The Cayley isomorphism property for groups of order $p^3q$

Gábor Somlai
Department of Algebra and Number Theory
Eötvös Loránd University
1117 Budapest, Pázmány Péter sétány 1/C, Hungary
e-mail: gsomlai@cs.elte.hu

Abstract

For every prime $p > 3$ and for every prime $q > p^3$ we prove that $\mathbb{Z}_q \times \mathbb{Z}_p^3$ is a DCI-group.

1 Introduction

Let $G$ be a finite group and $S$ a subset of $G$. The Cayley graph $\text{Cay}(G, S)$ is defined by having the vertex set $G$ and $g$ is adjacent to $h$ if and only if $gh^{-1} \in S$. The set $S$ is called the connection set of the Cayley graph $\text{Cay}(G, S)$. A Cayley graph $\text{Cay}(G, S)$ is undirected if and only if $S = S^{-1}$, where $S^{-1} = \{ s^{-1} \in G \mid s \in S \}$. Every right multiplication via elements of $G$ is an automorphism of $\text{Cay}(G, S)$, so the automorphism group of every Cayley graph on $G$ contains a regular subgroup isomorphic to $G$. Moreover, this property characterises the Cayley graphs of $G$.

It is clear that automorphism $\mu$ of the group $G$ induces an isomorphism between $\text{Cay}(G, S)$ and $\text{Cay}(G, S^\mu)$. Such an isomorphism is called a Cayley isomorphism. A Cayley graph $\text{Cay}(G, S)$ is said to be a CI-graph if, for each $T \subset G$, the Cayley graphs $\text{Cay}(G, S)$ and $\text{Cay}(G, T)$ are isomorphic if and only if there is an automorphism $\mu$ of $G$ such that $S^\mu = T$. Furthermore, a group $G$ is called a DCI-group if every Cayley graph of $G$ is a CI-graph and it is called a CI-group if every undirected Cayley graph of $G$ is a CI-graph.

The problem of investigating the isomorphism problem of Cayley graphs started with Ádám’s conjecture [1], which states that every circulant graph is a CI-graph. Using our terminology, it was conjectured that every cyclic group is a DCI-group. This conjecture was first disproved by Elspas and Turner [8] for directed Cayley graphs of $\mathbb{Z}_8$ and for undirected graphs of Cayley graphs of $\mathbb{Z}_{16}$.

*Research supported by the Hungarian Scientific Fund (OTKA), grant no. K84233
By investigating the spectrum of circulant graph Elspas and Turner [8], and independently Djoković [6] proved that every cyclic group of order \( p \) is a CI-group if \( p \) is a prime. Also a lot of research was devoted to the investigation of circulant graphs. One of the most important results for our investigation is that \( Z_{pq} \) is a DCI-group for every pair of primes \( p < q \). This result was first proved by Alspach and Parsons [2] and later by Pöschel and Klin [11] using Schur rings, and by Godsil [9]. Finally, Muzychuk [14, 15] proved that a cyclic group \( Z_n \) is a DCI-group if and only if \( n = k \) or \( n = 2k \), where \( k \) is square-free. Furthermore, \( Z_n \) is a CI-group if and only if \( n \) is as above or \( n = 8, 9, 18 \).

It is easy to see that every subgroup of a (D)CI-group is also a (D)CI-group so it is natural to investigate \( p \)-groups which are the Sylow \( p \)-subgroups of a finite group. Babai and Frankl [5] proved that if \( G \) is a \( p \)-group, which is a CI-group, then \( G \) can only be elementary abelian \( p \)-group, the quaternion group of order 8 or one of a few cyclic groups \( Z_4, Z_9, Z_9 \) or \( Z_{27} \). Muzychuk’s result about cyclic groups shows that \( Z_{27} \) is not a CI-group and \( Z_9 \) is not a DCI-group. They also asked whether every elementary abelian \( p \)-group is a CI-group.

The cyclic group of order \( p \), which is a CI-group, can also be considered as an elementary abelian \( p \)-group of rank 1. The best general result was given by Hirasaka and Muzychuk [10] who proved that \( Z_p^3 \) is a CI-group for every prime \( p \).

For our investigation the following weaker results are also important. Dobson [7] proved that \( Z_p^3 \) is a CI-group for every prime \( p \) and Alspach and Nowitz shoved [3] that \( Z_p^3 \) is a CI-group with respect to Cayley color digraphs. However Muzychuk [16] showed that an elementary abelian \( p \)-group of rank \( 2p - 1 + (2p - 1)^p \) is not a CI-group.

Severe restriction on the structure of CI-groups was given by Li and Praeger and then a more precise list of candidates for CI-groups was given by Li, Lu and Pálfy [13].

New family of CI-groups was found by Kovács and Muzychuk [12], that is, \( Z_{p^2} \times Z_q \) is a CI-group for every prime \( p \) and \( q \). It was also conjectured in [12], that the direct product of CI-groups of coprime order is a CI-group.

**Theorem 1.** For every prime \( p \) and every prime \( q > p^3 \) the group \( Z_{p^3} \times Z_q \) is a DCI-group.

Our paper is organized as follows. In Section 2 we introduce the notation that will be used throughout this paper. In Section 3 we collect important ideas that we will use in the proof of Theorem 4. Finally, Section 4 contains the proof of Theorem 4.

