On Isomorphisms of Cayley Digraphs on Dihedral Groups

Haipeng Qu*

Department of Mathematics
Peking University
Beijing 100871
People's Republic of China

Jinsong Yu

Department of Mathematics
Washington University
St. Louis, MO 63130
U.S.A
E-mail: yujs@math.wustl.edu

Abstract

In this paper, we investigate m-DCI and m-CI properties of dihedral groups. We show that for any $m \in \{1, 2, 3\}$, the dihedral group D_{2k} is m-DCI if and only if D_{2k} is m-CI if and only if $2 \nmid k$.

§1. Preliminaries

Let G be a finite group and S a subset of G with $1 \notin S$. We use $\Gamma = \mathrm{Cay}(G; S)$ to denote the *Cayley digraph of G with respect to S*, defined to be the directed graph with vertex set and edge set given by

$$V(\Gamma) = G, \quad E(\Gamma) = \{(g, sg) \mid g \in G, \ s \in S\}.$$

When a digraph contains both undirected edges and directed edges, we refer to directed edges as *arcs* and undirected edges as *edges*.

Let D_{2k} be the dihedral group, $D_{2k} = \langle \alpha, \beta \mid \alpha^k = \beta^2 = 1, \ \beta\alpha\beta = \alpha^{-1} \rangle$. Whenever we refer to α and β in this paper, we mean the generators of the dihedral group D_{2k}.

*The work for this paper was supported by the National Natural Science Foundation of China and the Doctorial Program Foundation of Institutions of Higher Education (P. R. China).

We use $\mathrm{ord}(g)$ to denote the order of an element g in a group, use $|S|$ to denote the cardinal number of a set S, and use $\gcd(i,j)$ to denote the greatest common divisor of two integers i and j.

Let $\mathrm{Cay}(G;S)$ be the Cayley digraph of G with respect to S. Take $\pi \in \mathrm{Aut}(G)$ and set $S^\pi = T$. Obviously we have $\mathrm{Cay}(G;S) \cong \mathrm{Cay}(G;T)$. This kind of isomorphism between two Cayley digraphs is called a *Cayley isomorphism.*

DEFINITION 1.1 *Given a subset S of G, we call S a CI-subset of G, if for any subset T of G with $\mathrm{Cay}(G;S) \cong \mathrm{Cay}(G;T)$, there exists $\pi \in \mathrm{Aut}(G)$ such that $S^\pi = T$.*

DEFINITION 1.2 *A finite group G is called an m-DCI-group if any subset S of G with $1 \notin S$ and $|S| \leq m$ is a CI-subset. The group G is called an m-CI-group if any subset S of G with $1 \notin S$, $S^{-1} = S$ and $|S| \leq m$ is a CI-subset, where $S^{-1} = \{s^{-1} \mid s \in S\}$.*

A number of authors have investigated the m-DCI properties of abelian groups for $m \leq 3$, and m-CI properties of abelian groups for $m \leq 5$ (see [1–6]).

THEOREM 1.3 ([7, Theorem 2.5], or see [1–6])
1. *The finite cyclic group Z_k is m-DCI if $2 \nmid k$, $m = 1, 2, 3$.*
2. *Any finite cyclic group Z_k is 4-CI.*

DEFINITION 1.4 *A finite group G is called homogeneous if whenever H and K are two isomorphic subgroups and σ is an isomorphism $\sigma : H \to K$, then σ can be extended to an automorphism of G.*

The following lemmas are very easy to prove.

LEMMA 1.5 *If $\mathrm{Cay}(G;S) \cong \mathrm{Cay}(G;T)$, then $|\langle S \rangle| = |\langle T \rangle|$.*

LEMMA 1.6
1. *Any finite cyclic group Z_k is homogeneous.*
2. *For any finite cyclic group Z_k and for any $a, b \in Z_k$ with $\mathrm{ord}(a) = \mathrm{ord}(b)$, there exists an $\pi \in \mathrm{Aut}(Z_k)$ such that $a^\pi = b$.*

