Also available at http://amc-journal.eu
ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 8 (2015) 433–444

The Cayley isomorphism property for groups of order $8p$

Gábor Somlai *
Eötvös Loránd University, Department of Algebra and Number Theory, 1117 Pázmány Péter sétány 1/C , Budapest, Hungary

Received 31 December 2013, accepted 10 September 2014, published online 26 June 2015

Abstract

For every prime $p > 3$ we prove that $Q \times \mathbb{Z}_p$ is a DCI-group, where Q denotes the quaternion group of order 8. Using the same method we reprove the fact that $\mathbb{Z}_2^3 \times \mathbb{Z}_p$ is a CI-group for every prime $p > 3$, which was obtained in [3]. This result completes the description of CI-groups of order $8p$.

Keywords: Cayley graphs, CI-groups.

Math. Subj. Class.: 05C25

1 Introduction

Let G be a finite group and S a subset of G. The Cayley graph $Cay(G, S)$ is defined by having the vertex set G and g is adjacent to h if and only if $g^{-1}h \in S$. The set S is called the connection set of the Cayley graph $Cay(G, S)$. A Cayley graph $Cay(G, S)$ is undirected if and only if $S = S^{-1}$, where $S^{-1} = \{ s^{-1} \in G \mid s \in S \}$. Every left multiplication via elements of G is an automorphism of $Cay(G, S)$, 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.

Similarly to Cayley graphs one can also define ternary Cayley relational structures. $(V, E_1, E_2, \ldots, E_l)$ is a colour ternary relational structure if $E_i \subset V^3$ for $i = 1, \ldots, l$. We say that a colour ternary relational structure $(V, E_1, \ldots, E_l)$ is a Cayley ternary relational structure of the group G if the automorphism group of $(V, E_1, \ldots, E_l)$ contains a regular subgroup isomorphic to G.

It is clear that $Cay(G, S) \cong Cay(G, \mu(S))$ for every $\mu \in Aut(G)$. A Cayley graph $Cay(G, S)$ is said to be a CI-graph if, for each $T \subset G$, the Cayley graphs $Cay(G, S)$

*Research supported by the Hungarian Scientific Fund (OTKA), grant no. K84233
E-mail address: gsomlai@cs.elte.hu (Gábor Somlai)

and $Cay(G,T)$ are isomorphic if and only if there is an automorphism μ of G such that $\mu(S) = T$. 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.

Similarly, a group G is called a CI-group with respect to colour ternary relational structures, if for any pair of isomorphic colour ternary relational structures of G there exists an isomorphism induced by an automorphism of G.

Let G be a CI-group of order $8p$, where p is an odd prime. It is easy to verify that $\mathbb{Z}_2 \times \mathbb{Z}_4$ and the dihedral group of order 8 are not CI-groups. It can easily be seen that every subgroup of a CI-group is also a CI-group. Therefore the Sylow 2-subgroup of G can only be $\mathbb{Z}_8$, $\mathbb{Z}_2^3$ or the quaternion group Q of order 8.

It was proved by Li, Lu and Pálfy [5, Theorem 1.2 (b)] that a finite CI-group of order $8p$ containing an element of order 8 can only be

$$H = \left\langle a, z \mid a^p = 1, z^8 = 1, z^{-1}az = a^{-1} \right\rangle.$$

It was also shown in [5, Theorem 1.3] that H is a CI-group, though not a DCI-group. In view of these results, for the rest of the discussion, we assume that the Sylow 2-subgroup of G is isomorphic to Q or $\mathbb{Z}_2^3$.

It was proved by Dobson [2] that $\mathbb{Z}_2^3 \times \mathbb{Z}_p$ is a CI-group with respect to ternary relational structures if $p \geq 11$. Moreover, Dobson and Spiga [3] proved that $\mathbb{Z}_2^3 \times \mathbb{Z}_p$ is a DCI-group with respect to colour ternary relational structures if and only if $p \neq 3$ and 7. As a consequence of this result it was proved in [3] that $\mathbb{Z}_2^3 \times \mathbb{Z}_p$ is a DCI-group for all primes p.

If $p > 8$ or $p = 5$, then by Sylow's Theorem the Sylow p-subgroup of G is a normal subgroup, therefore G is isomorphic to one of the following groups: $\mathbb{Z}_2^3 \times \mathbb{Z}_p$, $Q \times \mathbb{Z}_p$, $\mathbb{Z}_2^3 \ltimes \mathbb{Z}_p$ or $Q \ltimes \mathbb{Z}_p$. It can also be seen from [5, Theorem 1.2] that neither $Q \ltimes \mathbb{Z}_p$ nor $\mathbb{Z}_2^3 \ltimes \mathbb{Z}_p$ is a CI-group.

If $p = 7$, then either the Sylow 7-subgroup is normal, in which case G is as before, or G has 8 Sylow 7-subgroups and the Sylow 2-subgroup of G is normal. Then the Sylow 7-subgroup of G acts transitively by conjugation on the the non-identity elements of the Sylow 2-subgroup. Hence $G \cong \mathbb{Z}_2^3 \rtimes \mathbb{Z}_7$, which is not a CI-group by [5, Theorem 1.2.(b)].

If $p = 3$, then the order of G is 24. A complete list of CI-groups of order at most 31 was given in the Ph.D. thesis of Royle, see [7]. The CI-groups of order 24 are the following: $Q \times \mathbb{Z}_3$, $\mathbb{Z}_8 \ltimes \mathbb{Z}_3$ and $\mathbb{Z}_2^3 \times \mathbb{Z}_3$.

Spiga [6] proved that $Q \times \mathbb{Z}_3$ is not a CI-group with respect to colour ternary relational structures.

Using different methods depending on whether $p > 8$, or $p = 5, 7$ we show that the other groups are DCI-groups. By extending our result with the fact that $\mathbb{Z}_2^3 \times \mathbb{Z}_3$ is a CI-group we get that $Q \times \mathbb{Z}_p$ is a CI-group for every odd prime p.

Theorem 1.1. For every prime $p \geq 3$ the group $Q \times \mathbb{Z}_p$ is a DCI-group.

We also prove the following result which was first obtained in [3].

