Isomorphism Criterion for Monomial Graphs

Vasyl Dmytrenko,[1] Felix Lazebnik,[1] and Raymond Viglione[2]

[1]*DEPARTMENT OF MATHEMATICAL SCIENCES*
UNIVERSITY OF DELAWARE, NEWARK
DELAWARE 19716
E-mail: dmytrenk@math.udel.edu; lazebnik@math.udel.edu

[2]*DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE*
KEAN UNIVERSITY, UNION, NEW JERSEY 07083
E-mail: rviglion@kean.edu

Received May 23, 2003; Revised June 23, 2004

Published online in Wiley InterScience(www.interscience.wiley.com).
DOI 10.1002/jgt.20055

Abstract: Let q be a prime power, $\mathbb{F}_q$ be the field of q elements, and k, m be positive integers. A bipartite graph $G = G_q(k, m)$ is defined as follows. The vertex set of G is a union of two copies P and L of two-dimensional vector spaces over $\mathbb{F}_q$, with two vertices $(p_1, p_2) \in P$ and $[l_1, l_2] \in L$ being adjacent if and only if $p_2 + l_2 = p_1^k l_1^m$. We prove that graphs $G_q(k, m)$ and $G_{q'}(k', m')$ are isomorphic if and only if $q = q'$ and $\{\gcd(k, q-1), \gcd(m, q-1)\} = \{\gcd(k', q-1), \gcd(m', q-1)\}$ as multisets. The proof is based on counting the number of complete bipartite subgraphs in the graphs. © 2005 Wiley Periodicals, Inc. J Graph Theory 48: 322–328, 2005

Keywords: *algebraic constructions; graph isomorphism; number of complete bipartite subgraphs*

1. INTRODUCTION AND RESULTS

Let q be a prime power, and let $\mathbb{F}_q$ be the field of q elements. For a function $f : \mathbb{F}_q^2 \to \mathbb{F}_q$, let a bipartite graph $G = G_q(f)$ be defined as follows. The vertex set

of G is a union of two copies P and L of two-dimensional vector spaces over $\mathbb{F}_q$. Their elements are called *points* and *lines*, respectively, and a point $(p)=(p_1,p_2)$ and a line $[l]=[l_1,l_2]$ are adjacent, denoted $(p)\sim[l]$, if and only if

$$p_2+l_2=f(p_1,l_1). \tag{1}$$

Graphs $G_q(f)$ are the simplest representatives of the general family of graphs defined by systems of equations. For the definition of these graphs, their origins and numerous applications, see [7] and references therein. For more recent applications, see [2]–[6] and [8]. Though most constructions in the papers mentioned above were motivated by particular applications, the study of general properties of these graphs, initiated in [7] and continued in [8], turned out to be an exciting area of research. Understanding graphs $G_q(f)$, which are defined by a single equation (1), is fundamental for understanding the graphs defined by systems of equations which contain equation (1). This is due to the fact that no matter what the other equations of a defining system are, there exists a covering homomorphism of the graph defined by the system on the graph $G_q(f)$, see [7].

In studying graphs $G_q(f)$, one of the first questions that arises is the isomorphism question. Given q and two functions f and g, when are $G_q(f)$ and $G_q(g)$ isomorphic? The question has already been shown to be hard for 4-cycle free graphs, since it is related to the question of isomorphism of finite projective planes, see [4]. To our knowledge, the only non-trivial case for the isomorphism problem which has been partially settled is the case when both f and g can be represented by monomials. We refer to these graphs as *monomial* graphs, and for $f=x^k y^m$, we denote the graph $G_q(x^k y^m)$ by $G_q(k,m)$. In [8], a necessary and sufficient condition for the isomorphism of two monomial graphs is given for sufficiently large q. In this note, we strengthen that result by extending it to all prime powers q. The graph invariant used in [8] was surprisingly simple: the number of 4-cycles in the graph. The invariants we consider are its generalizations, namely the numbers of complete bipartite subgraphs with fixed partition sizes.

For a positive integer a, let $\bar{a}=\gcd(a,q-1)$ denote the greatest common divisor of a and $q-1$. Our main result is the following.