## 2 Technical details

In this section we introduce some notation. Let \( G \) be a group. We use \( H \unlhd G \) to denote that \( H \) is a subgroup of \( G \) and by \( N_G(H) \) and \( C_G(H) \) we denote the normalizer and the centralizer of \( H \) in \( G \), respectively. The center of a group \( G \) will be denoted by \( Z(G) \).
Let us assume that the group $H$ acts on the set $\Omega$ and let $G$ be an arbitrary group. Then by $G \wr H$ we denote the wreath product of $G$ and $H$. Every element $g \in G \wr H$ can be uniquely written as $hk$, where $k \in K = G^\Omega$ and $h \in H$. The group $K = G^\Omega$ is called the base group of $G \wr H$ and the elements of $K$ can be treated as functions from $\Omega$ to $G$. If $g \in G \wr H$ and $g = hk$ we denote $k$ by $(g)_b$. In order to simplify the notation $\Omega$ will be omitted if it is clear from the definition of $H$ and we will write $G \wr H$.

The symmetric group on the set $\Omega$ will be denoted by $\text{Sym}(\Omega)$. Let $G$ be a permutation group on the set $\Omega$. For a $G$-invariant partition $B$ of the set $\Omega$ we use $G^B$ to denote the permutation group on $B$ induced by the action of $G$ and similarly, for every $g \in G$ we denote by $g^B$ the action of $g$ on the partition $B$.

For a group $G$, let $\hat{G}$ denote the subgroup of the symmetric group $\text{Sym}(G)$ formed by the elements of $G$ acting by right multiplication on $G$. For every Cayley graph $\Gamma = \text{Cay}(G, S)$ the subgroup $\hat{G}$ of $\text{Sym}(G)$ is contained in $\text{Aut}(\Gamma)$.

**Definition 1.** Let $G \leq \text{Sym}(\Omega)$ be a permutation group. Let

$$G^{(2)} = \left\{ \pi \in \text{Sym}(\Omega) \mid \exists a, b \in \Omega \ \exists g_{a,b} \in G \text{ with } \pi(a) = g_{a,b}(a) \text{ and } \pi(b) = g_{a,b}(b) \right\}.$$  

We say that $G^{(2)}$ is the 2-closure of the permutation group $G$.

**Lemma 1.** Let $\Gamma$ be a graph. If $G \leq \text{Aut}(\Gamma)$, then $G^{(2)} \leq \text{Aut}(\Gamma)$.

### 3 Basic ideas

In this section we collect some results and some important ideas that we will use in the proof of Theorem.  

We begin with a fundamental lemma that we will use all along this paper.

**Lemma 2** (Babai [4]). $\text{Cay}(G, S)$ is a CI-graph if and only if for every regular subgroup $\hat{G}$ of $\text{Aut}(\text{Cay}(G, S))$ isomorphic to $G$ there is a $\mu \in \text{Aut}(\text{Cay}(G, S))$ such that $\hat{G} \mu = \hat{G}$.

We introduce the following definition.

**Definition 2.** (a) We say that a Cayley graph $\text{Cay}(G, S)$ is a $C^{(2)}$-graph if and only if for every regular subgroup $\hat{G}$ of $\text{Aut}(\text{Cay}(G, S))$ isomorphic to $G$ there is a $\sigma \in \langle \hat{G}, \hat{G} \rangle^{(2)}$ such that $\hat{G}^\sigma = \hat{G}$.

(b) A group $G$ is called a $DC^{(2)}$-group if for every $S \subset G$ the Cayley graph $\text{Cay}(G, S)$ is a $C^{(2)}$-graph.

**Definition 3.** Let $\Gamma$ be an arbitrary graph and $A, B \subset V(\Gamma)$ such that $A \cap B = \emptyset$. We write $A \sim B$ if one of the following four possibilities holds:

(a) For every $a \in A$ and $b \in B$ there is an edge from $a$ to $b$ but there is no edge from $b$ to $a$.
(b) For every \(a \in A\) and \(b \in B\) there is an edge from \(b\) to \(a\) but there is no edge from \(a\) to \(b\).

(c) For every \(a \in A\) and \(b \in B\) the vertices \(a\) and \(b\) are connected with an undirected edge.

(d) There is no edge between \(A\) and \(B\).

We also write \(A \not\sim B\) if none of the previous four possibilities holds.

**Lemma 3.** Let \(A, B\) be two disjoint subsets of cardinality \(p\) of a graph. We write \(A \cup B = \mathbb{Z}_p \cup \mathbb{Z}_p\). Let us assume that \(\hat{\mathbb{Z}}_p\) acts naturally on \(A \cup B\) and for a generator \(\hat{g}\) of the cyclic group \(\hat{\mathbb{Z}}_p\) the action of \(\hat{g}\) is defined by \((a_1, a_2)\hat{g} = (a_1 + b, a_2 + c)\) for some \(b, c \in \mathbb{Z}_p\).

(a) If \(b = c\), then the action of \(\hat{\mathbb{Z}}_p\) and \(\hat{\mathbb{Z}}_p\) on \(A \cup B\) are the same.

(b) If \(A \not\sim B\), then \(b = c\).

(c) If \(A \sim B\), then every \(\pi \in \text{Sym}(A \cup B)\) which fixes \(A\) and \(B\) setwise is an automorphism of the graph defined on \(A \cup B\) if \(\pi | A \in \text{Aut}(A)\) and \(\pi | B \in \text{Aut}(B)\).

**Proof.** These statements are obvious. \(\blacksquare\)

**Lemma 4.** Let us assume that \(H\) is a regular abelian subgroup of \(\text{Sym}(p^n)\) and let \(P \geq H\) be a Sylow \(p\)-subgroup of \(\text{Sym}(p^n)\). Then \(H\) contains \(Z(P)\).

