ELSEVIER

Discrete Mathematics 147 (1995) 87–94

DISCRETE MATHEMATICS

Isomorphism problem for Cayley graphs of Z_p^3 ☆

Edward Dobson

Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, 16 Mill Lane, Cambridge, CB2 1SB, England, UK and Department of Mathematics, Louisiana State University, Baton Rouge, LA 70803, USA

Received 23 November 1993; revised 20 January 1995

Abstract

We prove that if two Cayley graphs of Z_p^3 are isomorphic, then they are isomorphic by a group automorphism of Z_p^3.

In [3], Babai and Frankl conjectured that Z_p^3 is a CI-group with respect to graphs for all primes p and $k \geqslant 1$. The case $k = 1$ was settled positively by several authors [1, 3, 5, 6]. It was shown by Godsil [7] that the conjecture is true for $k = 2$. Recently, Nowitz [8] gave an example showing that Z_p^k is not a CI-group with respect to graphs for all $k \geqslant 6$, and asked if there existed a prime p_0 so that if $p \geqslant p_0$ and p is prime, then Z_p^3 is not a CI-group with respect to graphs. We will answer this question negatively by showing that Z_p^3 is a CI-group with respect to graphs for all primes p.

1. Preliminaries

For general information on permutation groups, the reader is referred to [9]. Let G be a group and $H \subseteq G - \{1\}$ such that $H = H^{-1}$. We define the *Cayley graph* $\Gamma(G,H)$ to be the graph with $V(\Gamma(G,H)) = G$ and $E(\Gamma(G,)) = \{(g,gh)\colon g \in G, h \in H\}$. H is said to be the *connection set* of $\Gamma(G,H)$. We will say Γ is a Cayley graph for G if $\Gamma = \Gamma(G,H)$ for some $H \subseteq G - \{1\}$, $H = H^{-1}$. Clearly if Γ is a Cayley graph for G then $G_L = \{g_L\colon G \to G\colon g_L(x) = gx,\ g \in G\} \leqslant \mathrm{Aut}(\Gamma)$. We shall say that a Cayley graph Γ of G is a *CI-graph* with respect to G if, given any Cayley graph Γ' of G such

☆ This work was done towards partial completion of a Ph.D. degree at Louisiana State University under the supervision of Professor Béla Bollobás.

Correspondence address: Department of Mathematics, Louisiana State University, Baton Rouge, LA 70803, USA.

SSDI 0012-365X(95)00099-2

that Γ is isomorphic to Γ', then Γ and Γ' are isomorphic by some $\alpha \in \mathrm{Aut}(G)$. Babai [2] characterized this property in the following way:

Lemma 1. *For a Cayley graph Γ of G the following are equivalent:*

(i) *Γ is a CI-graph.*

(ii) *Given a permutation $\phi \in S_G$ such that $\phi^{-1}G_L\phi \leqslant \mathrm{Aut}(\Gamma)$, G_L and $\phi^{-1}G_L\phi$ are conjugate in* $\mathrm{Aut}(\Gamma)$.

Let G be a transitive group of degree mk such that there exists a transitive subgroup $H < G$ such that H admits a complete block system $\mathscr{B}$ of m blocks each of size k. Enumerate the blocks $B_0, B_1, \ldots, B_{m-1}$. Define a map $\pi_1 : H \to S_m$ by $\pi_1(\alpha) = \alpha/\mathscr{B}$ where $\alpha/\mathscr{B}(i) = j$ if and only if $\alpha(B_i) = B_j$. Clearly π_1 is a homomorphism. Let $H/\mathscr{B} = \mathrm{Im}(\pi_1)$.

A graph Γ is said to be an (m,p)-galactic graph if there exists $\alpha \in \mathrm{Aut}(\Gamma)$ such that all of the orbits of α have order p, and $|V(\Gamma)| = mp$. Let $[\alpha]$ be the subgroup of $\mathrm{Aut}(\Gamma)$ such that if $\delta \in [\alpha]$, then the orbits of $\delta^{-1}\alpha\delta$ are the same as the orbits of α. A graph Γ will be called an (m,p)-uniformly galactic graph if Γ is an (m,p)-galactic graph and $[\alpha]$ is transitive.

Let G be a transitive permutation group that admits a complete block system $\mathscr{B} = \{B_i : i \in \mathbf{Z}_m\}$ of m blocks of size p, p a prime, and $\mathscr{B}$ is formed by the orbits of some normal subgroup $N \lhd G$. Then for each B_i there exists $\alpha_i \in N$ such that $\alpha_i|_{B_i}$ is a p-cycle. Define an equivalence relation $\equiv$ on the blocks $B_0, \ldots, B_{m-1}$ by $B_i \equiv B_j$ if and only if whenever $\alpha \in N$ and $\alpha|_{B_i}$ is a p-cycle then $\alpha|_{B_j}$ is also a p-cycle. Denote the equivalence classes of $\equiv$ by $C_0, \ldots, C_a$ and let $E_i = \bigcup_{j \in C_i} B_j$. Then

