1}{2} v^{n+1}, \quad \text{and} \quad s + t = uv^n. \tag{1}
\]
If \(u = v\), then the first and the second equation of system (1) imply \(s = t\), and so vertices \(\alpha\) and \(\beta\) are equal. Therefore, \(u \neq v\).

It follows from (1) that the equation \(s + t = uv^n\) can be rewritten as
\[
\frac{1}{2} u^{n+1} + \frac{1}{2} v^{n+1} = uv^n. \tag{2}
\]
Note that neither \(u\) nor \(v\) is 0. Indeed, if \(u = 0\), then substituting it to the first and to the third equation of the system (1), we get \(s = 0\) and \(s + t = 0\). Hence, \(t = 0\), and from the second equation we get \(v = 0\). Hence, \(\alpha = \beta = (0, 0)\) — a contradiction. Therefore, \(u \neq 0\). Similarly, \(v \neq 0\), and \(uv \neq 0\). Dividing both sides of (2) by \((1/2)uv^n\), we obtain
\[
(u/v)^n + (v/u) = 2.
\]
Setting \(w = u/v\), we rewrite this equation as \(w^{n+1} - 2w + 1 = 0\). Hence, \(u/v\) is a root of the polynomial \(f_n(X) = X^{n+1} - 2X + 1 \in \mathbb{F}_p[X]\). It is not equal to the obvious root 1, as \(u \neq v\).
Consequently, \( N(D_n, K) = (p - 1)R(n) \), where \( R(n) \) is the number of distinct roots of \( f_n \) in \( \mathbb{F}_p \setminus \{1\} \); any choice of root and any choice of \( u \) must determine \( \alpha \) and \( \beta \) uniquely.

Now if \( m \) and \( n \) are integers satisfying the conditions of the theorem, we have from before that

\[
(p - 1)R(m) = N(D_m, K) = N(D_n, K) = (p - 1)R(n),
\]

and so \( R(m) = R(n) \).

Thus, from an isomorphism problem for digraphs, we have arrived at an interesting fact concerning trinomials over finite fields. The theorem can be immediately generalized in various ways and proved directly, i.e., without considering graphs or digraphs. We suggest that the reader find a proof for the following generalization.

**Exercise.** For any prime power \( q \) (even or odd) and any natural numbers \( m \) and \( n \) satisfying \( mn \equiv 1 \mod (q - 1) \), polynomials \( X^{m+1} + aX + b \) and \( X^{n+1} + aX + b^m \) have the same number of distinct roots in the finite field \( \mathbb{F}_q \) for any \( a, b \in \mathbb{F}_q \).

We end this note with two open questions concerning monomial digraphs which we find very interesting. Though we do not know the answers even for prime \( q \), we state the questions for any prime power \( q \). Let \( D_1 = D(q; m_1, n_1) \) and \( D_2 = D(q; m_2, n_2) \).

**Problem.** Is there a digraph \( H \) such that the equality \( N(D_1, H) = N(D_2, H) \) is equivalent to \( D_1 \cong D_2 \)?

**Problem.** Find necessary and sufficient conditions on \( q, m_1, n_1, m_2, n_2 \), such that digraphs \( D_1 \) and \( D_2 \) are isomorphic.

A related conjecture appears in [16]:

**Conjecture.** 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

\[
m_2 \equiv km_1 \mod (q - 1) \quad \text{and} \quad n_2 \equiv kn_1 \mod (q - 1).
\]

**Acknowledgement.** The authors are thankful to the anonymous referees whose thoughtful comments improved the paper. The work of the last author was partially supported by a grant from the Simons Foundation #426092.

**References**

Summary We present an example of a result in graph theory that is used to obtain a result in another branch of mathematics. More precisely, we show that the isomorphism of certain directed graphs implies that some trinomials over finite fields have the same number of roots.

ROBERT S. COULTER (615822) (coulter@udel.edu) joined the faculty at the University of Delaware in 2003, having previously held positions at the University of Queensland, Queensland University of Technology, and Deakin University. He received his Ph.D. from the Department of Computer Science and Electrical Engineering at the University of Queensland in 1998. He is an Australian, and greatly misses Farmers Union Iced Coffee and the lack of snow shovels.

STEFAAN DE WINTER (723701) (sgdewint@mtu.edu) moved to Michigan Technological University in 2011 and made such a great impression that he was promoted early to Associate Professor. Though he heralds from Belgium, he abandoned the great chocolate and beer of his homeland, not to mention the cycling, and moved to the United States in pursuit of happiness, a pursuit in which he was ironically successful through the medium of another foreign national!

ALEX KODESS (886420) (alex.kodess@farmingdale.edu) has recently moved to the Empire State and joined the Mathematics Department of Farmingdale State College. In the past he escaped the clutches of the state institution of the second smallest state in the country, only to be subsumed by the smallest. In exchanging the University of Rhode Island for the University of Delaware, he could at least be content in the knowledge his status “improved” from Ph.D. student to faculty member. His only regret is that he now finds he is expected to act like a responsible adult.
FELIX LAZEBNIK (111260) (fellaz@udel.edu) has been at the University of Delaware since receiving his Ph.D. from the University of Pennsylvania under Herbert S. Wilf in 1987. He claims to understand Robert’s English, Alex’ Ph.D. Thesis and some of Stefaan’s geometry.