Theorem 1.2 (Dobson, Spiga [3])**.** For every prime $p \geq 3$ the group $\mathbb{Z}_2^3 \times \mathbb{Z}_p$ 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 which are useful in the proof of Theorem 1.1 and 1.2. Section 4 contains the proof of Theorem 1.1 and 1.2 for primes $p > 8$ and Section 5 contains the proof of Theorem 1.1 and 1.2 for $p = 5$ and 7.

2 Technical details

In this section we introduce some notation. Let G be a group. We use $H \leq G$ 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.

Let us assume that the group H acts on the set Ω and let G be an arbitrary group. Then by $G \wr_\Omega H$ we denote the wreath product of G and H. Every element $g \in G \wr_\Omega H$ can be uniquely written as hk, where $k \in K = \prod_{\omega \in \Omega} G_\omega$ and $h \in H$. The group $K = \prod_{\omega \in \Omega} G_\omega$ is called the base group of $G \wr_\Omega H$ and the elements of K can be treated as functions from Ω to G. If $g \in G \wr_\Omega H$ and $g = hk$ we denote k by $(g)_b$. In order to simplify the notation Ω 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 Ω will be denoted by $Sym(\Omega)$. Let G be a permutation group on the set Ω. For a G-invariant partition $\mathcal{B}$ of the set Ω we use $G^{\mathcal{B}}$ to denote the permutation group on $\mathcal{B}$ induced by the action of G and similarly, for every $g \in G$ we denote by $g^{\mathcal{B}}$ the action of g on the partition $\mathcal{B}$.

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

Definition 2.1. Let $G \leq Sym(\Omega)$ be a permutation group. Let

$$G^{(2)} = \left\{ \pi \in Sym(\Omega) \middle| \begin{array}{ll} \forall a, b \in \Omega\ \exists g_{a,b} \in G \text{ with} & \pi(a) = g_{a,b}(a) \text{ and} \\ & \pi(b) = g_{a,b}(b) \end{array} \right\}.$$

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

The following lemma is well-known and follows directly from the definition of $G^{(2)}$.

Lemma 2.2. *Let Γ be a graph. If $G \leq Aut(\Gamma)$, then $G^{(2)} \leq Aut(\Gamma)$.*

3 Basic ideas

In this section we collect some results and some important ideas that we will use in the proof of Theorem 1.1 and Theorem 1.2.

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

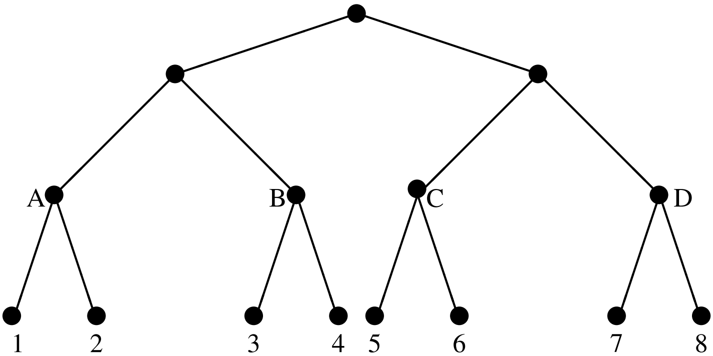
Lemma 3.1 (Babai [1]). *The Cayley graph $Cay(G, S)$ is a CI-graph if and only if for every regular subgroup $\mathring{G}$ of $Aut(Cay(G, S))$ isomorphic to G there is a $\mu \in Aut(Cay(G, S))$ such that $\mathring{G}^\mu = \hat{G}$.*

We introduce the following definition.

Definition 3.2. (a) We say that a Cayley graph $Cay(G, S)$ is a CI$^{(2)}$-graph if and only if for every regular subgroup $\mathring{G}$ of $Aut(Cay(G, S))$ isomorphic to G there is a $\sigma \in \langle \mathring{G}, \hat{G} \rangle^{(2)}$ such that $\mathring{G}^\sigma = \hat{G}$.

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

Let R be either Q or $\mathbb{Z}_2^3$. Let us assume that $A = Aut(Cay(G, S)) \leq Sym(8p)$ contains two copies of regular subgroups, $\mathring{R} \times \mathring{\mathbb{Z}}_p$ and $\hat{R} \times \hat{\mathbb{Z}}_p$. By Sylow's theorem we may assume that $\mathring{\mathbb{Z}}_p$ and $\hat{\mathbb{Z}}_p$ are in the same Sylow p-subgroup P of $Sym(8p)$. If $p > 8$, then P is isomorphic to $\mathbb{Z}_p^8$. Moreover, P is generated by 8 disjoint p-cycles. It follows that both $\mathring{R}$ and $\hat{R}$ normalize P so we may assume that $\mathring{R}$ and $\hat{R}$ lie in the same Sylow 2-subgroup of $N_A(P)$. Let P_2 denote a Sylow 2-subgroup of $Sym(8)$. It is also well known that P_2 is isomorphic to the automorphism group of the following graph Δ:



Every automorphism of Δ permutes the leaves of the graph and the permutation of the leaves determines the automorphism, therefore $Aut(\Delta)$ can naturally be embedded into $Sym(8)$.

Lemma 3.3. *(a) There are exactly two regular subgroups of P_2 which are isomorphic to Q.*

(b) There are exactly two regular subgroups of P_2 which are isomorphic to $\mathbb{Z}_2^3$.

Proof. (a) Let Q be a regular subgroup of $Aut(\Delta)$ isomorphic to the quaternion group with generators i and j. Since Q is regular, for every $1 \leq m \leq 4$ there is a $q_m \in Q$ (not necessarily distinct) such that $q_m(2m-1) = 2m$. These are automorphisms of Δ so $q_m(2m) = 2m-1$ and hence since Q is regular the order of q_m is 2. There is only one involution in Q so $q_m = i^2$ for every $1 \leq m \leq 4$ and this fact determines completely the action of i^2 on Δ. Note that the automorphisms q_m are all equal.

We can assume that $i(1) = 3$. Such an isomorphism of Δ fixes setwise $\{1, 2, 3, 4\}$ so we have that $i(3) = 2$, $i(2) = 4$ and $i(4) = 1$ since i is of order 4. Using again the fact that Q is regular on Δ and $i^2(5) = 6$, we get that there are two choices for the action of i: $i = (1324)(5768)$ or $i = (1324)(5867)$.