Lemma 2. *Let Γ be a vertex transitive growth with $G \leqslant \mathrm{Aut}(\Gamma)$ as above. Then there exists $H \leqslant \mathrm{Aut}(\Gamma)$ such that $G \leqslant H$ and each E_i is a block of H. Further, Γ is an (m,p)-uniformly galactic graph and for each $0 \leqslant i \leqslant a$ there exists $\alpha_i \in H$ such that $\alpha_i|_{E_i}$ is semiregular of order p and $\alpha_i|_{E_j} = 1$ for every $i \neq j$.*

Proof. We first show that if $B_j \in E_i$, $B_k \notin E_i$ and some vertex of B_j is adjacent to some vertex of B_k, then every vertex of B_j is adjacent to every vertex of B_k. This will imply that for each equivalence class E_i there exists $\alpha_i \in \mathrm{Aut}(\Gamma)$ such that $\alpha_i|_{B_s}$ is a p-cycle for every $B_s \in E_i$ and $\alpha_i|_{B_t} = 1$ for every $B_t \notin E_i$, and so that Γ is an (m,p)-uniformly galactic graph. We then show that each E_i is a block of $H = \langle G, \alpha_i : 0 \leqslant i \leqslant a \rangle$.

As $B_j \in E_i$ and $B_k \notin E_i$, there exists $\gamma_j \in G$ such that either $\gamma_j|_{B_j}$ is a p-cycle and $\gamma_j|_{B_k}$ is not, or $\gamma_j|_{B_k}$ is a p-cycle and $\gamma_j|_{B_j}$ is not. Without loss of generality, assume that $\gamma_j|_{B_j}$ is a p-cycle and $\gamma_j|_{B_k} = 1$. Let $\delta_k \in G$ such that $\delta_k|_{B_k}$ is a p-cycle. If $\delta_k | B_j$ is not a p-cycle, then we assume without loss of generality that $\delta_k|_{B_j} = 1$. Then $\gamma_j\delta_k|_{B_j}$ is a p-cycle and $\gamma_j\delta_k|_{B_k}$ is a p-cycle. We conclude that each vertex of B_j is adjacent to some vertex of B_k. Further, as $\gamma_j \in G$, each vertex of B_k is adjacent to every vertex of B_j, and, similarly, as $\delta_k \in G$ every vertex of B_k is adjacent to every vertex of B_j. If $\delta_k|_{B_j}$ is a p-cycle, then each vertex of B_k is adjacent to some vertex of B_j. As $\gamma_j \in G$, each vertex of B_k is adjacent to every vertex of B_j. Hence every vertex of B_j is adjacent to every vertex of B_k.

Hence for each equivalence class E_i there exists $\alpha_i \in \mathrm{Aut}(\Gamma)$ such that $\alpha_i|_{B_s}$ is a p-cycle for every $B_s \in E_i$ and $\alpha_i|_{B_t} = 1$ for every $B_t \notin E_i$. Suppose $\beta \in H$ such that $\beta(E_i) \cap E_i \neq \emptyset$ and $\beta(E_i) \neq E_i$. Then there exists $B_s \in E_i$ such that $\beta(B_s) \notin E_i$ and $B_t \in E_i$ such that $\beta(B_t) \in E_i$. Then $\beta\alpha_i\beta^{-1}|_{\beta(B_t)}$ is a p-cycle and there exists $B_u \in E_i$ such that $\beta\alpha_i\beta^{-1}|_{B_u} = 1$, a contradiction. Hence each E_i is a block of H. □

2. The main result

We first prove a lemma that settles the case when Γ is a wreath product of two graphs.

Lemma 3. *If Γ is a Cayley graph of $\mathbf{Z}_p^3$ and Γ is isomorphic to a Cayley graph of $\mathbf{Z}_p^3$ that is the wreath product of a circulant graph of order p over a Cayley graph of $\mathbf{Z}_p^3$ or the wreath product of a Cayley graph of $\mathbf{Z}_p^3$ over a circulant graph of order p, then Γ is a CI-graph with respect to $\mathbf{Z}_p^3$.*

Proof. We will show that if Γ is a Cayley graph of $\mathbf{Z}_p^3$ and Γ is isomorphic to a wreath product of a circulant graph Γ_1 of order p over a Cayley graph Γ_2 of $\mathbf{Z}_p^3$, then Γ is a CI-graph. The other case follows with a similar argument.

