Automorphisms of Groups and Isomorphisms of Cayley Digraphs

Jixiang Meng
Department of Mathematics, Xinjiang University, Urumqi, Xinjiang 830046, P.R.China

Mingyao Xu
Institute of Mathematics, Beijing University, Beijing 100871, P.R.China

Abstract. Let G be a graph and S a subset of G not containing the identity element 1 of G. The Cayley digraph of G with respect to S, denoted $D(G,S)$, is a directed graph with vertex set G and for x and y in G, there is an arc from x to y if and only if $x^{-1}y \in S$. In this paper, we discuss the relationships between the isomorphisms of $D(G,S)$ and the automorphisms of G. The results are applied to studying the isomorphisms and automorphisms of hierarchical Cayley digraphs of abelian groups.

§1. Introduction

Let G be a finite group and S a subset of G with $1 \notin S$. The Cayley digraph $D = D(G,S)$ of G with respect to S is defined by

$$V(D) = G$$
$$E(D) = \{(g, gs) : g \in G, s \in S\}$$

For any $a \in G$, the left multiplication $\tau_a : x \mapsto ax$ is clearly an automorphism of any Cayley digraph of G, and all these left multiplications constitute the left regular representation group $L(G)$ of G, which is a subgroup of the automorphism group of any Cayley digraph of G. It is well known that $L(G)$ acts regularly on G. Thus Cayley digraphs are vertex transitive.

Throughout, G is a finite group and I the identity permutation on G, and I^- denotes the mapping: $x \longrightarrow x^{-1}$ $(x \in G)$. Set

$$ST(G,S) = \{\sigma \in Aut[D(G,S)] : \sigma(1) = 1\}$$
$$Aut(G,S) = \{\sigma \in AutG : \sigma(S) = S\}.$$

Then it is routine to check that $Aut(G,S) \subseteq ST(G,S)$. What we are concerned about is when $Aut(G,S) = ST(G,S)$. In section 2, we will give a necessary and sufficient condition for $Aut(G,S) = ST(G,S)$.

Let G be a group and $S \subseteq G \setminus \{1\}$. For any $\alpha \in Aut(G)$, set $T = \alpha(S)$. Then it is routine to check that $D(G,S) \overset{\alpha}{\cong} D(G,T)$. What about the converse? Formally stated, if $D(G,S) \cong D(G,T)$, when does there exist some $\alpha \in Aut(G)$

such that $T = \alpha(S)$? Adam [1] conjectured that this is true for Cayley digraphs of the finite cyclic groups, and Elspas and Turner disproved the conjecture in [6]. Inspired by these, many researchers devoted time to studying which groups have this property(see [3], [7] and [12]), or which subsets of a given group have this property(see [5] and [13]). In section 2, we will give a sufficient condition.

A set S of generators of a group G is said to be hierarchical if there exists an ordering of the elements in S, say $S = \{s_1, s_2, \cdots, s_k\}$ such that, for any $i = 1, 2, \cdots, k-1$, the group generated by $\{s_1, s_2, \cdots, s_i\}$ is a proper subgroup of the group generated by $\{s_1, s_2, \cdots, s_{i+1}\}$. The Cayley digraphs of a group with respect to hierarchical generating subsets of G are called hierarchical Cayley digraphs.

The study of hierarchical Cayley digraphs is important since many interconnection networks are modeled as hierarchical Cayley digraphs. For the results on hierarchical Cayley digraphs, see [2], [8] and [9] for references. In section 3, we study the isomorphisms and automorphisms of hierarchical Cayley digraphs of abelian groups. The results obtained here partially generalize those of [10] and [11].

§2. Main results

Let G be a finite group. Recall that $L(G) = \{\tau_a : a \in G\}$ is the left regular representation group of G, where τ_a is the left multiplication of G determined by a. Clearly, $\tau_a\tau_b = \tau_{ab}, \tau_1 = I$ and $\tau_{a^{-1}} = \tau_a^{-1}$.

Theorem 1. $ST(G,S) = Aut(G,S)$ if and only if $ST(G,S)$ is contained in the normalizer subgroup of the left regular representation group of G in $Aut[D(G,S)]$.