**Proof.** It is well known that the center of \(P\) is a cyclic \(p\)-group. Let \(z\) be a generator of \(Z(P)\). Then \((H, z)\) is a transitive abelian group. Hence \((H, z)\) is regular. Since \(H\) is also regular, we have that \(z\) has to be in \(H\). \(\blacksquare\)

### 4 Main result

In this section we will prove that \(\mathbb{Z}_p^3 \times \mathbb{Z}_q\) is a DCI-group if \(q > p^3\) and \(p > 3\).

Our technique is based on Lemma 2 so we fix a Cayley graph \(\Gamma = \text{Cay}(\hat{\mathbb{Z}}_p^3 \times \mathbb{Z}_q, S)\). Let \(A = \text{Aut}(\Gamma)\) and \(\hat{G} = \hat{\mathbb{Z}}_p^3 \times \hat{\mathbb{Z}}_q\) be a regular subgroup of \(A\) isomorphic to \(\mathbb{Z}_p^3 \times \mathbb{Z}_q\). In order to prove Theorem 1 we have to find an \(\alpha \in A\) such that \(\hat{G} = \hat{G}^\alpha = \hat{\mathbb{Z}}_p^3 \times \hat{\mathbb{Z}}_q\), what we will achieve in three steps.

#### 4.1 Step 1

We may assume \(\hat{\mathbb{Z}}_q\) and \(\hat{\mathbb{Z}}_q\) lie in the same Sylow \(p\)-subgroup \(Q\) of \(\text{Sym}(p^3q)\). Then both \(\hat{\mathbb{Z}}_p^3\) and \(\hat{\mathbb{Z}}_p^3\) are subgroups of \(N_{\text{Sym}(p^3q)}(Q) \cap A\) so we may assume that \(\hat{\mathbb{Z}}_p^3\) and \(\hat{\mathbb{Z}}_p^3\) lie in the same Sylow \(p\)-subgroup of \(N_{\text{Sym}(p^3q)}(Q) \cap A\) which is contained in a Sylow \(p\)-subgroup \(P\) of \(A\).

The Sylow \(q\)-subgroup \(Q\) gives a partition \(B = \{B_1, B_2, \ldots, B_{p^3}\}\) of the vertices of \(\Gamma\), where \(|B_i| = q\) for every \(i = 1, \ldots, p^3\). It is easy to see that \(B\) is
invariant under the action of $\mathbb{Z}_p^3$ and $\mathbb{Z}_p^3$ and hence $\langle \hat{G}, \hat{G} \rangle \leq \text{Sym}(q) \cap \text{Sym}(p^3)$. Moreover, both $\hat{G}$ and $\hat{G}$ are regular so $\mathbb{Z}_p^3$ and $\mathbb{Z}_p^3$ induce regular action on $\mathcal{B}$ which we denote by $H_1$ and $H_2$, respectively. The assumption that $\mathbb{Z}_p^3$ and $\mathbb{Z}_p^3$ lie in the same Sylow $p$-subgroup of $A$ implies that $H_1$ and $H_2$ are in the same Sylow $p$-subgroup of $\text{Sym}(p^3)$, what we denote by $P_1$.

4.2 Step 2

Let us assume that $\hat{Z}_q \neq \hat{Z}_q$ which is generated by $p^3$ disjoint $q$-cycles. We intend to find an element $\alpha \in A$ such that $\hat{Z}_q = \hat{Z}_q$.

We define a graph $\Gamma_0$ on $\mathcal{B}$ such that $B_i$ is connected to $B_j$ if and only if $B_i \sim B_j$. This is an undirected graph with vertex set $\mathcal{B}$ and both $\mathbb{Z}_p^3$ and $\mathbb{Z}_p^3$ are regular subgroups of $\text{Aut}(\Gamma_0)$. It follows that $\Gamma_0$ is a Cayley graph of $\mathbb{Z}_p^3$.

**Definition 4.** (a) For a pair $(B_i, B_j) \in \mathcal{B}^2$ we write $B_i \equiv B_j$ if either there exists a path $C_1, C_2, \ldots, C_n$ in $\Gamma_0$ such that $C_1 = B_1$, $C_n = B_2$, or $i = j$.

(b) For a pair $(B_i, B_j) \in \mathcal{B}^2$ we write $B_i \not\equiv B_j$ if $B_i \equiv B_j$ does not hold.

(c) If both $H$ and $K$ are subsets of the vertices of $\Gamma_0$ such that $H \cap K = \emptyset$ and for every $B_i \in H$, $B_j \in K$ we have $B_i \not\equiv B_j$, then we write $H \not\equiv K$.

**Observation 1.** (a) The relation $\equiv$ defines an equivalence relation on $\mathcal{B}$. The connected components of $\Gamma_0$ will be called equivalence classes.

(b) Since $H_1$ acts transitively on $\mathcal{B}$ we have that the size of the equivalence classes defined by the relation $\equiv$ divides $p^3$.

We can also define a colored graph $\Gamma_1$ on $\mathcal{B}$ by coloring the edges of the complete directed graph on $p^3$ points. $B_i$ is connected to $B_j$ with the same color as $B_i$ is connected to $B_j$ in $\Gamma_1$ if and only if there exists a graph isomorphism $\phi$ from $B_i \cup B_j$ to $B_i' \cup B_j'$ such that $\phi(B_i) = B_i'$ and $\phi(B_j) = B_j'$. The graph $\Gamma_1$ is a colored Cayley graph of the elementary abelian $p$-group $\mathbb{Z}_p^3$. Moreover, both $H_1$ and $H_2$ act regularly on $\Gamma_1$.

We prove the following two lemmas what we will use several times in this step.