Theorem 1.1. *Let k,m,k',m' be positive integers and let q,q' be prime powers. The graphs $G_q(k,m)$ and $G_{q'}(k',m')$ are isomorphic if and only if $q=q'$ and $\{\bar{k},\bar{m}\}=\{\bar{k'},\bar{m'}\}$ as multisets.*

Let $G=G_q(k,m)$. For a fixed prime power q and fixed integers $k\geq 1$ and $s\geq 2$, let

$$J_{k,s}=\frac{1}{s!}(q-1)(\bar{k}-1)(\bar{k}-2)\cdots(\bar{k}-(s-1))=\frac{q-1}{\bar{k}}\binom{\bar{k}}{s}.$$

Of course, $\binom{a}{b} = 0$ for all integers a, b such that $0 \le a < b$. By $I_G(s,t)$, we will denote the number of subgraphs of G isomorphic to the complete bipartite graph $K_{s,t}$, $s, t \ge 2$.

Our proof of Theorem 1.1 is based on the following theorem, which is also of independent interest.

Theorem 1.2. *Let q be a prime power, let k, m, s, t be positive integers, $s, t \ge 2$, and let $G = G_q(k,m)$. Then*

(a) $I_G(s,t) = q\left(\binom{q}{s}(J_{k,t} + J_{m,t}) + \binom{q}{t}(J_{k,s} + J_{m,s}) - J_{k,s}J_{m,t} - J_{k,t}J_{m,s}\right)$, if $s \ne t$,

(b) $I_G(s,s) = q\left(\binom{q}{s}\left(J_{k,s} + J_{m,s}\right) - J_{k,s}J_{m,s}\right)$.

Theorem 1.1 allows an immediate generalization to some graphs $G_q(f)$, where f is not a monomial. Let α, β be two bijections on $\mathbb{F}_q$, and k, m be positive integers. A bipartite graph $G_q(\alpha, \beta, k, m)$ is defined to have the same partition classes P and L as graph $G_q(k,m)$, with two vertices $(p_1, p_2) \in P$ and $[l_1, l_2] \in L$ being adjacent if and only if $p_2 + l_2 = (\alpha(p_1))^k (\beta(l_1))^m$.

Corollary 1.3. *Let k, m, k', m' be positive integers, let q, q' be prime powers, let α, β be two bijections on $\mathbb{F}_q$, and let α', β' be two bijections on $\mathbb{F}_{q'}$. The graphs $G_q(\alpha, \beta, k, m)$ and $G_{q'}(\alpha', \beta', k', m')$ are isomorphic if and only if $q = q'$ and $\{\bar{k}, \bar{m}\} = \{\bar{k'}, \bar{m'}\}$ as multisets. In case of isomorphism, both graphs are isomorphic to $G_q(k,m)$.*

2. PROOFS

We begin with several simple observations. Since $x^q = x$ for any $x \in \mathbb{F}_q$, we can always assume $0 \le k, m \le q-1$ when considering $G_q(k,m)$.

Lemma 2.1. (i) *Graphs $G_q(k,m)$ and $G_q(m,k)$ are isomorphic.*

(ii) *Graphs $G_q(f)$ (in particular, graphs $G_q(k,m)$) are q-regular. Moreover, a neighbor of any vertex is uniquely determined by the neighbor's first coordinate.*

(iii) *Let α, β be two bijections on F_q. Then graphs $G_q(\alpha, \beta, k, m)$ and $G_q(k,m)$ are isomorphic.*

Proof. (i) The map φ, defined by $\varphi((p_1, p_2)) = [p_1, p_2]$ and $\varphi([l_1, l_2]) = (l_1, l_2)$, is an isomorphism of $G_q(k,m)$ to $G_q(m,k)$.

(ii) For a fixed point (p), and for every $l_1 \in \mathbb{F}_q$, l_2 is uniquely determined from (1). Hence every neighbor $[l]$ of (p) is uniquely determined by its first coordinate l_1, and every point has exactly q neighbors. The argument for the the neighbors of a line is similar.