Proof: Set $A = Aut[D(G,S)]$. The proof of one way follows from the simple observation that $\sigma\tau_g\sigma^{-1} = \tau_{\sigma(g)}$ for all $g \in G$ and all $\sigma \in ST(G,S)$.

For the converse, suppose that $ST(G,S) \subseteq N_A(L(G))$, and we will prove that $ST(G,S) = Aut(G,S)$. It suffices to show that $ST(G,S) \subseteq Aut(G,S)$ since $Aut(G,S) \subseteq ST(G,S)$ holds for any G and S. Let $\sigma \in ST(G,S)$ and $g \in G$. Since $ST(G,S) \subseteq N_A(L(G))$, we may suppose that $\sigma\tau_g\sigma^{-1} = \tau_{g'}$, where $g' \in G$. Then $g' = \tau_{g'}(1) = \sigma\tau_g\sigma^{-1}(1) = \sigma(g)$. Thus $\sigma\tau_g\sigma^{-1} = \tau_{\sigma(g)}$ for any $g \in G$. Now, for any a and b in G, we have that $\sigma\tau_{ab}\sigma^{-1} = \tau_{\sigma(ab)}$. On the other hand, $\sigma\tau_{ab}\sigma^{-1} = \sigma\tau_a\tau_b\sigma^{-1} = \sigma\tau_a\sigma^{-1}\sigma\tau_b\sigma^{-1} = \tau_{\sigma(a)}\tau_{\sigma(b)} = \tau_{\sigma(a)\sigma(b)}$. Therefore, $\tau_{\sigma(ab)} = \tau_{\sigma(a)\sigma(b)}$, and so $\sigma(ab) = \sigma(a)\sigma(b)$. Thus $\sigma \in Aut(G)$. Since $\sigma(1) = 1$, we have that $\sigma(S) = S$, so $\sigma \in Aut(G,S)$. This completes the proof.

Theorem 2. If $ST(G,S)$ is the identity group, then for any isomorphism $D(G,S) \cong D(G,T)$ of Cayley digraphs of G, there exists some $\alpha \in Aut(G)$ such

that $T = \alpha(S)$.

Proof: Suppose that $D(G,S) \overset{\sigma}{\cong} D(G,T)$. Since Cayley digraphs are vertex transitive, we may assume that $\sigma(1) = 1$. We proceed to prove that $\sigma \in Aut(G)$. For any $a \in G$, $\sigma^{-1}\tau_{(\sigma(a))^{-1}}\sigma\tau_a$ is clearly an automorphism of $D(G,S)$. On the other hand, $\sigma^{-1}\tau_{(\sigma(a))^{-1}}\sigma\tau_a(1) = 1$. Thus $\sigma^{-1}\tau_{(\sigma(a))^{-1}}\sigma\tau_a \in ST(G,S)$, and so $\sigma^{-1}\tau_{(\sigma(a))^{-1}}\sigma\tau_a = I$. That is, $\sigma\tau_a = \tau_{\sigma(a)}\sigma$. Therefore, $\sigma(ab) = \sigma(a)\sigma(b)$ for any a and b in G, so $\sigma \in Aut(G)$. On the other hand, since $\sigma(1) = 1$, we have $\sigma(S) = T$. This completes our proof.

Babai and Frankl [13] proved that the stabilizer subgroup 1 in the automorphism groups of almost all Cayley digraphs for nilpotent groups with odd order is the identity group. This implies that Theorem 2 is applicable for 'almost all' Cayley digraphs of nilpotent groups of odd order.

Theorem 2 can not be strengthened in the sense that there exists a Cayley digraph $D(G,S)$ such that the stabilizer subgroup $ST(G,S)$ is a group of order 2, but it does not satisfies Adam's conjecture.

Example 1. $D(Z_8,\{1,2,5\}) \cong D(Z_8,\{3,2,7\})$, but there is no automorphism of Z_8 mapping $\{1,2,5\}$ into $\{3,2,7\}$ (see [2]). On the other hand, it is routine to check that $ST(Z_8,\{1,2,5\}) = \{I,\phi\}$ (here, the identity element is 0), where ϕ is defined by

$$x \mapsto 5x \ (x \in Z_8).$$

We note that, in the above example, ϕ is an automorphism of Z_8. The following Theorem 3 tells us that this is a particular case of a general result.