We can also assume that $j(1) = 5$. This implies that $j(5) = j^2(1) = i^2(1) = 2$, and $j(2) = 6$ since $j \in Aut(\Delta)$ and $j(6) = 1$. The action of i determines the action of j on Δ since $iji = j$. Applying this to the leaf 3 we get that $j(3) = 8$ if $i = (1324)(5768)$ and $j(3) = 7$ if $i = (1324)(5867)$ so there is no more choice for the action of j. Finally, i and j generate Q and this gives the result.

(b) One can prove this using an argument similar to the previous case.

□

The previous proof also gives the following.

Lemma 3.4. *(a) The following two pairs of permutations generate the two regular subgroups of $Aut(\Delta) \le Sym(8)$ isomorphic to Q:*

$$i_1 = (1324)(5768),\ j_1 = (1526)(3748) \text{ and}$$
$$i_2 = (1324)(5867),\ j_2 = (1526)(3847).$$

(b) The elements of these regular subgroups of $Aut(\Delta)$ are the following:

Q_l:		Q_r:	
id	(12)(34)(56)(78)	id	(12)(34)(56)(78)
(1324)(5768)	(1423)(5867)	(1324)(5867)	(1423)(5768)
(1526)(3847)	(1625)(3748)	(1526)(3748)	(1625)(3847)
(1728)(3546)	(1827)(3645)	(1728)(3645)	(1827)(3546)

Using the identification given in the following table, Q_l and Q_r act on Q by left-and right-multiplication with the elements of Q, respectively:

$\{1,\dots,8\}$	1	2	3	4	5	6	7	8
Q	1	-1	i	$-i$	j	$-j$	k	$-k$

(c) $A_1 = \langle x_1, x_2, x_3\rangle$ and $A_2 = \langle y_1, y_2, y_3\rangle$ are subgroups of $Aut(\Delta) \le Sym(8)$ isomorphic to $\mathbb{Z}_2^3$, where

$$x_1 = (12)(34)(56)(78),\ x_2 = (13)(24)(57)(68),\ x_3 = (15)(26)(37)(48) \text{ and}$$
$$y_1 = (12)(34)(56)(78),\ y_2 = (13)(24)(58)(67),\ y_3 = (15)(26)(38)(47).$$

Lemma 3.5. *Let us assume that $G_1 \le P_2$ is generated by two different regular subgroups Q_a and Q_b of $Aut(\Delta)$ which are isomorphic to Q and $G_2 \le P_2$ is generated by two different regular subgroups A_1 and A_2 of $Aut(\Delta)$ which are isomorphic to $\mathbb{Z}_2^3$. Then $G_1 = G_2$.*

Proof. It is clear that $|P_2| = |Aut(\Delta)| = 2^7$. One can see using Lemma 3.4 (a) and (c) that G_1 and G_2 are generated by even permutations. Both G_1 and G_2 induce an action on the set $V = \{A, B, C, D\}$ which is a set of vertices of Δ and it is easy to verify that every permutation of V induced by G_1 and G_2 is even. This shows that G_1 and G_2 are contained in a subgroup of P_2 of cardinality 2^5.

Lemma 3.4 (b) shows that $|Q_a \cap Q_b| = 2$ and one can also check using Lemma 3.4 (c) that $|A_1 \cap A_2| = 2$. This gives $|G_1| \ge 2^5$ and $|G_2| \ge 2^5$, finishing the proof of Lemma 3.5. □

Proposition 3.6. *(a) The quaternion group Q is a $DCI^{(2)}$-group.*

(b) The elementary abelian group $\mathbb{Z}_2^3$ is a $DCI^{(2)}$-group.

Proof. (a) Let Q_a and Q_b be two regular subgroups of $Sym(8)$ isomorphic to the quaternion group Q. By Sylow's theorem we may assume that Q_a and Q_b lie in the same Sylow 2-subgroup of $H = \langle Q_a, Q_b\rangle$. Since every Sylow 2-subgroup of H is contained in a Sylow 2-subgroup of $Sym(8)$, we may assume that Q_a and Q_b are subgroups of $Aut(\Delta)$.

Our aim is to find an element $\pi \in \langle Q_a, Q_b\rangle^{(2)}$ such that $Q_a^\pi = Q_b$. Let us assume that $Q_a \neq Q_b$. Using Lemma 3.4 (a) we may also assume that Q_a and Q_b are generated by the permutations $(1324)(5768), (1526)(3748)$ and $(1324)(5867), (1526)(3847)$, respectively. Lemma 3.4 (b) shows that H contains the following three permutations:

$$\begin{aligned}(12)(34) &= (1324)(5768)(1324)(5867)\\ (12)(56) &= (1526)(3748)(1526)(3847)\\ (12)(78) &= (1728)(3546)(1728)(3645).\end{aligned}$$

Now one can easily see that the permutation (12) is in $H^{(2)}$. Finally, it is also easy to check using Lemma 3.4 (b) that $Q_a^{(12)} = Q_b$.

(b) One can prove this statement using Lemma 3.4 and Lemma 3.5.

Definition 3.7. Let Γ 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 $A \nsim B$ if none of the previous four possibilities holds.

The following lemma follows easily:

Lemma 3.8. *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 a generator $\hat{g}$ of $\hat{\mathbb{Z}}_p$ acts by $\hat{g}(a_1, a_2) = (a_1 + 1, a_2 + 1)$ on $A \cup B$ and for a generator $\mathring{a}$ of the cyclic group $\mathring{\mathbb{Z}}_p$ the action of $\mathring{a}$ is defined by $\mathring{a}(a_1, a_2) = (a_1 + b, a_2 + c)$ for some $b, c \in \mathbb{Z}_p$.*

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

(b) If $A \nsim B$, then $b = c$.

(c) If $A \sim B$, then every $\pi \in Sym(A \cup B)$ which fixes A and B setwise is an automorphism of the graph defined on $A \cup B$ as long as $\pi|_A \in Aut(A)$ and $\pi|_B \in Aut(B)$.