Let $\Gamma \cong \Gamma_1 \wr \Gamma_2$ be as above. Let Γ' be a Cayley graph of $\mathbf{Z}_p^3$ such that Γ' is isomorphic to Γ. Let $\tau_1, \tau_2, \tau_3 : \mathbf{Z}_p^3 \to \mathbf{Z}_p^3$ by $\tau_1(i,j,k) = (i+1, j, k)$, $\tau_2(i,j,k) = (i, j+1, k)$, and $\tau_3(i,j,k) = (i,j,k+1)$. Then $G = \langle \tau_1, \tau_2, \tau_3 \rangle \leqslant \mathrm{Aut}(\Gamma)$, $G \leqslant \mathrm{Aut}(\Gamma')$, and $G \cong \mathbf{Z}_p^3$. Let Π be a Sylow p-subgroup of $\mathrm{Aut}(\Gamma)$ that contains G. Then Π has a nontrivial center so there exists $\alpha \in \mathrm{C}(\Pi)$, the center of Π, $\alpha \neq 1$. As $\alpha \in \mathrm{C}(\Pi)$, $\alpha \in \mathrm{C}_{S_{\mathbf{Z}_p^3}}(G)$, the centralizer of G in $S_{\mathbf{Z}_p^3}$, and as G is regular and abelian, $\alpha \in G$. Now, Π admits a complete block system $\mathscr{B}$ of p^2 blocks of size p, where the blocks of size p are formed by the orbits of α. Define $\pi_1 : \Pi \to S_{\mathbf{Z}_p^3/\mathscr{B}}$ by $\pi_1(\gamma) = \gamma/\mathscr{B}$. Then $\Pi/\mathscr{B}$ is a p-group and there exists $\beta \in \Pi$ such that $\beta/\mathscr{B} \in \mathrm{C}(\Pi/\mathscr{B})$, $\beta\mathscr{B} \neq 1$. As $G/\mathscr{B} \leqslant \Pi/\mathscr{B}$, $\beta/\mathscr{B} \in G/\mathscr{B}$, so that $\beta = \beta'\omega$, $\beta' \in G$, $\omega \in \mathrm{Ker}(\pi_1)$. Hence we may assume without loss of generality that $\beta \in G$. Then Π admits a complete block system $\mathscr{C}$ of p blocks of size p^2, where the elements of $\mathscr{C}$ are formed by the orbits of $\langle \alpha, \beta \rangle$. Define $\pi_2 : \Pi \to S_p$ by $\pi_2(\gamma) = \gamma/\mathscr{C}$. Then $|\Pi/\mathscr{C}| = p$, and if $\gamma \in \Pi$ such that $\gamma/\mathscr{C} \neq 1$, then $\gamma = \gamma'\omega'$, $\gamma' \in G$, $\omega' \in \mathrm{Ker}(\pi_2)$. Thus we assume that $\gamma \in G$. Hence $\langle \alpha, \beta, \gamma \rangle = \langle \tau_3, \tau_2, \tau_1 \rangle$ and so by [4] there exists $\delta_1 \in \mathrm{Aut}(\mathbf{Z}_p^3)$ so that $\delta_1^{-1}\alpha\delta_1 = \tau_3$, $\delta_1^{-1}\beta\delta_1 = \tau_2$, and $\delta_1^{-1}\gamma\delta_1 = \tau_1$. Further, Γ is a CI-graph if and only if $\delta_1(\Gamma)$ is a CI-graph, and as $\langle \alpha|_C, \beta|_C : C \in \mathscr{C} \rangle \leqslant \Pi$, $\delta_1(\Gamma)$ is the wreath product of an order p-circulant Γ_1' over a Cayley graph Γ_2' of $\mathbf{Z}_p^3$. As $\mathbf{Z}_p^3$ is a CI-group with respect to graphs [7], clearly there exists $\delta_2 \in \mathrm{Aut}(\mathbf{Z}_p^3)$ such that $\delta_2\delta_1(\Gamma) = \Gamma_1 \wr \Gamma_2$. By analogous arguments, there exist $\delta_1', \delta_2' \in \mathrm{Aut}(\mathbf{Z}_p^3)$ so that $\delta_2'\delta_1'(\Gamma') = \Gamma_1 \wr \Gamma_2$ so that $\delta_1'^{-1}\delta_2'^{-1}\delta_2\delta_1(\Gamma) = \Gamma'$. Hence Γ is a CI-graph for $\mathbf{Z}_p^3$. □

Theorem 4. *Z_p^3 is a CI-group with respect to graphs.*

Proof. Let Γ and Γ' be isomorphic Cayley graphs for Z_p^3, and $\varphi:\Gamma \to \Gamma'$ an isomorphism. Let τ_1, τ_2, τ_3 and G be as in Lemma 3. We must show that there exists $\delta \in \mathrm{Aut}(Z_p^3)$ such that $\delta(\Gamma) = \Gamma'$ or that $\varphi^{-1}G\varphi$ and G are conjugate in $\mathrm{Aut}(\Gamma)$. Now, G and $\varphi^{-1}G\varphi$ are contained in Sylow p-subgroups Π and Π', respectively, of $\mathrm{Aut}(\Gamma)$, and so there exists $\gamma \in \mathrm{Aut}(\Gamma)$ such that $\gamma^{-1}\varphi^{-1}G\varphi\gamma \leqslant \Pi$. As Π is a p-group, there exists $\alpha \in \mathrm{C}(\Pi)$, $\alpha \neq 1$, and by arguments in Lemma 3, we may assume $\alpha \in G$. Hence Π admits a complete block system $\mathscr{B}$ of p^2 blocks of size p, where the elements of $\mathscr{B}$ are the orbits of α. Define π_1 as in Lemma 3. By Lemma 2, $|\mathrm{Ker}(\pi_1)| = p$, p^p, or p^{p^2}. If $|\mathrm{Ker}(\pi_1)| = p^{p^2}$, then $\mathrm{Ker}(\pi_1) = \langle \alpha|_B\colon B \in \mathscr{B}\rangle$ and Γ is isomorphic to the wreath product of a Cayley graph of Z_p^3 over an order p-circulant. Thus by Lemma 3, there exists $\delta \in \mathrm{Aut}(Z_p^3)$ such that $\delta(\Gamma) = \Gamma'$. We therefore assume that $|\mathrm{Ker}(\pi_1)| = p$ or p^p.