Theorem 3. If $ST(G,S) = \{I,\phi\}$, then $\phi \in Aut(G)$.

Proof: For any $a \in G$, consider the mapping $\tau^{-1}_{\phi(a)}\phi\tau_a$. Clearly, $\tau^{-1}_{\phi(a)}\phi\tau_a(1) = 1$. Thus $\tau^{-1}_{\phi(a)}\phi\tau_a \in ST(G,S)$. If $\tau^{-1}_{\phi(a)}\phi\tau_a = I$, then $\phi = \tau_{\phi(a)}\tau_a^{-1}$ and so $1 = \phi(1) = \tau_{\phi(a)}\tau_a^{-1}(1) = \phi(a)a^{-1}$. Now $I = \tau_1 = \tau_{\phi(a)a^{-1}} = \tau_{\phi(a)}\tau_{a^{-1}} = \tau_{\phi(a)}\tau_a^{-1} = \phi$, a contradiction. Thus $\tau^{-1}_{\phi(a)}\phi\tau_a = \phi$, and so $\phi(ab) = \phi(a)\phi(b)$. Thus, we have that $\phi \in Aut(G)$. This completes the proof.

If the isomorphism ϕ in Theorem 3 is I^-, then, since, $I^- \in Aut(G)$, G must be an abelian group. In this case, we have the following:

Theorem 4: If $ST(G,S) = \{I,I^-\}$ and G is abelian, then for any isomorphism $D(G,S) \cong D(G,T)$ of Cayley digraphs of G, there exists $\sigma \in Aut(G)$ such that $\sigma(S) = T$.

Proof. Let σ be any isomorphism from $D(G,S)$ to $D(G,T)$ with $\sigma(1) = 1$. Then for any $a \in G$, we know $\sigma^{-1}\tau^{-1}_{\sigma(a)}\sigma\tau_a \in ST(G,S)$, so $\sigma^{-1}\tau^{-1}_{\sigma(a)}\sigma\tau_a = I$ or I^-. Classify each element $a \in G$ as of type + or type − according to whether $\sigma^{-1}\tau^{-1}_{\sigma(a)}\sigma\tau_a = I$ or $\sigma^{-1}\tau^{-1}_{\sigma(a)}\sigma\tau_a = I^-$, and note that the identity element of G

is of type $+$. We now proceed to show that every element of G is of type $+$, by contradiction.

Assume G contains an element b of type $-$. Then $\sigma\tau_b = \tau_{\sigma(b)}\sigma I^-$ and so $\sigma(bx) = \sigma(b)\sigma(x^{-1})$ for every $x \in G$. Taking $x = b^{-1}$ gives $1 = \sigma(1) = \sigma(b)^2$, therefore $\sigma(b)$ has order 2, for every element b of type $-$.

On the other hand, if a is any element of G of type $+$, then $\sigma\tau_a = \tau_{\sigma(a)}\sigma$ and so $\sigma(ax) = \sigma(a)\sigma(x)$ for every $x \in G$. In particular, taking $x = a^{-1}$ gives $1 = \sigma(a)\sigma(a^{-1})$ and therefore $\sigma(a)^{-1} = \sigma(a^{-1})$. But instead if x is taken as any element b of type $-$, then $\sigma(ab) = \sigma(a)\sigma(b)$ while also $\sigma(ab) = \sigma(ba) = \sigma(b)\sigma(a^{-1})$, and thus $\sigma(a)^{-1} = \sigma(a^{-1}) = \sigma(a)$. Hence $\sigma(a)$ has order 1 or 2, for every element a of type $+$.

It follows that $\sigma(g)$ has order 1 or 2 for every $g \in G$, and therefore every element of G has order 1 or 2. In this case however, $I^- = I$, so we have no counter-example!

Thus $\sigma^{-1}\tau_{\sigma(a)}^{-1}\sigma\tau_a = I$ for all $a \in G$, and in particular, $\sigma(ax) = \sigma(a)\sigma(x)$ for all $a, x \in G$, showing $\sigma \in Aut(G)$.

§3. Isomorphisms of hierarchical Cayley digraphs

We first establish a lemma.