4 Main result for $p > 8$

In this section, we will prove that $R \times \mathbb{Z}_p$ is a DCI-group if $p > 8$, where R is either Q or $\mathbb{Z}_2^3$.

Proposition 4.1. *For every prime $p > 8$, the group $R \times \mathbb{Z}_p$ is a DCI-group.*

Our technique is based on Lemma 3.1 so we have to fix a Cayley graph $\Gamma = Cay(R \times \mathbb{Z}_p, S)$. Let $A = Aut(\Gamma)$ and $\mathring{G} = \mathring{R} \times \mathring{\mathbb{Z}}_p$ be a regular subgroup of A isomorphic to $R \times \mathbb{Z}_p$. In order to prove Proposition 4.1 we have to find an $\alpha \in A$ such that $\mathring{G}^\alpha = \hat{G} = \hat{R} \times \hat{\mathbb{Z}}_p$. We will achieve this in three steps.

4.1 Step 1

Since $p > 8$, the Sylow p-subgroup of Sym(8p) is generated by 8 disjoint p-cycles. We may assume $\hat{\mathbb{Z}}_p$ and $\mathring{\mathbb{Z}}_p$ lie in the same Sylow p-subgroup P of $Sym(8p)$. Then both $\mathring{R}$ and $\hat{R}$ are subgroups of $N_{Sym(8p)}(P) \cap A$ so we may assume that $\mathring{R}$ and $\hat{R}$ lie in the same Sylow 2-subgroup of $N_{Sym(8p)}(P) \cap A$ which is contained in a Sylow 2-subgroup of A.

Since $p > 8$, the Sylow p-subgroup P gives a partition $\mathcal{B} = \{B_1, B_2, \dots, B_8\}$ of the vertices of Γ, where $|B_i| = p$ for every $i = 1, \dots, 8$ and $\mathcal{B}$ is P-invariant. It is easy to see that $\mathcal{B}$ is invariant under the action of $\hat{R}$ and $\mathring{R}$ and hence $\langle \hat{G}, \mathring{G} \rangle \leq Sym(p) \wr Sym(8)$. Moreover, both $\mathring{G}$ and $\hat{G}$ are regular so $\mathring{R}$ and $\hat{R}$ induce regular action on $\mathcal{B}$ which we denote by R_1 and R_2, respectively. The assumption that $\mathring{R}$ and $\hat{R}$ lie in the same Sylow 2-subgroup of A implies that R_1 and R_2 are in the same Sylow 2-subgroup of $Sym(8)$.

4.2 Step 2

Let us assume that $R_1 \neq R_2$. We intend to find an element $\alpha \in A$ such that $\left(\mathring{R}^{\alpha}\right)^{\mathcal{B}} = R_2$.

We define a graph Γ_0 on $\mathcal{B}$ such that B_m is adjacent to B_n if and only if $B_m \not\sim B_n$. This is an undirected graph with vertex set $\mathcal{B}$ and both R_1 and R_2 are regular subgroups of $Aut(\Gamma_0)$. It follows that Γ_0 is a Cayley graph of R.

Observation 4.1. Since $R_1 \leq Aut(\Gamma_0)$ acts transitively on $\mathcal{B}$ we have that the order of eah connected component of Γ_0 divides 8.

We can also define a coloured graph Γ_1 on $\mathcal{B}$ by colouring the edges of the complete directed graph on 8 vertices. The vertex B_m is adjacent to the vertex B_n with the same coloured edge as $B_{m'}$ is adjacent to $B_{n'}$ in Γ_1 if and only if there exists a graph isomorphism ϕ from the induced subgraph of Γ on $B_m \cup B_n$ to the induced subgraph of Γ on $B_{m'} \cup B_{n'}$ such that $\phi(B_m) = B_{m'}$ and $\phi(B_n) = B_{n'}$. The graph Γ_1 is a coloured Cayley graph of R. Moreover, both R_1 and R_2 act regularly on Γ_1. Using the fact that R has property $DCI^{(2)}$, it is clear that there exists an $\alpha' \in \langle R_1, R_2 \rangle^{(2)} \leq Aut(\Gamma_1)$ such that $R_2^{\alpha'} = R_1$. We would like to lift α' to an automorphism α of Γ such that $\alpha^{\mathcal{B}} = \alpha'$.

(a) Let us assume first that Γ_0 is a connected graph.

Lemma 4.2. *(a)* $\mathring{R} \times \mathring{\mathbb{Z}}_p \leq \hat{\mathbb{Z}}_p \wr Sym(8)$.

(b) If $\mathring{R} \times \mathring{\mathbb{Z}}_p \leq \hat{\mathbb{Z}}_p \wr Sym(8)$, *then for every* $\mathring{r} \in \mathring{R}$ *we have* $(\mathring{r})_b = id$.

Proof. (a) We first prove that $\hat{\mathbb{Z}}_p = \mathring{\mathbb{Z}}_p$. Let x and y generate $\hat{\mathbb{Z}}_p$ and $\mathring{\mathbb{Z}}_p$, respectively. Since x and y lie in the same Sylow p-subgroup and $|B_1| = p$, we can assume that $x|_{B_1} = y|_{B_1}$. Using Lemma 3.8(b) we get that $x|_{B_m} = y|_{B_n}$ if there exists a path in Γ_0 from B_m to B_n. This shows that $x = y$ since Γ_0 is connected. Moreover, $\mathring{R} \times \hat{\mathbb{Z}}_p \leq \hat{\mathbb{Z}}_p \wr Sym(8)$ since the elements of $\mathring{\mathbb{Z}}_p$ and the elements of $\mathring{R}$ commute.

(b) Let $A' = A \cap \left(\hat{\mathbb{Z}}_p \wr Sym(8)\right)$. We have already assumed that $\mathring{R}$ and $\hat{R}$ lie in the same Sylow 2-subgroup of A'. Let $\mathring{r}$ be an arbitrary element of $\mathring{R}$. For every $(a, u) \in R \times \mathbb{Z}_p$ we have $\mathring{r}(a, u) = (b, u + t)$ for some $b \in R$ and $t \in \mathbb{Z}_p$, where t only depends on $\mathring{r}$ and a since $\mathring{r} \leq \hat{\mathbb{Z}}_p \wr Sym(8)$. The permutation group $\hat{G}$ is transitive, hence there exist $\hat{r}_1, \hat{r}_2 \in \hat{R}$ such that $\hat{r}_1(1, u) = (a, u)$

and $\hat{r}_2(b, u+t) = (1, u+t)$. The order of $\hat{r}_2\mathring{r}\hat{r}_1$ is a power of 2 since $\hat{r}_2, \mathring{r}, \hat{r}_1$ lie in a Sylow 2-subgroup. Therefore $t = 0$ and hence $(\mathring{r})_b = id$.