If $|\mathrm{Ker}(\pi_1)| = p^p$, then by Lemma 2 Π admits a complete block system $\mathscr{C}$ of p blocks of size p^2, where if $C \in \mathscr{C}$, then there exists $\alpha_C \in \mathrm{Ker}(\pi_1)$ such that $\alpha_C(c) \neq c$ for all $c \in C$ and $\alpha_C(d) = d$ for all $d \in Z_p^3 - C$. Define π_2 as in Lemma 3. Clearly $\mathscr{C}$ is also a complete block system for G, and $|G/\mathscr{C}| = p$. Hence there exists $\beta \in G$ such that $\beta/\mathscr{C} = 1$ but $\beta \notin \langle\alpha\rangle$. Thus $\mathscr{C}$ is formed by the orbits of $\langle\alpha, \beta\rangle$. Further, $\Pi/\mathscr{C} = G/\mathscr{C}$ so there exists $\gamma \in \Pi$ such that $\gamma/\mathscr{C}$ is semiregular, $\gamma/\mathscr{C} \in G/\mathscr{C}$. By the arguments above, we assume $\gamma \in G$. Then $\langle\alpha, \beta, \gamma\rangle = G$ and by the arguments in Lemma 3 we may assume that $\alpha = \tau_3$, $\beta = \tau_2$, and $\gamma = \tau_1$.

Now, $|\Pi/\mathscr{B}| = p^2$ or $|\Pi/\mathscr{B}| > p^2$. If $|\Pi/\mathscr{B}| > p^2$, then as the elements of $\mathscr{C}$ are formed by the orbits of $\langle\tau_2, \tau_3\rangle$, $\tau_2(C) = C$ for all $C \in \mathscr{C}$. Hence $\mathrm{Ker}(\pi_1) = \langle\tau_3|_C\colon C \in \mathscr{C}\rangle$. Let $C_i = \{(i,j,k)\colon j,k \in Z_p\}$ and $B_{i,j} = \{(i,j,k)\colon k \in Z_p\}$. Then $\mathscr{C} = \{C_i\colon i \in Z_p\}$ and $\mathscr{B} = \{B_{i,j}\colon i,j \in Z_p\}$. Suppose that some vertex of $B_{i,a}$ is adjacent to some vertex of $B_{j,b}$, $i \neq j$. Then every vertex of $B_{i,a}$ is adjacent to every vertex of $B_{j,b}$. As $|\Pi/\mathscr{B}| > p^2$, there exists $\beta \in \Pi$ such that $\beta|_{C_c}/\mathscr{B} = 1$ and $\beta|_{C_d}/\mathscr{B} \neq 1$, $c \neq d$. As p is prime, we may assume that $c - d \equiv i - j \bmod p$, and by conjugating by τ_1, if necessary, that $c = i$ and $d = j$. As $\beta|_{C_i}/\mathscr{B} \neq 1$, $\beta|_{C_i}/\mathscr{B}$ is a p-cycle on the blocks $\{B_{i,k}\colon k \in Z_p\}$, and as $\beta|_{C_j}/\mathscr{B} = 1$, β fixes each block $B_{j,k}$, $k \in Z_p$. Thus every vertex of $B_{i,a}$ is adjacent to every vertex of C_j, and by symmetry, every vertex of C_i is adjacent to every vertex of C_j. We conclude that Γ is the wreath product of an order p-circulant over a Cayley graph of Z_p^2, and so Γ is a CI-graph for Z_p^3.

If $|\Pi/\mathscr{B}| = p^2$, then $\mathrm{Ker}(\pi_1) = \langle\tau_3|_C\colon C \in \mathscr{C}\rangle$, and so if $\varphi_1 = \varphi\gamma$, then $\varphi_1^{-1}\mathscr{C}\varphi_1 = \mathscr{C}$. Hence $\varphi_1(i,j,k) = (\sigma(i), \xi_i(j,k))$, $\sigma \in S_p$, $\xi_i \in S_{Z_p^2}$. As $\mathrm{Ker}(\pi_2)|_C \cong Z_p^2$ for all $C \in \mathscr{C}$, $\xi_i(j,k) = \omega_i(j,k) + (a_i, b_i)$, $\omega_i \in \mathrm{Aut}(Z_p^2)$, a_i, $b_i \in Z_p$. As $\omega_i \in \mathrm{Aut}(Z_p^2)$,

$$\omega_i(j,k) = (\alpha_i j + \beta_i k, \gamma_i k + \iota_i j),$$

$\alpha_i, \beta_i, \gamma_i, \iota_i \in Z_p$, where the 2×2 matrix with first row $\alpha_i\ \beta_i$ and second row $\gamma_i\ \iota_i$ has nonzero determinant. If $\beta_i \neq 0$ for any i, then, as $\mathrm{Ker}(\pi_1) = \langle\tau_3|_C\colon C \in \mathscr{C}\rangle$, $|\Pi/\mathscr{B}| > p^2$, so $\beta_i = 0$ for all $i \in Z_p$. As $\mathrm{Aut}(\Gamma') = \varphi_1^{-1}\,\mathrm{Aut}(\Gamma)\varphi_1$, we conclude that

$\mathrm{Ker}(\pi_1) \leqslant \mathrm{Aut}(\Gamma')$ and so we may assume (by right multiplication by elements of $\mathrm{Ker}(\pi_1)$) that $b_i = 0$ for all $i \in \mathbf{Z}_p$. We now show that $\alpha_i = \alpha_j$ for all $i,j \in \mathbf{Z}_p$.