Lemma 1. Suppose that $D(G,S)$ is strongly connected and $D(G,S) \cong D(G,T)$. If for every isomorphism σ from $D(G,S)$ to $D(G,T)$ with $\sigma(1) = 1$, we have $\sigma(ab) = \sigma(a)\sigma(b)$ for all a and b in S, then $\sigma \in Aut(G)$ for all such σ.

Proof: For any a, b and g in G, we have

$$\begin{aligned}&\sigma(gab)\\ &= \sigma[\tau_g(ab)]\\ &= \tau_{\sigma(g)}\tau_{\sigma(g)}^{-1}\sigma\tau_g(ab).\end{aligned}$$

Since $\tau_{\sigma(g)}^{-1}\sigma\tau_g$ is an isomorphism from $D(G,S)$ to $D(G,T)$ satisfying $\tau_{\sigma(g)}^{-1}\sigma\tau_g(1) = 1$, we have

$$\begin{aligned}&\sigma(gab)\\ &= \tau_{\sigma(g)}\tau_{\sigma(g)}^{-1}\sigma\tau_g(a)\tau_{\sigma(g)}^{-1}\sigma\tau_g(b)\\ &= \sigma(ga)[\sigma(g)]^{-1}\sigma(gb).\end{aligned}$$

Since $D(G,S)$ is strongly connected, any element of G can be expressed in the form $\prod_{i=1}^m a_i$ $(a_i \in S)$. By applying induction on m and the above equality we can deduce that $\sigma(\prod_{i=1}^m a_i) = \prod_{i=1}^m \sigma(a_i)$. Thus $\sigma \in Aut(G)$.

In the following, we always suppose that G is a finite abelian group and $S = \{s_1, s_2, \ldots, s_k\}$ is a hierarchical generating subset of G, meaning that:

$$\langle s_1 \rangle \subset \langle s_1, s_2 \rangle \subset \cdots \subset \langle s_1, s_2, \cdots, s_k \rangle = G.$$

Let $D = D(G, S)$. Suppose that U is a subset of G. Set

$$N^+(U) = \{v \in G \setminus U : \exists u \in U \ s.t. \ (u, v) \in E(D)\}.$$

Theorem 5. Let G be an abelian group and $S = \{s_1, s_2, \cdots, s_k\}$ be a hierarchical generating subset of G such that $s_i^2 \neq s_j^2$ whenever $i \neq j$. Then, for any isomorphism $D(G, S) \overset{\phi}{\cong} D(G, T)$ with $\phi(1) = 1$, we have $\phi \in Aut(G)$.

Proof: We use Lemma 1 to prove the result. Proceeding to this, we make two observations:

Observation 1. For distinct i and j $(1 \leq i, j \leq k)$, we have $| N^+(s_i) \cap N^+(s_j) | \leq 2$.

In fact, let $s_j s_q \in N^+(s_i) \bigcap N^+(s_j)$. Then there exists some s_p in S such that $s_i s_p = s_j s_q$. Assume, without loss of generality that $i < j$. We prove that $q \in \{i, j\}$ as follows:

Let $m = max\{i, j, p, q\}$. As $s_i s_p = s_j s_q$ but $s_m \notin \langle s_1, s_2, \cdots, s_{m-1} \rangle$, we know m is equal to two of i, j, p, q. Clearly $p \neq q$ (since $i < j$), so either $m = j = p$ (in which case $q = i$) or $m = j = q$.

Observation 2. Every vertex $a \in N^+(S)$ is the common out-adjacency vertex of at most three vertices of S.

In fact, by the proof of Observation 1, we know that if $a = s_i s_p = s_j s_q$ and $i < j$, then $q = j$ or $q = i$. Thus a is the common out adjacency vertex of at most three vertices s_i, s_p and s_j.

Now we prove that $\phi(s_i s_j) = \phi(s_i)\phi(s_j)$ for any $s_i, s_j \in S$ by induction on $i + j$. First, s_1^2 is the out-adjacency of only one vertex s_1 in S. (Otherwise, suppose $s_1^2 \in N^+(s_p)$ with $p > 1$, then there exists some s_q in S such that $s_1^2 = s_p s_q$. By our condition, we have $p \neq q$ and if $p < q$, then $\langle s_1, s_2, \cdots, s_{q-1} \rangle = \langle s_1, s_2, \cdots, s_q \rangle$, a contradiction). Hence $\phi(s_1^2)$ must be the out-adjacency vertex of only one vertex $\phi(s_1)$ in T. Thus $\phi(s_1^2) = [\phi(s_1)]^2$.