□

Lemma 4.2 says that if Γ_0 is connected, then $\langle \mathring{R}, \hat{R}\rangle \leq \hat{\mathbb{Z}}_p \wr Sym(8)$ and $(r)_b = id$ for every $r \in \langle \mathring{R}, \hat{R}\rangle$. Therefore we can define $\alpha = \alpha' id_{\mathcal{B}}$ to be an element of the wreath product $\hat{\mathbb{Z}}_p \wr Sym(8)$ and clearly $\alpha' id_{\mathcal{B}}$ is an element of A with $\alpha^{\mathcal{B}} = \alpha'$.

(b) Let us assume that Γ_0 is the empty graph.

Then Lemma 3.8(c) shows that every permutation in $\langle R_1, R_2\rangle^{(2)}$ lifts to an automorphism of Γ.

(c) Let us assume that Γ_0 is neither connected nor the empty graph.

Observation 4.2. If $R_1 \neq R_2$, then $\langle \mathring{R}, \hat{R}\rangle \leq A$ contains β_1, β_2, β_3 such that

$$\beta_1^{\mathcal{B}} = (B_1B_2)(B_3B_4),\ \beta_2^{\mathcal{B}} = (B_1B_2)(B_5B_6),\ \beta_3^{\mathcal{B}} = (B_1B_2)(B_7B_8).$$

Proof. Recall from Lemma 3.5 that $\langle \hat{R}, \mathring{R}\rangle$ is the same group whether R is Q or $\mathbb{Z}_2^3$. By Lemma 3.4 the elements β_1, β_2, β_3 can be generated as products of an element of $\mathring{R}$ and $\hat{R}$, as in the proof of Proposition 3.6, if $R = Q$. □

Lemma 4.3. *We claim that B_{2k-1} and B_{2k} are in the same connected component of Γ_0 for $k = 1, 2, 3, 4$.*

Proof. Since Γ_0 is a Cayley graph and R_1 is transitive on the pairs of the form (B_{2k-1}, B_{2k}) it is enough to prove that B_1 and B_2 are in the same connected component of Γ_0. If $B_1 \nsim B_2$, then B_1 is adjacent to B_2 in Γ_0, so we can assume that $B_1 \sim B_2$. Since Γ_0 is not the empty graph B_1 is adjacent to B_l for some $l > 2$, so $B_1 \nsim B_l$. By Observation (4.2) there exists $\beta \in A$ such that $\beta(B_1) = B_2$ and $\beta(B_l) = B_l$. This shows that $B_2 \nsim B_l$ and hence there is a path from B_1 to B_2 in Γ_0. □

Γ_0 is not connected, so the order of the connected components of Γ cannot be bigger than 4. Since B_1 and B_2 are in the same connected component of Γ_0 there exists a partition $H_1 \cup H_2 = \mathcal{B}$ such that $|H_1| = |H_2| = 4$, $B_1, B_2 \in H_1$ and no vertex in H_1 is adjacent to any vertex of H_2 in Γ_0.

Lemma 4.4. *There exists $\alpha \in A$ such that $\alpha^{\mathcal{B}} = \alpha'$.*

Proof. Let us assume first that $H_1 = \{B_1, B_2, B_3, B_4\}$. Then we define α_1 to be equal to β_2 on H_1 and the identity on H_2, where β_2 is defined in Observation 4.2. Using Lemma 3.8(c) we get that α_1 is in $\langle \mathring{R}, \hat{R}\rangle^{(2)}$.

If $H_1 = \{B_1, B_2, B_5, B_6\}$ or $H_1 = \{B_1, B_2, B_7, B_8\}$, then we define α_2 by $\alpha_2|_{H_1} = \beta_1$ and $\alpha_2|_{H_2} = id$, where β_1 is defined in Observation 4.2. Lemma 3.8(c) shows again that $\alpha_2 \in A$.

It is easy to see that $\alpha_1^{\mathcal{B}} = \alpha_2^{\mathcal{B}} = (B_1B_2)$. Therefore A contains an element α such that $R_1^{\alpha^{\mathcal{B}}} = R_2$. □

We conclude that we can assume that $R_1 = R_2$.

4.3 Step 3

Let us now assume that $R_1 = R_2$. We intend to find $\gamma \in A$ such that $\mathring{R}^\gamma = \hat{R}$.

Let $\hat{x}$ and $\mathring{x}$ denote the generators of $\hat{\mathbb{Z}}_p$ and $\mathring{\mathbb{Z}}_p$, respectively. We may assume that $\hat{x}|_{B_1} = \mathring{x}|_{B_1}$.

Lemma 4.5. *There exists $\gamma \in A$ such that $\mathring{x}^\gamma = \hat{x}$.*

Proof. Let us assume first that Γ_0 is connected. It is clear by Lemma 3.8 (b) that $\mathring{x} = \hat{x}$. So, we may take $\gamma = 1$.

Let us assume that Γ_0 is not connected. In this case there are at least two connected components which we denote by $\mathscr{C}_1, \dots, \mathscr{C}_n$. We may assume that $B_1 \in \mathscr{C}_1$. The permutations $\hat{x}$ and $\mathring{x}$ are elements of the base group of $\hat{\mathbb{Z}}_p \wr Sym(8)$ and hence they can be considered as functions on $\mathcal{B}$. We may assume that $\hat{x}(r, u) = (r, u + 1)$ for every $(r, u) \in R \times \mathbb{Z}_p$. By Lemma 3.8 (b), the function $\mathring{x}$ is constant on each equivalence class.