As $|\Pi/\mathscr{C}| = p$, $\sigma(i) = ri + c$, $r \in \mathbf{Z}_p^*$, $c \in \mathbf{Z}_p$, and as $\tau_1 \in \mathrm{Aut}(\Gamma')$, we may assume that $\sigma(i) = ri$. Hence

$$\varphi_1(i,j,k) = (ri, \alpha_i j + a_i, \gamma_i k + \iota_i j),$$

and so

$$\varphi_1^{-1}(i,j,k) = (r^{-1}i, \alpha_{r^{-1}i}^{-1}(j - a_{r^{-1}i}), \gamma_{r^{-1}i}^{-1}k - \gamma_{r^{-1}i}^{-1}\iota_{r^{-1}i}j).$$

Hence if $\tau = \tau_1^{-r^{-1}}\varphi_1^{-1}\tau_1\varphi_1$, then $\tau \in \mathrm{Ker}(\pi_2)$ and

$$\tau(i,j,k) = (i, \alpha_{i+r^{-1}}^{-1}\alpha_i j + c_i, \theta_i(j,k)),$$

for some $c_i \in \mathbf{Z}_p$ and $\theta_i : \mathbf{Z}_p^2 \to \mathbf{Z}_p$. Now, $|\tau| = p^t$, $t \geqslant 0$, and $|\mathbf{Z}_p^*| = p - 1$, so that $\alpha_{i+r^{-1}}^{-1}\alpha_i = 1$. Hence $\alpha_i = \alpha_{i+r^{-1}}$, and as $\langle r^{-1} \rangle = \mathbf{Z}_p$, $\alpha_i = \alpha_j$ for all $i,j \in \mathbf{Z}_p$.

Let $\alpha = \alpha_0$. Then

$$\tau(i,j,k) = (i, j + \alpha^{-1}(a_i - a_{i+r^{-1}}), \theta_i(j,k)).$$

As $|\Pi/\mathscr{B}| = p^2$, $\alpha^{-1}(a_i - a_{i+r^{-1}}) = c$, $c \in \mathbf{Z}_p$, so $a_{i+r^{-1}} = a_i - \alpha c$. As $\tau_2 \in \mathrm{Aut}(\Gamma')$, we may assume that $a_0 = 0$ and so $a_{ir^{-1}} = -i\alpha c$. Hence $a_i = -ir\alpha c$. Define $\phi : \mathbf{Z}_p^3 \to \mathbf{Z}_p^3$ by $\phi(i,j,k) = (i, j - ir\alpha c, k)$. Then $\phi \in \mathrm{Aut}(\mathbf{Z}_p^3)$, and if $\varphi'_1 = \varphi_1\phi$, we may assume without loss of generality (by replacing Γ' by $\phi^{-1}(\Gamma')$) that $c = 0$ and $\varphi_1 = \varphi'_1$. Hence $a_i = a_{i+r}$, and as $\langle r^{-1} \rangle = \mathbf{Z}_p$,

$$\varphi_1(i,j,k) = (ri, \alpha j + a, \gamma_i k + \iota_i j).$$

As $\tau_2 \in \mathrm{Aut}(\Gamma')$, we may assume that $a = 0$. Now, elementary calculations will show that

$$\theta_i(j,k) = \gamma_{i+r^{-1}}^{-1}\gamma_i k + \gamma_{i+r^{-1}}^{-1}(\iota_i - \iota_{i+r^{-1}})j.$$

Further, $\tau \in \mathrm{Ker}(\pi_1)$ and so $\theta_i \in \langle \tau_3|_C : C \in \mathscr{C} \rangle$. Thus $\theta_i(j,k) = k + c_i$, $c_i \in \mathbf{Z}_p$. Hence for $k = 0$,

$$(\iota_i - \iota_{i+r^{-1}})j = \gamma_{i+r^{-1}}c_i$$

for all $j \in \mathbf{Z}_p$. We conclude that $\iota_i = \iota_{i+r^{-1}}$ for all $i \in \mathbf{Z}_p$, and so $\iota_i = \iota_j$ for all $i,j \in \mathbf{Z}_p$. Let $\iota = \iota_0$. Then $\theta_i(j,k) = \gamma_{i+r^{-1}}^{-1}\gamma_i k$, and as $|\theta_i| = p$, $\gamma_{i+r^{-1}}^{-1}\gamma_i = 1$ for all $i \in \mathbf{Z}_p$. Hence $\gamma_i = \gamma_j$ for all $i,j \in \mathbf{Z}_p$. Thus if $\gamma = \gamma_0$, then

$$\varphi_1(i,j,k) = (ri, \alpha j, \gamma k + \iota j),$$

and so $\varphi_1 \in \mathrm{Aut}(\mathbf{Z}_p^3)$. Hence Γ and Γ' are isomorphic by $\varphi_1 \in \mathrm{Aut}(\mathbf{Z}_p^3)$ and so Γ is a CI-graph.