LEMMA 1.7 *For any $i \in Z$ set $\gamma = \alpha^i\beta$. Then $D_{2k} = \langle \alpha, \gamma \mid \alpha^k = \gamma^2 = 1,\ \gamma\alpha\gamma = \alpha^{-1} \rangle$.*

LEMMA 1.8 *Given $\pi \in \mathrm{Aut}(Z_k)$ and $x \in Z_k$. Define a mapping $\bar{\pi} : D_{2k} \to D_{2k}$ by*

$$\left(\alpha^i\beta^j\right)^{\bar{\pi}} = \alpha^{i^\pi}\left(\alpha^x\beta\right)^j, \quad \forall i,j \in Z.$$

Then $\bar{\pi} \in \mathrm{Aut}(D_{2k})$.

LEMMA 1.9 *The dihedral group D_{2k} is homogeneous if $2 \nmid k$.*

§2. On the 1-DCI and 2-DCI Properties of Dihedral Groups

THEOREM 2.1 *D_{2k} is 1-DCI if and only if $2 \nmid k$.*

PROOF. Assume $2|k$. Then $\mathrm{ord}(\alpha^{\frac{k}{2}}) = 2$. Thus

$$\mathrm{Cay}(D_{2k}; \alpha^{\frac{k}{2}}) \cong \mathrm{Cay}(D_{2k}; \beta).$$

Obviously this is not a Cayley isomorphism, so D_{2k} is not 1-DCI.

Conversely, assume $2 \nmid k$. Take $a, b \in D_{2k}$ such that $\mathrm{Cay}(D_{2k}; a) \cong \mathrm{Cay}(D_{2k}; b)$. By Lemma 1.5, we have $\mathrm{ord}(a) = \mathrm{ord}(b)$, thus $\langle a \rangle \cong \langle b \rangle$. By Lemma 1.9, there exists a Cayley isomorphism between $\mathrm{Cay}(D_{2k}; a)$ and $\mathrm{Cay}(D_{2k}; b)$. Hence D_{2k} is 1-DCI.

COROLLARY 2.2 *D_{2k} is 1-CI if and only if $2 \nmid k$.*

THEOREM 2.3 *D_{2k} is 2-DCI if and only if $2 \nmid k$.*

PROOF. If D_{2k} is 2-DCI, then it follows from Theorem 2.1 that $2 \nmid k$.

Assume that $2 \nmid k$. Take $S, T \subseteq D_{2k}$ such that $|S| = |T| = 2$ and $\mathrm{Cay}(D_{2k}; S) \cong \mathrm{Cay}(D_{2k}; T)$. We consider three cases.
Case 1. $S \subseteq \langle \alpha \rangle$. So $|\langle T \rangle| = |\langle S \rangle|$ is odd, and hence $T \subseteq \langle \alpha \rangle$. By Theorem 1.3, there exists an isomorphism $\sigma : \langle S \rangle \to \langle T \rangle$ such that $S^\sigma = T$. By Lemma 1.9, σ can be extended to an automorphism of D_{2k}.
Case 2. $|S \cap \langle \alpha \rangle| = 1$. So there are just one edge and one arc starting from each vertex of $\mathrm{Cay}(D_{2k}; S)$. Hence $|T \cap \langle \alpha \rangle| = 1$. By Lemma 1.7, we can assume that $S = \{\alpha^i, \beta\}$ and $T = \{\alpha^u, \beta\}$. Since $|\langle S \rangle| = |\langle T \rangle|$ we have $\mathrm{ord}(\alpha^i) = \mathrm{ord}(\alpha^u)$. The conclusion follows from Lemma 1.6 and Lemma 1.8.
Case 3. $S \subseteq \langle \alpha \rangle \beta$. From the analysis above, we immediately get $T \subseteq \langle \alpha \rangle \beta$. Assume that $S = \{\alpha^i \beta, \beta\}$ and $T = \{\alpha^u \beta, \beta\}$. Since $|\langle S \rangle| = |\langle T \rangle|$ we have that $\gcd(k, i) = \gcd(k, u)$. By Lemma 1.6, there exists $\pi \in \mathrm{Aut}(Z_k)$ such that $i^\pi = u$. So

$$\bar{\pi} : \alpha^m \beta^n \mapsto \alpha^{m^\pi} \beta^n, \ \forall m, n \in Z$$

is an automorphism of D_{2k}, and $S^{\bar{\pi}} = T$.