**Lemma 5.** Let us assume that $C_1', C_2', \ldots, C_k'$ are the equivalence classes defined in $V(\Gamma_0)$ and let $C_i = \cup C_i' \subset V(\Gamma)$ for every $i = 1, \ldots, k$. Let $\alpha$ be a permutation on the vertex set $V(\Gamma)$ such that for every $1 \leq i \leq k$ the restriction $\alpha \mid C_i = \eta_i \mid C_i$ for some $\eta_i \in \text{Aut}(\Gamma)$ and $\alpha^{V(\Gamma_0)}$ is an automorphism of $\Gamma_0$. Then $\alpha$ is an automorphism of $\Gamma$.

**Proof.** Let $x$ and $y$ be points in $V(\Gamma)$. We have to prove that $x$ is connected to $y$ if and only if $\alpha(x)$ is connected to $\alpha(y)$. This holds if $x$ and $y$ are in the same $C_i$ for some $1 \leq i \leq k$ since $\alpha \mid C_i$ is defined by an automorphism of $\Gamma$ on $C_i$. If $x \in B_m$ and $y \in B_n$, where $B_m \sim B_n$ and $x$ is connected to $y$, then every element of $B_m$ is connected to every element of $B_n$. Since $\alpha^{V(\Gamma_0)} \in \text{Aut}(\Gamma_0)$ the
same holds for \( \alpha(B_m) \) and \( \alpha(B_n) \) and hence \( \alpha(x) \) is connected to \( \alpha(y) \). Similar argument shows that if \( x \in B_m \) and \( y \in B_n \), where \( B_m \sim B_n \) and \( x \) is not connected to \( y \), then \( \alpha(x) \) is not connected to \( \alpha(y) \).

Lemma 6.  
(a) Let \( A \) and \( B \) be two disjoint subsets of cardinality \( q \) of \( V(\Gamma) \). We write \( A = \{(a, x) \mid x \in \mathbb{Z}_q \} \) and \( B = \{(b, x) \mid x \in \mathbb{Z}_q \} \). Let us assume that \( \hat{\varphi} \) and \( \hat{\psi} \) are automorphisms of the graph \( \Gamma \) with \( \hat{\varphi}(a, x) = (a, x + 1) \), \( \hat{\psi}(b, x) = (b, x + 1) \) and \( \hat{\varphi}(b, x) = (b, x + d) \) for some \( d \in \mathbb{Z}_q \) for all \( x \in \mathbb{Z}_q \). Furthermore, let us assume that \( \hat{\varphi} \) and \( \hat{\psi} \) are automorphisms of the graph \( \Gamma \) with \( \hat{\varphi}(A) = \hat{\psi}(A) = B \) and \( \hat{\varphi} \) and \( \hat{\psi} \) commute with \( \hat{\varphi} \) and \( \hat{\psi} \), respectively. Then for \( \alpha = \hat{\varphi} \hat{\psi}^{-1} \) we have \( \hat{\varphi}^\alpha \mid_B = \hat{\psi}^\alpha \mid_B \).

(b) Let us assume that \( C = \{(c, x) \mid x \in \mathbb{Z}_q \} \) is a subset of \( V(\Gamma) \) with \( A \cap B = A \cap C = \emptyset \). We also assume that \( \hat{\varphi}(c, x) = (c, x + 1) \) and \( \hat{\psi}(c, x) = (c, x + d) \) for every \( x \in \mathbb{Z}_q \). Let us assume that \( \hat{\varphi} \in \text{Aut}(\Gamma) \) with \( \hat{\varphi}(A) = C \) and we also assume that \( \hat{\varphi} \) and \( \hat{\psi} \) commute. Then for \( \beta = \hat{\psi} \hat{\varphi}^{-1} \) we have \( \hat{\varphi}^\beta \mid_B = \hat{\psi}^\beta \mid_B \).

Proof.  
(a) Let us assume that \( \hat{\varphi}(a, 0) = (b, b_0) \) and \( \hat{\psi}(a, 0) = (b, b'_0) \) for some \( b_0, b'_0 \in \mathbb{Z}_q \). Using that \( \hat{\varphi} \) and \( \hat{\psi} \) commute we get that \( \hat{\varphi}(a, x) = (b, b_0 + x) \) for every \( x \in \mathbb{Z}_q \) and similarly we have \( \hat{\psi}(a, x) = (b, b'_0 + dx) \). Thus

\[
\alpha(b, x) = \alpha(b, b_0 + (x - b_0)) = \hat{\varphi}(a, x - b_0) = (b, b_0 + (x - b_0) + dx) = (b, (b'_0 - db_0) + dx).
\]

It is easy to derive that \( \alpha^{-1}(b, x) = \left(b, \frac{x - (b'_0 - db_0)}{d}\right) \). Using the previous two equations we get

\[
\alpha^{-1} \hat{\varphi} \mid_B(b, x) = \alpha^{-1} \hat{\psi} \left(b, (b'_0 - db_0) + dx\right) = \alpha^{-1} \hat{\varphi} \left(b, (b'_0 - db_0) + dx + d\right) = \left(b, \frac{(b'_0 - db_0) + dx + d - (b'_0 - db_0)}{d}\right) = (b, x + 1).
\]