For every $1 \le m \le n$ there exists $\mathring{r}_m \in \mathring{R}$ such that $\mathring{r}_m(\mathscr{C}_1) = \mathscr{C}_m$ and for every $\mathring{r}_m \in \mathring{R}$ there exists $\hat{r}_m \in \hat{R}$ such that $\mathring{r}_m^{\mathcal{B}} = \hat{r}_m^{\mathcal{B}}$. Let γ be defined as follows:

$$\gamma|_{\cup \mathscr{C}_1} = id$$
$$\gamma|_{\cup \mathscr{C}_m} = \mathring{r}_m \hat{r}_m^{-1} \text{ for } 2 \le m \le n.$$

Let $(b, v) \in \mathring{r}_m(B_e)$ with $B_e \in \mathscr{C}_1$ and we denote $\mathring{r}_m^{-1}(b, v)$ by (a, u). Since $\mathring{x}$ is constant on $\mathscr{C}_m$ we have $\mathring{x}^s(b, v) = (b, v + c_m s)$ for some c_m which only depends on $\mathscr{C}_m$. Thus $\mathring{r}_m(a, u + s) = (b, v + c_m s)$ since $\mathring{x}$ and $\mathring{r}_m$ commute and $\mathring{x}|_{B_e} = \hat{x}|_{B_e}$. Therefore we have

$$\gamma(b, w) = \mathring{r}_m(a, w) = \mathring{r}_m(a, u + (w - u)) = (b, v + c_m(w - u))$$

for every $(b, w) \in \mathring{r}_m(B_e)$. It is easy to verify that $\gamma^{-1}(b, w) = (b, \frac{w - v + uc_m}{c_m})$ for every $w \in \mathbb{Z}_p$ which gives

$$\gamma^{-1}\mathring{x}\gamma(b, w) = \gamma^{-1}\mathring{x}(b, wc_m + v - uc_m) = \gamma^{-1}(b, wc_m + v - uc_m + c_m) = (b, w + 1).$$

It follows that $\gamma^{-1}\mathring{x}\gamma = \hat{\gamma}$.

It remains to show that $\gamma \in A$. Let y and z be two elements of $R \times \mathbb{Z}_p$.

We denote by B_y and B_z the elements of $\mathcal{B}$ containing y and z, respectively. If B_y and B_z are in the same connected component of Γ_0, then either γ is defined on B_y and B_z by $\mathring{r}_m \hat{r}_m^{-1}$ which is the element of the group $\langle \mathring{G}, \hat{G} \rangle \le A$ or $\gamma(y) = y$ and $\gamma(z) = z$.

If B_y and B_z are not in the same connected component, then $B_y \sim B_z$. The definition of γ shows that $\gamma^{\mathcal{B}} = id$. Using Lemma 3.8 (c) we get that $\gamma|_{B_y \cup B_z}$ is an automorphism of the induced subgraph of Γ on the set $B_y \cup B_z$, which proves that $\gamma \in A$, finishing the proof of Lemma 4.5. □

Using Lemma 4.5 we may assume that $\mathring{x} = \hat{x}$. Since $\mathring{x}$ and $\mathring{r}$ commute we have $\mathring{R} \times \mathring{\mathbb{Z}}_p \le \hat{\mathbb{Z}}_p \wr Sym(8)$. Now we can apply Lemma 4.2 which gives $(\mathring{r})_b = id$ for every $\mathring{r} \in \mathring{R}$. This proves that $\mathring{R} = \hat{R}$ since $R_1 = R_2$. Therefore $\mathring{G} = \hat{G}$, finishing the proof of Proposition 4.1. □

It is straightforward to check that the proof of Proposition 4.1 only uses the fact that $p > 8$ in the first step of the argument. We can formulate this fact in Proposition 4.6.

Proposition 4.6. *Let Γ be a Cayley graph of $G = Q \times \mathbb{Z}_p$ or $G = \mathbb{Z}_2^3 \times \mathbb{Z}_p$, where p is an odd prime and let $\mathring{G} = \mathring{Q} \times \mathring{\mathbb{Z}}_p$ or $\mathring{G} = \mathring{\mathbb{Z}}_2^3 \times \mathring{\mathbb{Z}}_p$ be a regular subgroup of $Aut(\Gamma)$ isomorphic to G. Let us assume that there exists a $\langle \hat{G}, \mathring{G} \rangle$-invariant partition $\mathcal{B} = \{B_1, B_2, \dots, B_8\}$ of $V(\Gamma)$, where $|B_i| = p$ for every $i = \{1, \dots, 8\}$. In addition, we assume that $\mathring{\mathbb{Z}}_p$ is a subgroup of the base group of $\hat{\mathbb{Z}}_p \wr Sym(\mathcal{B})$. Then there is an automorphism α of the graph Γ such that $\hat{G}^\alpha = \mathring{G}$.*

5 Main result for $p = 5$ and 7

In this section we will prove that $Q \times \mathbb{Z}_5$, $Q \times \mathbb{Z}_7$, $\mathbb{Z}_2^3 \times \mathbb{Z}_5$ and $\mathbb{Z}_2^3 \times \mathbb{Z}_7$ are CI-groups.

The whole section is based on the paper [5], so we will only modify the proof of Lemma 5.4 of [5].

Proposition 5.1. *Every Cayley graph of $Q \times \mathbb{Z}_5$, $Q \times \mathbb{Z}_7$, $\mathbb{Z}_2^3 \times \mathbb{Z}_5$ and $\mathbb{Z}_2^3 \times \mathbb{Z}_7$ is a CI-graph.*

We let R denote either Q or $\mathbb{Z}_2^3$, and let $p = 5$ or 7. Let Γ be a Cayley graph of $R \times \mathbb{Z}_p$ and let $A = Aut(\Gamma)$. We denote by P a Sylow p-subgroup of A. Let us assume that A contains two copies of regular subgroups which we denote by $\hat{G} = \hat{R} \times \hat{\mathbb{Z}}_p$ and $\mathring{G} = \mathring{R} \times \mathring{\mathbb{Z}}_p$. We can assume that Γ is neither the empty nor the complete graph and both $\hat{\mathbb{Z}}_p$ and $\mathring{\mathbb{Z}}_p$ are contained in P.