COROLLARY 2.4 *D_{2k} is 2-CI if and only if $2 \nmid k$.*

§3. On the 3-DCI Property of Dihedral Groups

LEMMA 3.1 *Let k be an odd positive integer. Let S and T be subsets of Z_k of the form $S = \{\pm i, \pm j, \pm(i - j)\}$, $T = \{\pm u, \pm v, \pm(u - v)\}$ where $|S| = |T| = 6$. If $\mathrm{Cay}(Z_k; S) \cong \mathrm{Cay}(Z_k; T)$, then there is an automorphism $\pi \in \mathrm{Aut}(Z_k)$ such that $S^\pi = T$.*

PROOF. All graphs we use here are undirected. So in this proof we will use (x, y) to denote an undirected edge rather than a directed arc in a graph. Put $X = \mathrm{Cay}(Z_k; S)$

and $X' = \mathrm{Cay}(Z_k; T)$. For a vertex x of X, we use $X_1(x)$ to denote the induced subdigraph of the neighborhood of x in X, so

$$V(X_1(x)) = \{y \in V(X) \mid (x, y) \in E(X)\},$$

$$E(X_1(x)) = \{(y, z) \mid y, z \in V(X_1(x)),\ (y, z) \in E(X)\}.$$

The same definition applies to X'. By Lemma 1.5, we have $|\langle S\rangle| = |\langle T\rangle|$. It suffices to show that the statement is true for the case $\langle S\rangle = \langle T\rangle = Z_k$. (If $\langle S\rangle \neq Z_k$, we still have $\mathrm{Cay}(\langle S\rangle; S) \cong \mathrm{Cay}(\langle T\rangle; T)$. Using the proof below, we can get an isomorphism $\pi_1 : \langle S\rangle \to \langle T\rangle$ with $S^{\pi_1} = T$. Then Lemma 1.6 applies and π_1 can be extended to an automorphism of Z_k.)

Write

$$E_1 = \{(i, i-j), (-i, -i+j), (j, -i+j), (-j, i-j), (i, j), (-i, -j)\}.$$

Then $E_1 \subseteq E(X_1(0))$, and therefore $|E(X_1(0))| \geq 6$. We consider three cases.

Case 1. $|E(X_1(0))| \geq 8$. Write

$$E_2 = \{(i, -i+j), (-i, i-j), (j, i-j), (-j, -i+j), (i, -j), (-i, j)\},$$

and

$$E_3 = \{(i, -i), (j, -j), (i-j, -i+j)\}.$$

If $E_2 \cap E(X_1(0)) = \emptyset$, then $|E_3 \cap E(X_1(0))| \geq 2$. Without loss of generality, we can assume that $(i, -i), (j, -j) \in E(X_1(0))$, and thus $2i, 2j \in S$. We deduce that $2i = -i$, since $3i = 0$ from $i, j, i-j \neq 0$ and $E_2 \cap E(X_1(0)) = \emptyset$. Similarly we have $3j = 0$. Hence $i = \pm j$. This contradicts the fact that $|S| = 6$. Hence it follows that $E_2 \cap E(X_1(0)) \neq \emptyset$, and without loss of generality we can assume that $(i, -j) \in E(X_1(0))$, and thus $-i-j \in S$. Hence $-i-j \in \{i, j\}$ since $i, j \neq 0$. So we have $-j = 2i$ or $-i = 2j$. Therefore, $S = \{\pm s, \pm 2s, \pm 3s\}$ where s is some integer. Similarly, it follows that $T = \{\pm t, \pm 2t, \pm 3t\}$ for some integer t because $|E(X'_1(0))| = |E(X_1(0))| \geq 8$. Since $\langle s\rangle = \langle t\rangle = Z_k$, the mapping $\pi : s \mapsto t$ can be extended to an automorphism of Z_k.