(b) Let us assume that \( \hat{\psi}(a, 0) = (c, c_0) \) for some \( c_0 \in \mathbb{Z}_q \). Then \( \hat{\psi}(a, x) = (c, c_0 + dx) \) for all \( x \in \mathbb{Z}_q \) Thus

\[
\beta(b, x) = \hat{\psi} \hat{\varphi}^{-1} \left(b, b_0 + (x - b_0)\right) = \hat{\psi} \left(a, x - b_0\right) = (c, c_0 + (x - b_0) + dx)
\]

and hence \( \beta^{-1}(c, x) = \left(b, \frac{x - c_0 + db_0}{d}\right) \). Similarly to the previous case we have

\[
\beta^{-1} \hat{\varphi} \beta(b, x) = \beta^{-1} \hat{\varphi} \left(c, c_0 + (x - b_0) + dx\right) = \beta^{-1} \left(c, (c_0 + (x - b_0)) + dx\right) = \left(b, \frac{c_0 + (x - b_0) + dx - c_0 + b_0}{d}\right) = (b, x + 1).
\]
The points of the graph $\Gamma_0$ and $\Gamma_1$ can be identified with the elements of $\mathbb{Z}_p^3$ and we may assume that the action of an element $r$ of the Sylow $p$-subgroup $P_1$ is the following:

$$r(a, b, c) = (a + x, b + s_a, c + t_{a,b}),$$

where $s_a$ only depends on $a$ and $t_{a,b}$ depends on $a$ and $b$.

Let $\hat{g}$ and $\bar{g}$ denote the generator of $\mathbb{Z}_q$ and $\hat{Z}_q$, respectively. We may assume that $\hat{g} \mid B_1 = \bar{g} \mid B_1$.

(a) Let us assume first that $\Gamma_0$ is a connected graph.

Using Lemma 3(b) we get that $\hat{g} \mid B_i = \bar{g} \mid B_i$ if there exists a path in $\Gamma_0$ from $B_i$ to $B_j$. This shows that $\hat{g} = \bar{g}$ since $\Gamma_0$ is connected in this case.

(b) Let us assume that $\Gamma_0$ is the empty graph.

For every $B_m \in \mathcal{B}$ there exist $\hat{r}_m$ and $\bar{r}_m$ such that $\hat{r}_m(B_1) = \bar{r}_m(B_1) = B_m$.

Let $\alpha$ be defined as follows

$$\alpha \mid B_1 = id$$
$$\alpha \mid B_m = \hat{r}_m \bar{r}_m^{-1} \text{ for } 2 \leq m \leq p^3. \quad (1)$$

It is easy to see that $\alpha^{B} = id$ so using Lemma 3 we get that $\alpha$ is an automorphism of $\Gamma$. Using Lemma 6(a) we get that $\hat{g}^\alpha = \bar{g}$.

(c) Let us assume that the size of the connected components of $\Gamma_0$ is $p$.

Let $C'_1, C'_2, \ldots, C'_{p^2}$ denote the equivalence classes defined by the relation $\equiv$ on $\Gamma_0$ and for $1 \leq m \leq p^2$ let $C_m = \bigcup C'_m$. For $C'_2, \ldots, C'_{p^2}$ we choose an element $\hat{u}_m$ of $\hat{Z}_q$ such that $\hat{u}_m(C_1) = C_m$. We may assume that $B_1 \subset C_1$. Since $H_3$ is regular on $\Gamma_0$, for every $2 \leq m \leq p^2$ there exists $\hat{u}_m$ such that $\hat{u}_m(B_1) = \hat{u}_m(B_1)$. For $2 \leq m \leq p^2$ let $\hat{u}_m = \hat{u}_m \hat{u}_m^{-1}$. Now we define the following permutation:

$$\alpha_1 \mid C_1 = id$$
$$\alpha_1 \mid C_m = \hat{u}_m \text{ for } 2 \leq m \leq p^2.$$ 

Clearly, for $2 \leq m \leq p^2$ we have $\hat{u}_m(B_j) = B_j$ for at least one $B_j \subset C_m$. Since $H_1$ and $H_2$ are in the same Sylow $p$-subgroup of $Sym(p^3)$ the order of $\hat{u}_m$ is a power of $p$. We also have that $C_m$ is the union of $p$ elements of $\mathcal{B}$ for $1 \leq m \leq p^2$ hence $\alpha_1^{B} = id$. We also have that $\alpha_1 \mid C_m$ is the restriction of an automorphism of the graph $\Gamma$ for $m = 1, \ldots, p$. Therefore by Lemma 6(a) $\alpha_1$ is an automorphism of the graph $\Gamma$.

Finally, Lemma 6(b) gives $\hat{g}^{\alpha_1} = \bar{g}$.

(d) Let us assume that the size of the connected components of $\Gamma_0$ and hence the size of the equivalence classes is $p^2$. Let $D'_0, D'_1, \ldots, D'_{p-1}$ denote the equivalence classes and let $D_m = \cup D'_m$ for $0 \leq m \leq p - 1$. 

7
Using Lemma 4 we get that $H \cap H_2 \neq \{1\}$. Let $z$ be an element of order $p$ of $H \cap H_2$ and we denote by $z_1$ and $z_2$ the element of $\mathbb{Z}_p^3$ and $\mathbb{Z}_p^3$ such that $z^p = z_2^p = z$, respectively. Then $(z_2^{-1}z_1)^p = id$ for $i = 1, \ldots, p - 1$.

Let us assume first that $z_1(D_0) \neq D_0$. We may assume that $z_1(D_0) = D_i$ for $i = 0, 1, \ldots, p - 1$. We define $\alpha_2$ in the following way:

$$\alpha_2 \mid D_0 = id$$
$$\alpha_2 \mid D_i = z_2z_1^{-i} \text{ for } 1 \leq i \leq p - 1.$$

Since $z^p = z_2^p = z$ we have $\alpha_2^p = id$. Using Lemma 5 again we get that $\alpha_2 \in Aut(\Gamma)$ and Lemma 6 gives $\hat{g}^{\alpha_2} = \hat{g}$.