If $|\mathrm{Ker}(\pi_1)| = p$, then $|\Pi/\mathscr{B}| = p^2$ or $|\Pi/\mathscr{B}| > p^2$. If $|\Pi/\mathscr{B}| = p^2$, then $|\Pi| = p^3$ so that G and $\varphi^{-1}G\varphi$ are conjugate in $\mathrm{Aut}(\Gamma)$ and so Γ is a CI-graph. If $|\Pi/\mathscr{B}| > p^2$, by the arguments in Lemma 3, there exist $\beta, \gamma \in G$ so that $\langle \alpha, \beta, \gamma \rangle = G$, and Π admits a complete block system $\mathscr{C}$ of p blocks of size p^2, where the elements of $\mathscr{C}$ are formed by the orbits of $\langle\alpha,\beta\rangle$. Also by arguments in Lemma 3, we assume without loss of generality that $\alpha=\tau_3$, $\beta=\tau_2$, and $\gamma=\tau_1$.

If $\mathrm{Ker}(\pi_2)|_C=\langle\tau_2,\tau_3\rangle|_C$, then if $\omega\in\mathrm{Ker}(\pi_2)$, $\omega(i,j,k)=(i,j+a_i,k+b_i)$, $a_i,b_i\in \boldsymbol{Z}_p$. Thus if $\omega\in\Pi$, $\omega(i,j,k)=(i+s,j+a_i,k+b_i)$, $s\in\boldsymbol{Z}_p$, and so

$$\gamma\tau_2(i,j,k)=(i+s,j+1+a_i,k+b_i)=\tau_2\gamma(i,j,k).$$

Hence $\tau_2\in \mathrm{C}(\Pi)$, and Π admits a complete block system $\mathscr{B}_\rho$ of p^2 blocks of size p, where $\mathscr{B}_\rho$ is formed by the orbits of $\rho\in\langle\tau_2,\tau_3\rangle$. Define $\pi_\rho:\Pi\to S_{\boldsymbol{Z}_p^3/\mathscr{B}_\rho}$ by $\pi_\rho(\gamma)=\gamma/\mathscr{B}_\rho$. If $|\mathrm{Ker}(\pi_\rho)|>p$ for any $\rho\in\langle\tau_2,\tau_3\rangle$, then by the arguments above Γ is a CI-object for $\boldsymbol{Z}_p^3$. We now show that such a ρ always exists.

As $|\mathrm{Ker}(\pi_1)|=p$, Γ is not isomorphic to a wreath product of a circulant graph of order p over a Cayley graph for $\boldsymbol{Z}_p^2$. Let $\alpha\in\Pi$ such that $\alpha/\mathscr{B}\neq 1$ but $\alpha/\mathscr{B}$ fixes some block $B\in\mathscr{B}$. Such an α exists as $|\Pi/\mathscr{B}|>p^2$. Without loss of generality, assume that $\alpha(B_{0,0})=B_{0,0}$. Then $\alpha|_{B_{0,0}}\in\langle\tau_3|_{B_{0,0}}\rangle$. Hence there exists $s\in\boldsymbol{Z}_p$ such that $\alpha\tau_3^s(0,0,0)=(0,0,0)$, so we assume that $\alpha(0,0,0)=(0,0,0)$. Hence $\alpha(0,j,k)=(0,j,k)$ for all $j,k\in\boldsymbol{Z}_p$. Let T be the connection set of Γ. As Γ is not isomorphic to a wreath product of an order p-circulant over a Cayley graph of $\boldsymbol{Z}_p^2$, there exists $i\in\boldsymbol{Z}_p$ such that $C_i\cap T\neq\emptyset$ but $C_i\nsubseteq T$. Further, as $\alpha/\mathscr{B}\neq 1$, there exists $j\in\boldsymbol{Z}_p$ such that $\alpha|_{C_{i,j}}=1$ but $\alpha|_{C_{i(j+1)}}\neq 1$. Let $\rho\in\langle\tau_2,\tau_3\rangle$ such that $\alpha|_{C_{i(j+1)}}=\rho|_{C_{i(j+1)}}$, and denote the orbits of $\rho|_{C_i}$ by $\mathscr{O}_0,\mathscr{O}_1,\dots,\mathscr{O}_{p-1}$. Then if $(0,0,0)$ is adjacent to $(i,j,k)\in\mathscr{O}_\ell$, then $(0,0,0)$ is adjacent to every vertex of $\mathscr{O}_\ell$. Observe that if $\tau\in\langle\tau_2,\tau_3\rangle$ such that $\tau\notin\langle\rho\rangle$, then each orbit of $\tau|_{C_k}$ contains exactly one element of each orbit of $\rho|_{C_k}$ for all $k\in\boldsymbol{Z}_p$. We conclude that $\alpha|_{C_{i(j+2)}}\in\langle\rho\rangle|_{C_{i(j+2)}}$, or $C_i\subseteq T$. As $C_i\nsubseteq T$, $\alpha|_{C_{i(j+2)}}\in\langle\rho\rangle|_{C_{i(j+2)}}$. Arguing similarly, we have that $\alpha|_{C_{i(j+3)}}\in\langle\rho\rangle|_{C_{i(j+3)}}$. Continuing in this fashion, we have that $\alpha|_{C_{ik}}\in\langle\rho\rangle|_{C_{ik}}$ for all $k\in\boldsymbol{Z}_p$, and so that $\alpha/\mathscr{B}_\rho=1$. As $\alpha\neq\rho$, $|\mathrm{Ker}(\pi_\rho)|>p$.