(iii) The map ψ, defined by $\psi((p_1, p_2)) = (\alpha^{-1}(p_1), p_2)$ and $\psi([l_1, l_2]) = [\beta^{-1}(l_1), l_2]$, is an isomorphism of $G_q(k,m)$ to $G_q(\alpha, \beta, k, m)$. ■

Lemma 2.2. *Vertices* $(a), [b], (c), [d]$ *are consecutive vertices of a* 4*-cycle in* $G_q(k,m)$ *if and only if*

$$a_1 \neq c_1,\ b_1 \neq d_1,\ \ \textit{and}\ \ (a_1^k - c_1^k)(b_1^m - d_1^m) = 0. \tag{2}$$

Proof. The first two inequalities ensure that all four vertices are distinct. The adjacency condition (1) in $G_q(k,m)$ implies:

$$(a) \sim [b] = [b_1, a_1^k b_1^m - a_2] \sim (c) = (c_1, c_1^k b_1^m - a_1^k b_1^m + a_2) \ \text{ and}$$

$$(a) \sim [d] = [d_1, a_1^k d_1^m - a_2] \sim (c) = (c_1, c_1^k d_1^m - a_1^k d_1^m + a_2).$$

Equating the second coordinates of point (c), we get $(a_1^k - c_1^k)(b_1^m - d_1^m) = 0$. Conversely, a solution (a_1, b_1, c_1, d_1) of (2) and an arbitrary a_2 determine a unique 4-cycle $(a)[b](c)[d](a)$. Moreover, any solution (a_1, b_1, c_1, d_1) of (2) determines precisely q 4-cycles $(a)[b](c)[d](a)$. ■

We are ready to prove Theorem 1.2.

Proof of Theorem 1.2. (a) Let K be a subgraph of $G_q(k,m)$ with the vertex set consisting of s points $(p_i) = (p_{i1}, p_{i2})$, $i = 1, \ldots, s$, and t lines $[l_u] = [l_{u1}, l_{u2}]$, $u = 1, \ldots, t$. Lemma 2.2 implies that $K \cong K_{s,t}$ if and only if for all i, j, u, v, $1 \leq i < j \leq s$, $1 \leq u < v \leq t$,

$$p_{i1} \neq p_{j1},\ l_{u1} \neq l_{v1} \ \text{ and } \ (p_{i1}^k - p_{j1}^k)(l_{u1}^m - l_{v1}^m) = 0. \tag{3}$$

From now on, let $\alpha = (p_{11}, \ldots, p_{s1}, l_{11}, \ldots, l_{t1})$ denote a solution of (3). Given α, there are precisely q subgraphs $K \cong K_{s,t}$, each uniquely determined by a choice of p_{12}. Let $N_{s,t}$ denote the number of all distinct ordered pairs $(\{p_{11}, \ldots, p_{s1}\}, \{l_{11}, \ldots, l_{t1}\})$ determined by all α. Since each copy of $K_{s,t}$ comes either with s points and t lines, or with t points and s lines, and $s \neq t$ by assumption,

$$I_G(s,t) = q(N_{s,t} + N_{t,s}).$$

Next, note that each solution of (3) belongs to at least one of the following two sets:

$$P_{s,t} = \{\alpha : p_{11}^k = p_{21}^k = \cdots = p_{s1}^k\} \ \text{ or } \ L_{s,t} = \{\alpha : l_{11}^m = l_{21}^m = \cdots = l_{t1}^m\}.$$

Indeed, if two p_{i1}^k (resp., l_{u1}^m) are distinct, then (3) implies that all l_{u1}^m (resp., p_{i1}^k) are equal. By the inclusion-exclusion formula, we have

$$N_{s,t} = |P_{s,t}| + |L_{s,t}| - |P_{s,t} \cap L_{s,t}|.$$

Let us determine $|P_{s,t}|$. For each $\alpha \in P_{s,t}$, $p_{i1} \neq 0$ for all $i = 1, \ldots, s$. Then $(p_{i1}/p_{11})^k = 1$, for all $i = 2, \ldots, s$. There are exactly $\bar{k}$ solutions of the equation $x^k = 1$ in $\mathbb{F}_q$ (see, e.g., [1]). Since all p_{i1} are distinct, then for each nonzero value of p_{11}, there are $\bar{k} - 1$ possible choices for p_{21}, $\bar{k} - 2$ ones for p_{31}, and so on. Hence we have $(q-1)(\bar{k}-1)(\bar{k}-2)\cdots(\bar{k}-(s-1))$ possible choices for the ordered sequence $(p_{11}, \ldots, p_{s1})$ and $\frac{1}{s!}(q-1)(\bar{k}-1)(\bar{k}-2)\cdots(\bar{k}-(s-1)) = J_{k,s}$ choices for the set $\{p_{11}, \ldots, p_{s1}\}$. With $\binom{q}{t}$ choices for $\{l_{11}, \ldots, l_{t1}\}$, we obtain $|P_{s,t}| = \binom{q}{t} J_{k,s}$. Similarly, $|L_{s,t}| = \binom{q}{s} J_{m,t}$.