If the order of every orbit of P on $V(\Gamma)$ is p, then it is clear from Proposition 4.6 that Γ is a CI-graph. Therefore P has an orbit $\Lambda \subset G$ such that $|\Lambda| = p^2$ since $p^3 > |G|$. The remaining orbits of P have order p since $2p^2 > 8p$.

It was proved in [5] Lemma 5.4 that the action of A on the vertices of the graph Γ cannot be primitive so there is a nontrivial A-invariant partition $\mathcal{B} = \{B_0, B_1, \dots, B_{t-1}\}$ of $V(\Gamma) = G$. The elements of the partition $\mathcal{B}$ have the same cardinality since the action of A is transitive on $\mathcal{B}$ so $|B_i| \leq 4p < p^2$ for every $i = 0, 1, \dots, t-1$. The partition $\mathcal{B}$ is P-invariant so P acts on $\mathcal{B}$. Since P is a p-group, the order of every orbit of P is a power of p.

Let $\mathscr{C} = \{C_0, C_1, \dots, C_{s-1}\}$ be an orbit of P on $\mathcal{B}$ such that $\Lambda \subseteq \cup_{i=0}^{s-1} C_i$. We may assume that $B_i = C_i$ for $i = 0, 1, \dots, s-1$. It is clear that s is a power of p. If $s \geq p^2$, then $\left|\cup_{i=0}^{s-1} C_i\right| \geq 2p^2 > 8p$ which is a contradiction. Since $|C_0| = |B_0| < p^2$, we cannot have $s = 1$. It follows that $1 < s < p^2$ which implies $s = p$.

For every $i < s$ and every $x \in P$ the following eqalities hold for some $j < s$

$$x(B_i \cap \Lambda) = x(B_i) \cap x(\Lambda) = B_j \cap \Lambda.$$

This implies that

$$|B_0 \cap \Lambda| = |B_i \cap \Lambda|$$

for every $0 \leq i < s$. Therefore

$$p^2 = |\Lambda| = \left|\cup_{i=0}^{s-1} (B_i \cap \Lambda)\right| = s\,|B_0 \cap \Lambda| = p\,|B_0 \cap \Lambda|\,.$$

This gives $|B_0 \cap \Lambda| = p$ so $|B_0|$ can only be p or 8 since $|B_0|\,t = 8p$ and both $|B_0|$ and $t \geq s$ are at least p.

If $|B_0| = p$, then Λ is the union of p elements of the A-invariant partition $\mathcal{B}$ and every orbit Λ' of P is an element of the partition $\mathcal{B}$ if $\Lambda' \neq \Lambda$. For every orbit $\Lambda' \neq \Lambda$ of P and for every $y \in \hat{\mathbb{Z}}_p \cup \mathring{\mathbb{Z}}_p$ we have $y(\Lambda') = \Lambda'$. In particular, $y(B_7) = B_7$. By Proposition 4.6 we may assume that there exists an element x' in $\hat{\mathbb{Z}}_p \cup \mathring{\mathbb{Z}}_p$ such that $x'(B_0) \neq B_j$ for some $j \neq 0, 7$ and clearly $x'(B_7) = B_7$. Since both $\hat{G}$ and $\mathring{G}$ are regular there exists $a \in C_A(x')$ such that $a(B_0) = B_7$. Since a and x' commute we have $a(B_j) = B_7$, which contradicts the fact that $a(B_0) = B_7$.

We must therefore have $|B_0| = 8$. Let $\hat{x}$ and $\mathring{x}$ generate $\hat{\mathbb{Z}}_p$ and $\mathring{\mathbb{Z}}_p$, respectively. Since $\hat{G}$ and $\mathring{G}$ are regular we have that neither $\hat{x}^{\mathcal{B}}$ nor $\mathring{x}^{\mathcal{B}}$ is the identity, so both $\hat{x}$ and $\mathring{x}$ are regular on $\mathcal{B}$. Since both $\hat{x}^{\mathcal{B}}$ and $\mathring{x}^{\mathcal{B}}$ generate a transitive subgroup in $Sym(\mathcal{B})$ of prime order $p > 2$, and every for $r \in \hat{R} \cup \mathring{R}$ the permutation $r^{\mathcal{B}}$ commutes with one of these two elements, we have $r^{\mathcal{B}} = id$. Since $\hat{x}$ and $\mathring{x}$ are in the same Sylow p-subgroup of P we may assume that $\hat{x}(B_i) = \mathring{x}(B_i) = B_{i+1}$ for $i = 0, 1, \ldots, p-1$, where the indices are taken modulo p. By Proposition 4.6 we may also assume that $\hat{x} \neq \mathring{x}$.

For every m there exists an l such that the action of $\hat{x}^l \mathring{x}^{-l}$ is nontrivial on B_m since $\hat{x} \neq \mathring{x}$. Therefore $A_{B_m}|_{B_m}$ contains a regular subgroup and a cycle of length p such that $p > \frac{|B_0|}{2}$. A theorem of Jordan on primitive permutation groups, which can also be found in [8, Theorem 13.1.], says that such a permutation group is 2-transitive and hence the induced subgraph of Γ on B_m is the complete or the empty graph for every m.

Lemma 5.2. $B_m \sim B_n$ *for* $0 \leq m < n \leq p-1$.

Proof. There exists a unique element $\hat{g} \in \hat{\mathbb{Z}}_p \leq P$ such that $\hat{g}(B_m) = B_n$. We also have a unique element $\mathring{g} \in \mathring{\mathbb{Z}}_p \leq P$ with $\hat{g}^{\mathcal{B}} = \mathring{g}^{\mathcal{B}}$. Since $\mathbb{Z}_p$ is a cyclic group of prime order and $\hat{x} \neq \mathring{x}$ we have $\hat{g} \neq \mathring{g}$. Moreover, we may also assume that $\hat{g}|_{B_m} \neq \mathring{g}|_{B_m}$ since $\hat{g} \neq \mathring{g}$ and the induced subgraphs of Γ on $B_{m+c} \cup B_{n+c}$ are all isomorphic, where both $m + c$ and $n + c$ are taken modulo p.