Therefore we may assume that $z_1(D_0) = D_0$. In this case the orbits of $z$ give a $(H_1, H_2)$-invariant partition $\mathcal{E} = \{E_{a,b} \mid a, b \in \mathbb{Z}_p\}$ of $\mathcal{B}$. Using that the elements of $B = V(\Gamma_0)$ can be identified with elements of $\mathbb{Z}_p^3$ we may assume that $E_{a,b}$ has the following form for every $(a, b) \in \mathbb{Z}_p^2$:

$$E_{a,b} = \{(a, b, c) \in \mathbb{Z}_p^3 \mid c \in \mathbb{Z}_p\}.$$

We may also assume that $D'_0 = \bigcup b \in \mathbb{Z}_p E_{a,b}$ for all $a \in \mathbb{Z}_p$.

Since $H_1$ acts regularly on $\Gamma_0$, there exists $h_1 \in H_1$ such that $h_1(E_{0,0}) = E_{0,1}$. Since $H_2$ is also regular, there exists $h_2 \in H_2$ such that $h_2(E_{0,0}) = h_1(E_{0,0})$. Since the order of $h_1$ and $h_2$ are $p$ and $h_1(D'_0) = h_2(D'_0) = D'_0$ we have that $h_1(D'_i) = h_2(D'_i) = D'_i$ for $i = 0, 1, \ldots, p - 1$.

We may assume that $z, h_1$ and $h_2$ act in the following way on $\mathbb{Z}_p^3$:

$$z(a, b, c) = (a, b, c + 1)$$
$$h_1(a, b, c) = (a, b + 1, c)$$
$$h_2(a, b, c) = (a, b + s_a, c + t_{a,b}).$$

The assumption that $h_1(E_{0,0}) = h_2(E_{0,0}) = E_{0,1}$ gives that $s_0 = 1$.

We claim that $s_a = 1$ for $1 \leq a \leq p - 1$. Since $H_2$ is regular on $\Gamma_0$, there exists $k_2 \in H_2$ such that $k_2(0, 0, 0) = (a, 0, 0)$. Since $h_2$ and $k_2$ we have that $k_2(0, i, 0) = (a, s_a i, w_i)$ for some $w_i \in \mathbb{Z}_p$. If $s_a \neq 1$, then such an element cannot be in the Sylow $p$-subgroup $P_1$.

Therefore $h_2(a, b, c) = (a, b + 1, c + t_{a,b})$ for all $(a, b, c) \in \mathbb{Z}_p^3$, where $t_{a,b} \in \mathbb{Z}_p$, only depends on $a$ and $b$.

**Lemma 7.** Let $a \neq a'$ be elements of $\mathbb{Z}_p$ and we fix two more elements $b$ and $b'$ of $\mathbb{Z}_p$. Then either $E_{a,b} \sim E_{a',b'}$ or $t_{a,b+n} = t_{a',b'+n}$ for all $n \in \mathbb{Z}_p$.

**Proof.** For all $m \in \mathbb{Z}_p$ the permutation $h_2^m h_1^{-m}$ fixes $E_{a,b}$ and $E_{a',b'}$. Moreover,

$$h_2^m h_1^{-m}(a, b, c) = (a, b, c + \sum_{i=1}^{n} t_{a,b-i})$$
$$h_2^m h_1^{-m}(a', b', c) = (a', b', c + \sum_{i=1}^{n} t_{a',b'-i})$$

(2)
One can see using Lemma 3 (b) that if \( \sum_{i=1}^{n} t_{a,b}^{-i} \neq \sum_{i=1}^{n} t_{a',b'}^{-i} \) for some \( m \in \mathbb{Z}_p \), then \( E_{a,b} \sim E_{a',b'} \). If \( \sum_{i=1}^{n} t_{a,b}^{-i} = \sum_{i=1}^{n} t_{a',b'}^{-i} \) for all \( m \in \mathbb{Z}_p \), then \( t_{a,b+n} = t_{a',b'+n} \) for \( n \in \mathbb{Z}_p \). \( \blacksquare \)

For each \( a \in \mathbb{Z}_p \) we define the following function from \( \mathbb{Z}_p \) to \( \mathbb{Z}_p \):

\[
t'_a(b) := t'_{a,b}.
\]

**Lemma 8.** Let us assume that \( t_a(b+n) = t'_a(b'+n) \) for all \( n \in \mathbb{Z}_p \) and we denote by \( k_2 \) the unique element of \( H_2 \) which maps \( (a,b,0) \) to \( (a',b',0) \). Then \( k_2(a,b+d,e) = (a',b'+d,e) \) for all \( d,e \in \mathbb{Z}_p \).

**Proof.** Since \( k_2 \) and \( z \) commute we have \( k_2(a,b,m) = (a',b',m) \) for all \( m \in \mathbb{Z}_p \). We also have that \( k_2 \) and \( h_2 \) commute which gives \( k_2(a,b+d,e) = (a',b'+d,e) \) for all \( d,e \in \mathbb{Z}_p \). \( \blacksquare \)

**Corollary 1.** If the conditions of Lemma 8 hold and \( k_1 \) is the unique element of \( H_1 \) such that \( k_1(a,b,0) = (a',b',0) \), then \( k_1 \upharpoonright E_{a,b} = k_2 \upharpoonright E_{a,b} \).

We define an equivalence relation on the set \( \{D'_0, D'_1, \ldots, D'_{p-1}\} \). We write \( D'_a \equiv D'_{a'} \) if and only if there exist \( b \) and \( b' \) in \( \mathbb{Z}_p \) such that \( t_{a,b+n} = t_{a',b'+n} \) for all \( n \in \mathbb{Z}_p \).