Each $\alpha \in P_{s,t} \cap L_{s,t}$ is uniquely defined by a choice of sets $\{p_{11}, \ldots, p_{s1}\}$ and $\{l_{11}, \ldots, l_{t1}\}$. Therefore $|P_{s,t} \cap L_{s,t}| = J_{k,s} J_{m,t}$, and

$$I_G(s,t) = q(N_{s,t} + N_{t,s}) = q(|P_{s,t}| + |L_{s,t}| - |P_{s,t} \cap L_{s,t}| + |P_{t,s}| + |L_{t,s}| - |P_{t,s} \cap L_{t,s}|),$$

which yields the desired formula.

(b) If $s = t$, then

$$I_G(s,s) = qN_{s,s} = q(|P_{s,s}| + |L_{s,s}| - |P_{s,s} \cap L_{s,s}|) = q\left(\binom{q}{s}\left(J_{k,s} + J_{m,s}\right) - J_{k,s}J_{m,s}\right),$$

and the proof of the theorem is finished. ■

Example 1. Consider the graph $G = G_3(2,2)$ (see Fig. 1). Here $q = 3$, $k = \bar{k} = m = \bar{m} = 2$, hence, $J_{2,2} = 1$ and $J_{2,3} = 0$. By Theorem 1.2, $I_G(2,3) = 6$ and $I_G(2,2) = 15$.

If graphs G and G' are isomorphic, then $I_G(s,t) = I_{G'}(s,t)$ for all $s, t \geq 2$. We show that for monomial graphs the converse is true, that is, the graph invariants $I_G(s,t)$ completely characterize the isomorphism class.

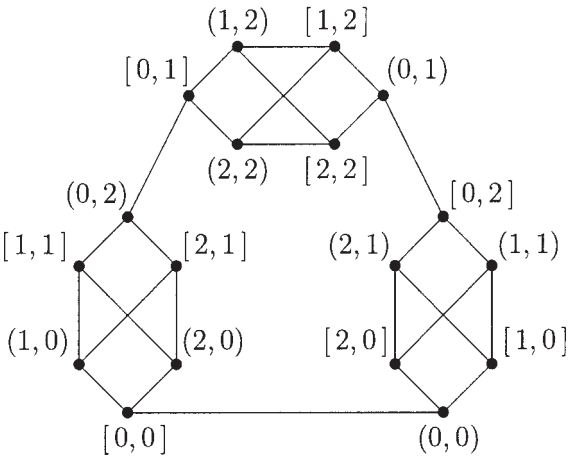

FIGURE 1. The graph $G_3(2,2)$.

We will need the following lemma from [8]. We include its short proof here for the convenience of the reader.

Lemma 2.3 ([8]). *Let a, b, and k be integers with $\gcd(a,k) = \gcd(b,k)$. Then there exists an integer x such that $ax \equiv b \bmod k$ and $\gcd(x,k) = 1$.*

Proof. Let $d = \gcd(a,k) = \gcd(b,k)$, and let $a' = a/d$, $b' = b/d$, $k' = k/d$. Note that x is a solution of $ax \equiv b \bmod k$ if and only if x is a solution of $a'x \equiv b' \bmod k'$. Since $\gcd(a',k') = 1$, the latter equation has a solution x_0, and all solutions are of the form $x_0 + k't$, $t \in \mathbb{Z}$. Moreover, $\gcd(x_0,k') = 1$, since x_0 is a unit in $\mathbb{Z}_{k'}$. Then by Dirichlet's Theorem (see [1]), in the arithmetic progression $\{x_0 + k't\}_{t\in\mathbb{Z}^+}$ there are infinitely many primes, in particular, for some $t_0 \in \mathbb{Z}^+$, $\gcd(x_0 + k't_0, k) = 1$. ∎