If $\mathrm{Ker}(\pi_2)|_C\neq\langle\tau_2,\tau_3\rangle|_C$, let $\alpha\in\mathrm{Ker}(\pi_2)$ such that $\alpha|_C\notin\langle\tau_2,\tau_3\rangle$. Consider $\alpha^{-1}\tau_2\alpha$. As $\Pi/\mathscr{B}\leqslant S_{\boldsymbol{Z}_p^2}$, $\Pi/\mathscr{B}$ is contained in a Sylow p-subgroup of $S_{\boldsymbol{Z}_p^2}$, which is isomorphic to $C_p\wr C_p$, where C_p is a cyclic group of order p. Hence $\langle\tau_2,\alpha\rangle/\mathscr{B}\leqslant 1_{S_p}\wr C_p$. As $1_{S_p}\wr C_p$ is an abelian group, $\alpha^{-1}\tau_2\alpha/\mathscr{B}=\tau_2/\mathscr{B}$. Thus $\alpha^{-1}\tau_2\alpha\tau_2^{-1}\in\mathrm{Ker}(\pi_2)$ and so $\alpha^{-1}\tau_2\alpha=\tau_2\tau_1^a$, $a\in\boldsymbol{Z}_p$. We conclude that $\alpha(i,j,k)=(i,\theta_i(j,k))$, where

$$\theta_i(j,k)=\omega_i(j,k)+(a_i,b_i),$$

$\omega_i\in\mathrm{Aut}(\boldsymbol{Z}_p^2)$, $a_i,b_i\in\boldsymbol{Z}_p$. Let $\beta_i:\boldsymbol{Z}_p^2\to\boldsymbol{Z}_p^2$ by $\beta_i(j,k)=(j+a_i,k+b_i)$. Then $\theta_i=\beta_i\omega_i$. Let, ω, $\beta:\boldsymbol{Z}_p^3\to\boldsymbol{Z}_p^3$ by $\omega(i,j,k)=(i,\omega_i(j,k))$ and $\beta(i,j,k)=(i,\beta_i(j,k))$. Then $\alpha=\beta\omega$ and so

$$\alpha^{-1}\tau_2\alpha=\omega^{-1}\beta^{-1}\tau_2\beta\omega=\omega^{-1}\tau_2\omega=\tau_2\tau_1^a,$$

where $a\in\boldsymbol{Z}_p$. Hence $\omega_i=\omega_j$ for all $i,j\in\boldsymbol{Z}_p$. Without loss of generality assume that $a_0=0$ and $b_0=0$. We will consider when $\alpha\in\mathrm{Aut}(\boldsymbol{Z}_p^3)$ and when $\alpha\notin\mathrm{Aut}(\boldsymbol{Z}_p^3)$.

If $\alpha\notin\mathrm{Aut}(\boldsymbol{Z}_p^3)$, then $\alpha^{-1}\tau_1\alpha\notin\langle\tau_1,\tau_2,\tau_3\rangle$. Further, note that

$$\alpha_1(i,j,k)=\tau_1^{-1}\alpha^{-1}\tau_1\alpha(i,j,k)=(i,(j,k))+\omega^{-1}((a_i,b_i)-(a_{i+1},b_{i+1})). \tag{1}$$

As $\alpha \notin \mathrm{Aut}(\boldsymbol{Z}_p^3)$, $\alpha_1 \notin \langle \tau_1, \tau_2, \tau_3 \rangle$. Let $H = \langle \tau_1, \tau_2, \tau_3, \alpha_1 \rangle$. Note that $\mathscr{B}$ and $\mathscr{C}$ are still complete block systems for $H \leqslant \Pi$. Define $\pi'_1 : H \to S_{\boldsymbol{Z}_p^2}$ by $\pi'_1(\delta) = \delta/\mathscr{B}$ and $\pi'_2 : H \to S_p$ by $\pi'_2(\delta) = \delta/\mathscr{C}$. Then $\mathrm{Ker}(\pi'_1) \leqslant \mathrm{Ker}(\pi_1) = \langle \tau_3 \rangle$ so that $\mathrm{Ker}(\pi'_1) = \langle \tau_3 \rangle$. As $|H| \geqslant p^4$ and $|\mathrm{Im}(\pi'_2)| = p$, $|\mathrm{Ker}(\pi'_2)| \geqslant p^3$. By (1), $\mathrm{Ker}(\pi'_2)|_C \leqslant \langle \tau_2, \tau_3 \rangle|_C$ for all $C \in \mathscr{C}$, and so by the arguments above there exists $\rho \in H \cap \langle \tau_2, \tau_3 \rangle$ such that if $\pi'_\rho : H \to S_{\boldsymbol{Z}_p^2}$ by $\pi'_\rho(\delta) = \delta/\mathscr{B}_\rho$ ($\mathscr{B}_\rho$ being the orbits of ρ), then $|\mathrm{Ker}(\pi'_\rho)| > p$. By Lemma 2, $\mathrm{Ker}(\pi'_\rho)| = p^{p^2}$ or p^p. If $|\mathrm{Ker}(\pi'_\rho)| = p^{p^2}$, then Γ is isomorphic to the wreath product of a Cayley graph of $\boldsymbol{Z}_p \times \boldsymbol{Z}_p$ over an order p-circulant, and so by Lemma 3, Γ is a CI-graph. If $|\mathrm{Ker}(\pi'_\rho)| = p^p$, then by Lemma 2 $\langle \rho|_C : C \in \mathscr{C} \rangle \leqslant \mathrm{Aut}(\Gamma)$. Further, $\rho \in \langle \tau_2, \tau_3 \rangle$ and $\rho \notin \langle \tau_3 \rangle$, so that $\rho = \tau_2^b \tau_1^c$, b, $c \in \boldsymbol{Z}_p$, $a \neq 0$. Thus ρ permutes the blocks of $\mathscr{B}$ as a p-cycle.