Case 2. $|E(X_1(0))| = 6$. Assume $\sigma : X \to X'$ is a graph isomorphism. We can assume that $0^\sigma = 0$ since X' is vertex-transitive. Therefore $S^\sigma = T$. By the symmetry of S and T, we can also assume that $i^\sigma = u$. It is easy to see that $X_1(0)$ is a cycle, and i is adjacent to $i-j$ and j. Similarly, $X'_1(0)$ is also a cycle and u is adjacent to $u-v$ and v. Hence $\{i-j, j\}^\sigma = \{u-v, v\}$. Again we can assume that $j^\sigma = v$, and therefore $(i-j)^\sigma = u-v$, $(-j)^\sigma = -v$, $(-i)^\sigma = -u$, $(-i+j)^\sigma = -u+v$. It is easy to show that $V(X_1(i)) \cap V(X_1(j)) = \{0, j, i \pm j, 2i, 2i-j\} \cap \{0, i, \pm i + j, 2j, 2j - i\} = \{0, i+j\}$ and $V(X'_1(u)) \cap V(X'_1(v)) = \{0, u+v\}$. Since $X_1(i)^\sigma = X'_1(u)$ and $X_1(j)^\sigma = X'_1(v)$, we have that $(i+j)^\sigma = u+v$. Similarly we can show that $(2i-j)^\sigma = 2u-v$, $(-i-j)^\sigma = -u-v$, $(-2i+j)^\sigma = -2u+v$, $(i-2j)^\sigma = u-2v$, $(-i+2j)^\sigma = -u+2v$. Now consider $X_1(i)$ again. Since $X_1(i)^\sigma = X'_1(u)$ and $\{0, j, i \pm j, 2i-j\}^\sigma = \{0, v, u \pm v, 2u-v\}$, we have $(2i)^\sigma = 2u$. Similarly, $(-2i)^\sigma = -2u$, $(2j)^\sigma = 2v$, $(-2j)^\sigma = -2v$. So we have that $(mi+nj)^\sigma = mu+nv$, where m, n are integers and $|m| + |n| \leq 2$. By the transitivity of X, it follows that if $x, y \in D_{2k}$ are such that $x^\sigma = y$, $(x+i)^\sigma = y + u$, $(x+j)^\sigma = y + v$, then $(x + mi + nj)^\sigma = y + mu + nv$ where $|m| + |n| \leq 2$. By induction on $|m| + |n|$, it follows that $(mi + nj)^\sigma = mu + nv$, $\forall m, n \in Z$. Thus $\sigma : Z_k \to Z_k$ is a group isomorphism.

Case 3. $|E(X_1(0))| = 7$. Then $|E(X_1(0)) \setminus E_1| = 1$. It is easy to show that $E(X_1(0)) \setminus E_1 \subseteq \{(i, -i), (j, -j), (i - j, j - i)\}$ (otherwise $|E(X_1(0))| > 7$). We can assume that $(i, -i) \in E(X_1(0))$. By the analysis in case 1, we have $3i = 0$. We can also assume that $(u, -u) \in E(X_1'(0))$. So $\pm i, \pm u$ are the only vertices of valency 3 in $X_1(0)$ and $X_1'(0)$. Assume the graph isomorphism $\sigma : X \to X'$ is such that $0^\sigma = 0$. Then $\{\pm i\}^\sigma = \{\pm u\}$. By the same argument as in case 2, we can complete the proof.

DEFINITION 3.2 *Given a digraph Γ, we define the Step-2-digraph of Γ, denoted by $X = ST(\Gamma)$, by $V(X) = V(\Gamma)$, $E(X) = \{(x, y) \mid x, y \in V(\Gamma), x \neq y, \exists z \in V(\Gamma)$ such that $(x, z), (z, y) \in E(\Gamma)\}$.*
Thus $x, y \in V(\Gamma)$ are adjacent in $ST(\Gamma)$ if and only if there is a path of length 2 connecting them in Γ.