Assume that the conclusion is already established for all s_i and s_j in S with $i+j \leq l$. Now we consider the case that $i+j = l+1$. Two cases are distinguished.

Case 1. $i = j$.

If s_i^2 is the out-adjacency vertex of only one vertex s_i in S, then, similarly to the above, we have that $\phi(s_i^2) = [\phi(s_i)]^2$. Otherwise, by the condition and Observation 2, we know that s_i^2 must be the common out-adjacency vertex of exactly three vertices, say s_i, s_{i_1}, s_{i_2} in S. Clearly $s_i^2 = s_{i_1}s_{i_2}$ and $max\{i_1, i_2\} < i$. Hence, $\phi(s_i^2)$ must be the common out-adjacency vertex of exactly three vertices $\phi(s_i)$, $\phi(s_{i_1})$ and $\phi(s_{i_2})$ in T. Assume that

$$\phi(s_i^2) = \phi(s_i)\phi(s_{j_1}) = \phi(s_{i_1})\phi(s_{j_2}) = \phi(s_{i_2})\phi(s_{j_3}).$$

Then $\{i, i_1, i_2\} = \{j_1, j_2, j_3\}$. By the induction hypothesis, $\phi(s_i^2) = \phi(s_{i_1}s_{i_2})$ $= \phi(s_{i_1})\phi(s_{i_2})$, so $j_2 = i_2$ and $j_3 = i_1$, and therefore $j_1 = i$, and $\phi(s_i^2)$ $= [\phi(s_i)]^2$.

Case 2. $i \neq j$.

Assume, without loss of generality that $i < j$. If s_is_j is the only common out-adjacency vertex of s_i and s_j, then $\phi(s_is_j)$ is the only common out-adjacency vertex of $\phi(s_i)$ and $\phi(s_j)$. Thus $\phi(s_is_j) = \phi(s_i)\phi(s_j)$. Otherwise, s_i and s_j have another common out-adjacency vertex, say u. Then, by Observation 1, we have that $N^+(s_i) \cap N^+(s_j) = \{s_is_j, u\}$, and so $\phi(s_i)\phi(s_j) \in N^+(\phi(s_i)) \cap N^+(\phi(s_j)) = \{\phi(s_is_j), \phi(u)\}$. Since u is a common out-adjacency vertex of s_i and s_j, we may suppose that $u = s_is_p = s_js_q$. Since S is a hierarchical generating subset of G and $i < j$, we have that $q = j$, and so $i \neq p$ and $p < j$. By the induction hypothesis, we have that $\phi(u) = \phi(s_i)\phi(s_p)$. Since $\phi(s_i)\phi(s_p) \neq \phi(s_i)\phi(s_j)$, we deduce that $\phi(s_is_j) = \phi(s_i)\phi(s_j)$.

Thus $\phi(s_is_j) = \phi(s_i)\phi(s_j)$ for any s_i and s_j in S. By lemma 1, we are done.

The following example shows that if the condition that $s_i^2 \neq s_j^2$ is not available, then the conclusion in Theorem 5 does not necessarily hold.

Example 2. Let $k \geq 2$ be an integer and $n = 2^k$. Let $G = Z_n \times Z_2$. Then $S = \{(2^{k-1}, 1), (0, 1), (1, 0)\}$ is a hierarchical generating subset of G. Let $T = \{(2^{k-2}, 1), (-2^{k-2}, 1), (1, 0)\}$. Then $D(G, S) \cong D(G, T)$. In fact, $G = \langle(1, 0)\rangle \cup (\langle(1, 0)\rangle + (2^{k-1}, 1)) = \langle(1, 0)\rangle \cup (\langle(1, 0)\rangle + (2^{k-2}, 1))$ and the mapping

$$i(1, 0) + j(2^{k-1}, 1) \mapsto i(1, 0) + j(2^{k-2}, 1)$$

is an isomorphism from $D(G, S)$ to $D(G, T)$. But there is no automorphism of G mapping S to T since T is not a hierarchical generating subset of G.