Proof of Theorem 1.1. Let $G = G_q(k,m)$ and $G' = G_{q'}(k',m')$. Suppose that $q = q'$ and $\{\bar{k}, \bar{m}\} = \{\bar{k}', \bar{m}'\}$ as multisets. By Lemma 2.1 (i), we may assume $\bar{k} = \bar{k}'$ and $\bar{m} = \bar{m}'$. By Lemma 2.3, there are u and v such that $ku \equiv k' \bmod q-1, mv \equiv m' \bmod q-1$, with $\bar{u} = 1$ and $\bar{v} = 1$. Then the maps $x \mapsto x^u$ and $x \mapsto x^v$ are bijections on $\mathbb{F}_q$, and the map $V(G') \to V(G)$, defined by $(p_1,p_2) \mapsto (p_1^u, p_2)$ and $[l_1,l_2] \mapsto [l_1^v, l_2]$, is a graph isomorphism by Lemma 2.1 (iii). Thus, $G_q(k,m) \cong G_q(ku,mv) = G_q(k',m')$ (all exponents are reduced modulo $q-1$).

Now let $G \cong G'$. By Lemma 2.1 (ii), G is q-regular and G' is q'-regular, therefore, $q = q'$. Without loss of generality, we may assume $\bar{k} \le \bar{m}$ and $\bar{k}' \le \bar{m}'$, since $G_q(k,m) \cong G_q(m,k)$ and $G_q(k',m') \cong G_q(m',k')$ by Lemma 2.1 (i).

Let $t = \max\{\bar{m}, \bar{m}'\} + 1$. Then $J_{k,t} = J_{m,t} = 0 = J_{k',t} = J_{m',t}$, and for any $s \ge 2$, $s \ne t$, the graph isomorphism implies

$$q\binom{q}{t}(J_{k,s} + J_{m,s}) = I_G(s,t) = I_{G'}(s,t) = q\binom{q}{t}(J_{k',s} + J_{m',s}). \tag{4}$$

Since $t \le q$, then $\binom{q}{t} \ne 0$, and we obtain

$$J_{k,s} + J_{m,s} = J_{k',s} + J_{m',s}. \tag{5}$$

Suppose that $\bar{k} < \bar{k}'$. Then $\bar{k}' \ge 2$. Set $s = \bar{k}'$. Then (5) implies $\bar{m}' < \bar{m}$. Since $\bar{k}' \le \bar{m}'$, we conclude that $\bar{k} < \bar{m}$. Then $\bar{m} \ge 2$. Setting $s = \bar{m}$ in (4), we get $I_G(\bar{m},t) = q\binom{q}{t} J_{m,\bar{m}} \ne 0$, whereas $I_{G'}(\bar{m},t) = 0$, a contradiction. Similarly if $\bar{k}' < \bar{k}$, then $\bar{m} < \bar{m}'$, and $I_G(\bar{m}',t) = 0 \ne I_{G'}(\bar{m}',t)$, a contradiction again.

Therefore $\bar{k} = \bar{k}'$, hence $J_{m,s} = J_{m',s}$. For $s = 2 < t$, we obtain $J_{m,2} = J_{m',2}$, and the latter implies $\bar{m} = \bar{m}'$. If $t = 2$, then $\bar{m} = \bar{m}' = 1$. Hence $\bar{k} = \bar{k}'$ implies $\bar{m} = \bar{m}'$. Thus, $\{\bar{k}, \bar{m}\} = \{\bar{k}', \bar{m}'\}$. ∎

A proof of Corollary 1.3 follows immediately from Lemma 2.1 (iii) and Theorem 1.1.

ACKNOWLEDGMENT

The authors are grateful to an anonymous referee for several useful suggestions.

REFERENCES

[1] K. Ireland and M. Rosen, A classical introduction to modern number theory, Second edition, Graduate texts in mathematics, vol. 84, Springer-Verlag, New York, 1990.

[2] J. -L. Kim, U. N. Peled, V. Pless, and I. Perepelitsa, Explicit construction of LDPC codes with girth at least six, to appear in Proceedings of the 40th Allerton Conference on Communication, Control and Computing, UIUC, Oct. 2002.

[3] F. Lazebnik and D. Mubayi, New lower bounds for Ramsey numbers of graphs and hypergraphs, Adv Appl Math 28 (3/4) (2002), 544–559.

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

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

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

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

[8] R. Viglione, Properties of some algebraically defined graphs, Ph.D. thesis, University of Delaware, 2002.