Now we can choose a point \( (a,b_0,0) \) in every \( D'_a \) such that if \( D_a \simeq D'_a \), then \( t_{a,b_0+n} = t_{a',b_0'+n} \) for all \( n \in \mathbb{Z}_p \). For every \( 1 \leq a \leq p-1 \) there exist \( \hat{v}_a \in \mathbb{Z}_p^3 \) and \( \hat{v}_a \in \mathbb{Z}_p^3 \) such that \( \hat{v}_a^R(0,b_0,0) = \hat{v}_a^B(0,b_0,0) = (a,b_0,0) \) since both \( H_1 \) and \( H_2 \) are regular.

Now we can define the following permutation:

\[
\alpha_3 \upharpoonright D_0 = \text{id}
\]

\[
\alpha_3 \upharpoonright D_a = \hat{v}_a \hat{v}_a^{-1} \text{ for } 1 \leq a \leq p-1.
\]

**Lemma 9.** \( \alpha_3 \) is an automorphism of \( \Gamma \).

**Proof.** We prove that \( \alpha_3^R \) is an automorphism of the graph \( \Gamma_1 \). If \( B_i \cup B_j \) is contained in \( D'_a \) for some \( a \in \mathbb{Z}_p \), then \( \alpha_3 \) is defined by the restriction of an automorphism of \( \Gamma \). Therefore we only have to investigate those pairs \( B_i, B_j \) of points which are not in the same set \( D'_a \) for any \( a \in \mathbb{Z}_p \).

Let us assume that \( B_i \in E_{a,b} \) and \( B_j \in E_{a',b'} \). By the definition of \( \alpha_3 \), for every \( c \in \mathbb{Z}_p \) at least one \( E_{c,d} \) is fixed by \( \alpha_3^R \). Therefore \( \alpha_3^R \) fixes every set \( E_{c,d} \) since the order of \( \alpha_3^R \upharpoonright D'_c \) is a power of \( p \) for every \( c \in \mathbb{Z}_p \).

Let us assume first that \( D_a \simeq D'_a \). Lemma 7 gives that \( B_i \) is connected to \( B_j \) if and only if \( \alpha'_3(B_i) \) is connected to \( \alpha'_3(B_j) \) since \( E_{a,b} \sim E_{a',b'} \).

Let us now assume that \( D'_a \simeq D'_a \). We denote by the pair \( (\hat{v}_a \hat{v}_a^{-1}, \hat{v}_a \hat{v}_a^{-1}) \) the restriction of the action of \( \alpha_3 \) to \( D'_a \cup D'_a \). Since \( \hat{v}_a \) and \( \hat{v}_a^{-1} \) are automorphisms of \( \Gamma \) the pair \( ((\hat{v}_a \hat{v}_a^{-1})^R, (\hat{v}_a \hat{v}_a^{-1})^B) \) is an automorphism of
the induced subgraph on $D'_a \cup D'_a$, if and only $(id^B, (\hat{v}_a^{-1}\hat{v}_a^{-1}\hat{v}_a)^B)$ is. Since both $\hat{Z}_3'$ and $\hat{Z}_p'$ are abelian we have

$$(id^B, (\hat{v}_a^{-1}\hat{v}_a^{-1}\hat{v}_a)^B) = (id^B, (\hat{v}_a\hat{v}_a)^B(\hat{v}_a\hat{v}_a^{-1})^B).$$

Clearly, $(\hat{v}_a\hat{v}_a^{-1})^B(a', b_a, 0) = (a, b_a, 0)$ and $(\hat{v}_a\hat{v}_a^{-1})^B(a, b_a, 0) = (a', b_a', 0)$. Using Corollary 1 we get that

$$(id^B, (\hat{v}_a^{-1}\hat{v}_a^{-1}\hat{v}_a)^B) = (id^B, id^B)$$

which is clearly an automorphism on $D'_a \cup D'_a$. This proves that $\alpha_3^B \in Aut(\hat{\Gamma}_1)$.

If $B_i \sim B_j$, then $\alpha_3(B_i) \sim \alpha_3(B_j)$ since $\alpha_3^B \in Aut(\Gamma_1)$ thus $p_i \in B_i$ is connected to $p_j \in B_j$ if and only if $\alpha_3(p_i)$ is connected to $\alpha_3(p_j)$.

If $B_i \sim B_j$, then there exists $a \in \mathbb{Z}_p$ such that $B_i$ and $B_j \subset D_a$. Since $\alpha_3$ is defined on $D_a$ by an automorphism of $\Gamma$ we have that $p_i \in B_i$ is connected to $p_j \in B_j$ if and only if $\alpha_3(p_i)$ is connected to $\alpha_3(p_j)$, finishing the proof of Lemma 9.

Finally, one can see using Lemma 6(b) that $\hat{g}^{\alpha_3} = \hat{g}$.

### 4.3 Step 3

Let us assume that for the generators of the cyclic groups $\hat{g} \in \hat{Z}_q$ and $\hat{g} \in \hat{\mathbb{Z}}_q$ we have $\hat{g} = \hat{g}.

Since $\hat{g} = \hat{g}$ we have that $\hat{Z}_3$ and $\hat{Z}_q$ are contained in $C_3(\hat{g})$. Using Sylow’s theorem again we may assume that $\hat{Z}_3$ and $\hat{Z}_q$ are in the same Sylow $p$-subgroup of $C_3(\hat{g})$. Using all these assumptions we prove the following Lemma.