We give below some corollaries of Theorem 5.

Corollary 1. Under the conditions of Theorem 1, we have that

$$Aut[D(G, S)] = \sum_{g \in G} \tau_g Aut(G, S).$$

Corollary 2. If G is an abelian group of odd order and S a hierarchical generating subset of G, then $Aut[D(G, S)] = \sum_{g \in G} \tau_g Aut(G, S)$.

Corollary 3. Let $S = \{s_1, s_2, \cdots, s_k\}$ be a hierarchical generating subset of the cyclic group Z_n. If $s_i^2 \neq s_j^2$ whenever $i \neq j$, then $Aut[D(Z_n, S)] \cong Z_n$.

Proof: By Corollary 1, we have that $Aut[D(Z_n, S)] = \sum_{a \in Z_n} \tau_a Aut(Z_n, S)$. On the other hand, for any $\sigma \in Aut(Z_n, S)$, there exists some λ prime to n such that $x \overset{\sigma}{\mapsto} \lambda x$ $(x \in Z_n)$. Now, since $\sigma(S) = S$, we have $\lambda S \equiv S$ mod(n). If there exists some $i(1 \leq i \leq k)$ such that $\lambda s_i \not\equiv s_i$ mod(n), then S is not a hierarchical generating subset of Z_n, a contradiction. Thus $\lambda s_i \equiv s_i$ mod(n) for any i $(1 \leq i \leq k)$. Since S is a generating subset of Z_n, we have that $gcd(s_1, s_2, \cdots, s_k, n) = 1$. Thus, there exist some integers $x_1, x_2, \cdots, x_k$ such that $\sum_{i=1}^{k} x_i s_i \equiv 1$ mod(n). Hence, $\lambda \sum_{i=1}^{k} x_i s_i \equiv \sum_{i=1}^{k} x_i s_i$ mod(n). Thus $\lambda \equiv 1$ mod(n) and so $\sigma = I$. This completes the proof.

It is easy to show that $a^2 \neq b^2$ if a and b are two distinct elements in a minimal generating subset of a finite cyclic group (see [10]). We thus have the following:

Corollary 4. If S is a minimal generating subset of the cyclic group Z_n, then $Aut[D(Z_n, S)] \cong Z_n$.

Acknowledgement. The authors wish to express their deep gratitude to the referee for providing a stronger version of Theorem 4 and a nice proof of this theorem.

References

[1] A.Adam, Research problem 2–10, J.Comb.Theory, 2(1967), 393.

[2] S.B.Akers and B.Krishnamurthy, On group graphs and their fault tolerance, IEEE. Trans. Comput., 36(1987) 885–888.

[3] B.Alspach and T.D.Parsons, Isomorphism of circulant graphs and digraphs, Discrete Math., 254(1979), 97–108.

[4] L.Babai and C.D.Godsil, Automorphism groups of almost all Cayley graphs, European J. Combin., 3(1982), 9-15

[5] C.Delorme, O.Favaron and M.Maheo, Isomorphism of Cayley multigraphs of degree 4 on finite abelian groups, European J.Combin., 13(1992), 5–7.

[6] B.Elspas and J.Turner, Graphs with circulant adjacency matrices, J.Comb.Theory, 9(1970), 297–307.

[7] C.D.Godsil, On Cayley graph isomorphism, Ars Combinatoria, 15(1983), 231–246.

[8] C.D.Godsil, Connectivity of minimal Cayley graphs, Arch. Math., 37(1981), 473–476.

[9] Y.O.Hamidoune, A.S.Llado and O.Serra, The connectivity of hierarchical Cayley digraphs, Discrete Applied Math., 37/38 (1992), 275–280.

[10] Qiongxiang Huang and Jixiang Meng, Isomorphisms and automorphism groups of circulant graphs and digraphs, submitted.

[11] Jixiang Meng and Qiongxiang Huang, Isomorphisms of circulant digraphs, to appear.

[12] P.P.Palfy, Isomorphism problem for relational structures with a cyclic automorphism, European. J. Combin., 8(1987), 35–43.

[13] L.Sun, Isomorphisms of circulant graphs, Chinese Annals of Mathematics, 9A:5(1988), 567-574.

(Received 6/10/94; revised 17/5/95)