LEMMA 3.3 *Let $\mathrm{Cay}(G; S)$ be the Cayley digraph of G with respect to S. Then $ST(\mathrm{Cay}(G; S)) = \mathrm{Cay}(G; S^2 \setminus \{1\})$ where $S^2 = \{s_1 s_2 \mid s_1, s_2 \in S\}$.*

LEMMA 3.4 *Let Γ_1 and Γ_2 be digraphs and let $\sigma : \Gamma_1 \to \Gamma_2$ be an isomorphism. Then*

$$\overline{\sigma} : ST(\Gamma_1) \to ST(\Gamma_2), \quad x \mapsto x^\sigma, \quad \forall x \in V(ST(\Gamma_1)) = V(\Gamma_1)$$

is an isomorphism.

THEOREM 3.5 *D_{2k} is 3-DCI if and only if $2 \nmid k$.*

PROOF If D_{2k} is 3-DCI, then $2 \nmid k$ by Theorem 2.1.
Suppose $2 \nmid k$. It is sufficient to show that any subset S of D_{2k} with $|S| = 3$ is a CI-subset. Take $S, T \subseteq D_{2k}$ such that $|S| = |T| = 3$ and $\mathrm{Cay}(D_{2k}; S) \cong \mathrm{Cay}(D_{2k}; T)$. We consider five cases.

Case 1. $S \subseteq \langle \alpha \rangle$. The proof is the same as the first case in Theorem 2.3.
Case 2. $|S \cap \langle \alpha \rangle| = 2$ and $\mathrm{Cay}(D_{2k}; S)$ is an undirected graph. So we can assume that $S = \{\alpha^{\pm i}, \beta\}$. It is easy to see that $|T \cap \langle \alpha \rangle| = 2$ or $T \subseteq \langle \alpha \rangle \beta$. If $T \subseteq \langle \alpha \rangle \beta$ then $\mathrm{Cay}(D_{2k}; T)$ must be a bipartite graph. But $\mathrm{Cay}(D_{2k}; S)$ is not bipartite since it contains a circuit of odd length. So we can assert that $|T \cap \langle \alpha \rangle| = 2$. Assume that $T = \{\alpha^{\pm u}, \beta\}$. We have $\mathrm{ord}(\alpha^i) = \mathrm{ord}(\alpha^u)$ from $|\langle S \rangle| = |\langle T \rangle|$. By Lemma 1.6, there exists $\pi \in \mathrm{Aut}(Z_k)$ such that $i^\pi = u$. By Lemma 1.8, we know that π can be extended to an automorphism $\overline{\pi}$ of D_{2k} with $S^{\overline{\pi}} = T$.
Case 3. $|S \cap \langle \alpha \rangle| = 2$ and $\mathrm{Cay}(D_{2k}; S)$ is not an undirected graph. So we can assume that $S = \{\alpha^i, \alpha^j, \beta\}$ where $i + j \not\equiv 0 \pmod{k}$. There are just one edge and two arcs starting from each vertex of $\mathrm{Cay}(D_{2k}; S)$. So we can assert that $|T \cap \langle \alpha \rangle| = 2$. Assume that $T = \{\alpha^u, \alpha^v, \beta\}$. If we delete all edges from $\mathrm{Cay}(D_{2k}; S)$ and $\mathrm{Cay}(D_{2k}; T)$, the two digraphs we get are again isomorphic, namely, $\mathrm{Cay}(D_{2k}; \alpha^i, \alpha^j) \cong \mathrm{Cay}(D_{2k}; \alpha^u, \alpha^v)$. Hence $\mathrm{Cay}(\langle \alpha \rangle; \alpha^i, \alpha^j) \cong \mathrm{Cay}(\langle \alpha \rangle; \alpha^u, \alpha^v)$. By

Theorem 1.3 and Lemma 1.8, it follows that there is an automorphism $\bar{\pi} \in \mathrm{Aut}(D_{2k})$ such that $S^{\bar{\pi}} = T$.

Case 4. $|S \cap \langle\alpha\rangle| = 1$. So there are exactly two edges and one arc starting from each vertex of $\mathrm{Cay}(D_{2k}; S)$. Hence $|T \cap \langle\alpha\rangle| = 1$. By Lemma 1.5, we have $|\langle S\rangle| = |\langle T\rangle|$. It suffices to show that the statement is true for the case $\langle S\rangle = \langle T\rangle = D_{2k}$. (If $\langle S\rangle \neq D_{2k}$, we still have $\mathrm{Cay}(\langle S\rangle; S) \cong \mathrm{Cay}(\langle T\rangle; T)$. Using the proof below, we can get an isomorphism $\pi_1 : \langle S\rangle \to \langle T\rangle$ with $S^{\pi_1} = T$. Then Lemma 1.9 applies and π_1 can be extended to an automorphism of D_{2k}.)