**Lemma 10.** (a) $\hat{Z}_3 \times \hat{\mathbb{Z}}_q \leq \hat{Z}_p \times Sym(p^3)$.

(b) If $\hat{Z}_3 \times \hat{\mathbb{Z}}_q \leq \hat{Z}_p \times Sym(p^3)$, then for every $\hat{u} \in \hat{Z}_p$ we have $(\hat{u})_b = id$.

**Proof.** (a) $\hat{Z}_3 \times \hat{\mathbb{Z}}_q \leq \hat{Z}_p \times Sym(p^3)$ since the elements of $\hat{Z}_3$ and $\hat{g}$ commute.

(b) Let $A' = A \cap \hat{\mathbb{Z}}_q \times Sym(p^3)$. We have already assumed that $\hat{Z}_p$ and $\hat{Z}_3$ lie in the same Sylow $p$-subgroup of $A'$, which is generated by $p^3$ disjoint $q$-cycles. Let $\hat{u}$ be an arbitrary element of $\hat{Z}_p$. For every $(b, s) \in \hat{Z}_p \times \hat{\mathbb{Z}}_q$ we have $\hat{u}(b, s) = (c, s + t)$ for some $c \in \hat{Z}_p$ and $t \in \mathbb{Z}_q$, where $t$ only depends on $\hat{u}$ and $b$ since $\hat{u} \in \hat{Z}_q \times Sym(p^3)$. The permutation group $\hat{G}$ is transitive, hence there exist $\hat{u}_1, \hat{u}_2 \in \hat{Z}_p$ such that $\hat{u}_1(0, s) = (b, s)$ and $\hat{u}_2(c, s + t) = (0, s + t)$. The order of $\hat{u}_2\hat{u}_1$ is a power of $p$ since $\hat{u}_2, \hat{u}$ and $\hat{u}_1$ lie in a Sylow $p$-subgroup. Therefore $t = 0$ and hence $(\hat{u})_b = id$. 


Lemma 10 says that for every $\hat{u} \in \hat{Z}_p^3$ we have $(u)_p = id$. We use again the graph $\Gamma_1$ defined on $B$. It is clear that $H_1$ and $H_2$ are regular subgroups in $Aut(\Gamma_1)$ and they are isomorphic to $Z_p^3$. Since $Z_p^3$ is a DCI$^{(2)}$-group we have that there exists $\mu \in \langle H_1, H_2 \rangle^{(2)}$ such that $H_2^\mu = H_1$. Let $\eta = \mu id_B$ be an element of the wreath product $\mathbb{Z}_q \wr \text{Sym}(p^3)$. Clearly, $\eta \in \langle \hat{G}, \hat{G} \rangle^{(2)}$ and hence $\eta$ is an automorphism of $\Gamma_0$, which conjugates $\hat{Z}_p^3$ to $\hat{Z}_p^3$. Moreover, the base group part of $\eta$ is the identity so $\eta \in CA(\hat{g})$. This proves that $\hat{G}^\eta = \hat{G}$, finishing the proof of Theorem 1.

References

[1] A. Ádám, Research Problem 2-10, J. Combin. Theory 2 (1967), 393.

[2] B. Alspach, T. D. Parsons, Isomorphism of Circulant graphs and digraphs, Discrete Mathematics 25 (1979) 97-108.

[3] B. Alspach, L. A. Nowitz, Elementary Proofs that $Z_p^2$ and $Z_p^3$ are CI-groups, Europ. J. Combinatorics 20 (1999), 607-617.

[4] L. Babai, P. Frankl, Isomorphism problem for a class of point-symmetric structures, Acta Math. Acad. Syi. Hungar. 29, 329-336.

[5] L. Babai, P. Frankl, Isomorphisms of Cayley graphs I, in: Colloqzeria Mathematica Societatis János Bolyai, Vol. 18. Combinatorics, Keszthely, 1976, North-Holland, Amsterdam (1978) 35-52.

[6] D. Ž. Djoković, Acta Math. Acad. Sci. Hungar. 21 (1970), 267-270.

[7] E. Dobson, Isomorphism problem for Cayley graphs of $Z_p^3$, Discrete Math. 147 (1995), 87-94.

[8] B. Elspas, J. Turner, Graphs with circulant adjacency matrices, J. Combin. Theory, 9 (1970), 297-307.

[9] C. D. Godsil, On Cayley graph isomorphisms, Ars Combin. 15 (1983), 231-246.

[10] M. Hirasaka, M. Muzychuk, The elementary abelian group of rank 4 is a CI-group, J. Combin. Theory Ser. A 94 (2001), 339-362.

[11] M. H. Klin and R. Poschel, 'The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings', Algebraic methods in graph theory, Szeged, 1978, Colloquia Mathematica Societatis János Bolyai 25 (North-Holland, Amsterdam, 1981) 405-434.

[12] I. Kovács, M. Muzychuk, The group $\mathbb{Z}_{p^2} \times \mathbb{Z}_q$ is a CI-group, Comm. Alg. 37 (2009), 3500-3515.
[13] C. H. Li, Z. P. Lu, P. P. Pálfy, Further restrictions on the structure of finite CI-groups, J. Algebr. Comb, 26 (2007), 161-181.

[14] M. Muzychuk, Ádám’s conjecture is true in the square-free case, J. Combin. Theory Ser. A 72 (1995), 118-134.

[15] M. Muzychuk, On Ádám’s conjecture for circulant graphs, Discrete Math. 167/168 (1997), 497-510; corrigendum 176 (1997), 285-298.

[16] M. Muzychuk, An elementary Abelian group of large rank is not a CI-group, Discrete Math. 264(1-3) (2003), 167-185.