Clearly, $\tilde{g} = \mathring{g}\hat{g}^{-1}$ is a cycle of length p on B_n. The vertices of $V(\Gamma) \setminus \Lambda$ are contained in P-orbits of order p that contain the orbit of the vertex under x, so meet each B_i in a single vertex, so $\tilde{g}$ fixes every vertex of the set $B_m \cup B_n \setminus \Lambda$ since $\tilde{g}^{\mathcal{B}} = id$.

Let $u \in B_m \setminus \Lambda$. It is enough to show that if u is adjacent to some $v \in B_n$, then u is adjacent to every vertex of B_n. We will prove that A is transitive on the following pairs: $\{(u, w) \mid w \in B_n\}$.

A is transitive on $\{(u, w) \mid w \in B_n \cap supp(\tilde{g})\} = \{(u, w) \mid w \in B_n \cap \Lambda\}$ since $\tilde{g}$ fixes u. Therefore we may assume that $v \in B_n \setminus \Lambda$ and we only have to find an element $a \in A$ such that $a(u) = u$ and $a(v) \in B_n \cap \Lambda$.

The restriction of $\tilde{g}$ to B_n is a cycle of length p so $\tilde{g}$ does not commute with $\mathring{r}|_{B_n}$, where $\mathring{r}$ is an involution of $\mathring{R}$. Since $\mathring{r}$ and $\mathring{g}$ commute we have that there is a $u' \in B_m$ such that $\mathring{r}\hat{g}(u') \neq \hat{g}\mathring{r}(u')$. Since the action of $\hat{R}$ is transitive on B_m there exists $\hat{r} \in \hat{R}$ such that $\hat{r}(u) = u'$. Then

$$(\mathring{r}\hat{r})\,\hat{g}(u) = \mathring{r}\hat{g}\hat{r}(u) = \mathring{r}\hat{g}(u') \neq \hat{g}\mathring{r}(u') = \hat{g}\,(\mathring{r}\hat{r})\,(u)$$

so there exists $a' \in A$ such that

$$a'\hat{g}(u) \neq \hat{g}a'(u). \tag{5.1}$$

Let us suppose that $v = \hat{g}(u)$. Notice that $\hat{g}(u)$ is in a P-orbit of order p, so $\hat{g}(u) \notin \Lambda$. Then the inequality (5.1) gives $a'(v) \neq \hat{g}a'(u)$. Since $\hat{R}|_{B_m}$ is regular on B_m there exists $\hat{s} \in \hat{R}$ such that $\hat{s}(u) = a'(u)$ and since $\hat{s}$ and $\hat{g}$ commute we have $\hat{s}(v) = \hat{s}\hat{g}(u) = \hat{g}\hat{s}(u) = \hat{g}a'(u)$. Therefore $\hat{s}(v) \neq a'(v)$ and hence $\hat{s}^{-1}a'$ fixes u and $\hat{s}^{-1}a'(v) \neq v$ so we may assume that $v \neq \hat{g}(u)$.

If $p = 7$, then $v \in B_n \cap \Lambda$.

Let us assume that $p = 5$. We claim that there exists $\hat{t} \in \hat{R}$ such that $\hat{t}(u) \in B_m \setminus \Lambda = B_m \setminus supp(\tilde{g})$ while $\hat{t}(v) \in B_n \cap \Lambda = B_n \cap supp(\tilde{g})$. It is clear that $\hat{g}(B_m \cap supp(\tilde{g})) = B_n \cap supp(\tilde{g})$ and $\hat{g}$ commutes with each element of $\hat{R}$. Therefore it is enough to show that if $u, v \in B_m \setminus supp(\tilde{g})$ with $u \neq v$, then there exists $\hat{t} \in \hat{R}$ such that $\hat{t}(u) \in B_m \setminus supp(\tilde{g})$ and $\hat{t}(v) \in B_m \cap supp(\tilde{g})$. This can easily be seen from the fact that $\gcd(|\hat{R}|, 5) = 1$.

The permutations $\hat{t}^{-1}\tilde{g}^l\hat{t}$ fix the vertex u for every $0 \leq l \leq 4$ and $\hat{t}^{-1}\tilde{g}^{l_1}\hat{t}(v) \neq \hat{t}^{-1}\tilde{g}^{l_2}\hat{t}(v)$ if $l_1 \not\equiv l_2 \ (mod\, p)$. At least one of the the four elements $\hat{t}^{-1}\tilde{g}\hat{t}$, $\hat{t}^{-1}\tilde{g}^2\hat{t}$, $\hat{t}^{-1}\tilde{g}^3\hat{t}$, $\hat{t}^{-1}\tilde{g}^4\hat{t}$ of A fixes u and maps v to an element of $B_n \cap supp(\tilde{g}) = B_n \cap \Lambda$ since $|B_n \setminus supp(\tilde{g})| = 3$, finishing the proof of the fact that $B_m \sim B_n$ for $0 \leq m \neq n \leq 7$. □

Every permutation of $V(\Gamma)$ which fixes B_m setwise for every m is an automorphism of Γ so there is an $a \in A$ such that $\mathring{x}^a = \hat{x}$. Applying Proposition 4.6 we get that there exists $\alpha \in A$ such that $\left(\hat{R} \times \hat{\mathbb{Z}}_p\right)^\alpha = \mathring{R} \times \mathring{\mathbb{Z}}_p$, finishing the proof of Proposition 5.1.

References

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

[2] E. Dobson, The isomorphism problem for Cayley ternary relational structures for some abelian groups of order $8p$, *Dicrete Math.* **310** (2010), 2895–2909.

[3] E. Dobson, P. Spiga, CI-groups with respect to ternary relational structures: new examples, *Ars Math. Contemp.* **6** (2012), 351–364.

[4] C. H. Li, On isomorphisms of finite Cayley graphs- a survey, *Discrete Mathematics* **256** (2002), 301–334.

[5] C. H. Li, Z. P. Lu, P. P. Pálfy, Further restrictions on the structure of finite CI-groups, *J. Algebr. Comb.* (2007), 161–181.

[6] P. Spiga, On the Cayley isomorphism problem for a digraph with 24 vertices, *Ars. Math. Contemp.* **1** (2008), 38–43.

[7] G. Royle, *Constructive enumeration of graphs*, Thesis submitted to The University of Western Australia, 1987.

[8] H. Wielandt, *Finite permutation groups*, Academic Press, London-New York, 1964.