Suppose that $\sigma : \mathrm{Cay}(D_{2k}; S) \to \mathrm{Cay}(D_{2k}; T)$ is an isomorphism. Since Cayley digraphs are vertex-transitive, we can assume $1^\sigma = 1$. In $\mathrm{Cay}(D_{2k}; S)$ we have that $\{x \in D_{2k} \mid \text{any path from 1 to } x \text{ contains even number of edges}\} = \langle\alpha\rangle$. And $\mathrm{Cay}(D_{2k}; T)$ has the same property. Hence $\langle\alpha\rangle^\sigma = \langle\alpha\rangle$. By Lemma 3.4, we know that σ induces an isomorphism $\bar{\sigma} : ST(\mathrm{Cay}(D_{2k}; S)) \to ST(\mathrm{Cay}(D_{2k}; T))$. Assume $S = \{\beta, \alpha^j\beta, \alpha^i\}$ and $T = \{\beta, \alpha^v\beta, \alpha^u\}$. By Lemma 3.3, we have

$$ST(\mathrm{Cay}(D_{2k}; S)) = \mathrm{Cay}\left(D_{2k}; \alpha^{2i}, \alpha^{\pm j}, \alpha^{\pm i}\beta, \alpha^{j\pm i}\beta\right),$$

and

$$ST(\mathrm{Cay}(D_{2k}; T)) = \mathrm{Cay}\left(D_{2k}; \alpha^{2u}, \alpha^{\pm v}, \alpha^{\pm u}\beta, \alpha^{v\pm u}\beta\right).$$

Because $\langle\alpha\rangle^\sigma = \langle\alpha\rangle$ and the subdigraph of $ST(\mathrm{Cay}(D_{2k}; S))$ spanned by $\langle\alpha\rangle$ is $\mathrm{Cay}\left(\langle\alpha\rangle; \alpha^{2i}, \alpha^{\pm j}\right)$, we have that $\mathrm{Cay}\left(\langle\alpha\rangle; \alpha^{2i}, \alpha^{\pm j}\right) \cong \mathrm{Cay}\left(\langle\alpha\rangle; \alpha^{2u}, \alpha^{\pm v}\right)$. By Theorem 1.3, there is an automorphism $\pi \in \mathrm{Aut}(Z_k)$ such that $\{2i, \pm j\}^\pi = \{2u, \pm v\}$. Hence $\{\pm j\}^\pi = \{\pm v\}$ and $\{2i\}^\pi = \{2u\}$. Since $2 \nmid k$, we have $i^\pi = u$. Now if $j^\pi = v$, by Lemma 1.8, there exists $\bar{\pi} \in \mathrm{Aut}(D_{2k})$ such that

$$\beta^{\bar{\pi}} = \beta,\ (\alpha^m)^{\bar{\pi}} = \alpha^{m^\pi},\ \forall m \in Z.$$

So $S^{\bar{\pi}} = T$. If $j^\pi = -v$, by Lemma 1.7, consider $\gamma = \alpha^v\beta$. Since $\beta = \alpha^{-v}\gamma$, it is the same as when $j^\pi = v$.