Now, $(\alpha|_{C_i})/\mathscr{B} \in \langle \tau_2|_{C_i} \rangle/\mathscr{B}$ for all $i \in \boldsymbol{Z}_p$. Let $d_i \in \boldsymbol{Z}_p$ such that $(\alpha|_{C_i})/\mathscr{B} = \tau_2^{d_i}/\mathscr{B}$. Let $f_0, f_1, \ldots, f_{p-1} \in \boldsymbol{Z}_p$ such that $f_i a = d_i$. Then

$$(\alpha \textstyle\prod_{i=0}^{p-1} \rho^{-f_i}|_{C_i})/\mathscr{B} = 1.$$

Let $\alpha' = \alpha \prod_{i=0}^{p-1} \rho^{-f_i}$. As $\alpha|_C \notin \langle \tau_2, \tau_3 \rangle|_C$ for some $C \in \mathscr{C}$ and $\rho^{-f_i}|_C \in \langle \tau_2, \tau_3 \rangle$ for all i, $\alpha'|_C \notin \langle \tau_2, \tau_3 \rangle$ and thus $\alpha' \notin \langle \tau_3 \rangle$ but $\alpha' \in \mathrm{Ker}(\pi_1)$, a contradiction. Hence $\alpha \in \mathrm{Aut}(\boldsymbol{Z}_p^3)$.

If $\alpha \in \mathrm{Aut}(\boldsymbol{Z}_p^3)$, then $\Pi \leqslant \mathrm{AGL}_3(p)$, the affine group over the field with p^3 elements. As is well known, this group is doubly transitive and, by [9, Theorem 11.5], $G = \langle \tau_1, \tau_2, \tau_3 \rangle$ is the only minimal normal subgroup of $\mathrm{AGL}_3(p)$, and also of Π. Thus $\varphi_1^{-1} G \varphi_1 = G$ and Γ is a CI-graph of $\boldsymbol{Z}_p^3$. □

It does not appear that this approach will generalize to determine whether a given Cayley graph of $\boldsymbol{Z}_p^k$ is a CI-graph for all $k \geqslant 1$. It may, however, generalize to $k = 4$ and, possibly, $k = 5$.

Several people have recently informed the author that the main result of this paper, Theorem 4, was independently obtained by Xu [10]. Our proof, however, seems to be both more combinatorial and more elementary.

Acknowledgements

The author would very much like to thank the referees for their obvious careful reading of this manuscript, and their many suggestions for improvements in the paper.

References

[1] B. Alspach and T.D. Parsons, Isomorphisms of circulant graphs and digraphs, Discrete Math. 24 (1979) 97–108.

[2] L. Babai, Isomorphism problem for a class of point-symmetric structures, Acta Math. Sci. Acad. Hung. 29 (1977) 329–336.

[3] L. Babai and P. Frankl, Isomorphisms of Cayley graphs I, in Colloq. Math. Soc. J. Boyai, 18 Combinatorics, Keszthely, 1976 (North-Holland, Amsterdam, 1978) 25–52.
[4] H.S.M. Coxseter and W.O.T. Moser, Generators and Relations for Discrete Groups (Springer, New York, 1965).
[5] D.Ž. Djoković, Isomorphism problem for a special class of graphs, Acta Math. Sci. Acad. Hung. 21 (1971) 267–270.
[6] B. Elpas and J. Turner, Graphs with circulant adjacency matrices, J. Combin. Theory 9 (1970) 297–307.
[7] C.D. Godsil, On Cayley graph isomorphisms, Ars Combin. 15 (1983) 231–246.
[8] L.A. Nowitz, A non-Cayley-invariant Cayley graph of the elementary Abelian group of order 64, Discrete Math. 110 (1992) 223–228.
[9] H. Wielandt, Finite Permutation Groups (Academic Press, New York, 1964) x, 114.
[10] M.Y. Xu, On isomorphism of Cayley digraphs and graphs of groups of order p^3, submitted.