Case 5. $S \subseteq \langle\alpha\rangle\beta$. By the analysis above, we immediately get $T \subseteq \langle\alpha\rangle\beta$. Assume $S = \{\beta, \alpha^i\beta, \alpha^j\beta\}$ and $T = \{\beta, \alpha^u\beta, \alpha^v\beta\}$. Write

$$S_2 = \left\{\alpha^{\pm i}, \alpha^{\pm j}, \alpha^{\pm(i-j)}\right\},\ T_2 = \left\{\alpha^{\pm u}, \alpha^{\pm v}, \alpha^{\pm(u-v)}\right\}.$$

By Lemma 3.3, we have

$$ST(\mathrm{Cay}(D_{2k}; S)) = \mathrm{Cay}(D_{2k}; S_2),$$

and

$$ST(\mathrm{Cay}(D_{2k}; T)) = \mathrm{Cay}(D_{2k}; T_2).$$

By Lemma 3.4, we have

$$\mathrm{Cay}(D_{2k}; S_2) \cong \mathrm{Cay}(D_{2k}; T_2).$$

Hence

$$\mathrm{Cay}(\langle\alpha\rangle; S_2) \cong \mathrm{Cay}(\langle\alpha\rangle; T_2).$$

Notice that $|S_2| = |T_2| = 2, 4$ or 6. If $|S_2| = |T_2| = 2$ or 4, by Theorem 1.3, $\langle\alpha\rangle$ is 2-CI and 4-CI, and thus there exists $\pi \in \mathrm{Aut}(\langle\alpha\rangle)$ such that ${S_2}^\pi = T_2$. So the conclusion is immediate. Now let us consider the case for $|S_2| = |T_2| = 6$. By Lemma 3.1, there exists $\pi \in \mathrm{Aut}(Z_k)$ such that $\{\pm i, \pm j, \pm(i-j)\}^\pi = \{\pm u, \pm v, \pm(u-v)\}$. Without loss of generality, we can assume that $i^\pi = u$, and hence $(-i)^\pi = -u$.
If $j^\pi = -v$, then $u + v = (i-j)^\pi \in \{\pm(u-v)\}$, and therefore $u = 0$ or $v = 0$. This contradicts the fact that $|T| = 3$.
If $j^\pi = -(u-v)$ we can get the same contradiction as above.
If $j^\pi = v$ then $(i+j)^\pi = u + v$. By Lemma 1.8, there exists $\bar{\pi} \in \mathrm{Aut}(D_{2k})$ such that

$$\beta^{\bar{\pi}} = \beta, \quad (\alpha^m)^{\bar{\pi}} = \alpha^{m^\pi}, \quad \forall m \in Z.$$

So $S^{\bar{\pi}} = T$.
If $j^\pi = (u-v)$, then $(i-j)^\pi = v$. By Lemma 1.8, there exists $\bar{\pi} \in \mathrm{Aut}(D_{2k})$ such that

$$\beta^{\bar{\pi}} = \alpha^u\beta, \quad (\alpha^m)^{\bar{\pi}} = \alpha^{-(m^\pi)}, \quad \forall m \in Z.$$

So $S^{\bar{\pi}} = T$.
The proof is completed by the analysis above.

COROLLARY 3.7 *D_{2k} is 3-CI if and only if $2 \nmid k$.*

Acknowledgment

Professor Ming-Yao Xu introduced us to this field. We are grateful for his encouragement and help. We thank the referee and the editor for very helpful suggestions.

References

[1] Xin-Gui Fang, A characterization of finite abelian 2-DCI-groups *(Chinese), J. of Math. (Wuhan)* **8** (1988), 315–317.

[2] Xin-Gui Fang, Abelian 3-DCI-groups of even order, *Ars Combinatoria* **32** (1991), 263–267.

[3] Xin-Gui Fang and Min Wang, Isomorphisms of Cayley graphs of valency m(≤ 5) for a finite commutative group *(Chinese), Chinese Ann. Math. Ser.A* **13** (1992), suppl.7–14.

[4] Xin-Gui Fang and Ming-Yao Xu, Abelian 3-DCI-groups of odd order, *Ars Combinatoria* **28** (1989), 247–251.

[5] Xin-Gui Fang and Ming-Yao Xu, On isomorphisms of Cayley graphs of small valency, *Algebra Colloq.* **1** (1994), 67–76.

[6] Cai Heng Li, Finite Abelian groups with the m-DCI property, *Ars Combinatoria* (summitted for publication.)

[7] Mingyao Xu, Some work on vertex-transitive graphs by Chinese mathematicians, in *Group Theory in China*, Science Press/Kluwer Academic Publishers, Beijing/New York, 1996; pp.224–254.

(Received 24/6/96)