

The CI problem for infinite groups

Joy Morris*

Department of Mathematics and Computer Science
University of Lethbridge
Lethbridge, AB. T1K 3M4. Canada
joy.morris@uleth.ca

Submitted: Feb 24, 2015; Accepted: Nov 21, 2016; Published: Dec 9, 2016
Mathematics Subject Classifications: 05C25, 20B27

Abstract

A finite group G is a DCI-group if, whenever S and S' are subsets of G with the Cayley graphs $\text{Cay}(G, S)$ and $\text{Cay}(G, S')$ isomorphic, there exists an automorphism φ of G with $\varphi(S) = S'$. It is a CI-group if this condition holds under the restricted assumption that $S = S^{-1}$. We extend these definitions to infinite groups, and make two closely-related definitions: an infinite group is a strongly (D)CI $_f$ -group if the same condition holds under the restricted assumption that S is finite; and an infinite group is a (D)CI $_f$ -group if the same condition holds whenever S is both finite and generates G .

We prove that an infinite (D)CI-group must be a torsion group that is not locally-finite. We find infinite families of groups that are (D)CI $_f$ -groups but not strongly (D)CI $_f$ -groups, and that are strongly (D)CI $_f$ -groups but not (D)CI-groups. We discuss which of these properties are inherited by subgroups. Finally, we completely characterise the locally-finite DCI-graphs on \mathbb{Z}^n . We suggest several open problems related to these ideas, including the question of whether or not any infinite (D)CI-group exists.

1 Introduction

Although there has been considerable work done on the Cayley Isomorphism problem for finite groups and graphs, little attention has been paid to its extension to the infinite case.

Definition 1.1. A Cayley (di)graph $\Gamma = \text{Cay}(G; S)$ is a *(D)CI-graph* if whenever $\phi : \Gamma \rightarrow \Gamma'$ is an isomorphism, with $\Gamma' = \text{Cay}(G; S')$, there is a group automorphism α of G with $\alpha(S) = S'$ (so that α can be viewed as a graph isomorphism).

*This research was supported in part by the National Science and Engineering Research Council of Canada, Discovery Grant 238552-2011

Notice that since $\text{Aut}(\Gamma) = \text{Aut}(\bar{\Gamma})$ (where $\bar{\Gamma}$ denotes the complement of Γ) and any isomorphism from Γ to Γ' is also an isomorphism from $\bar{\Gamma}$ to $\bar{\Gamma}'$, a graph is a (D)CI-graph if and only if its complement is also a (D)CI-graph. Since at least one of Γ and $\bar{\Gamma}$ must be connected, the problem of determining (D)CI-graphs can be reduced to the connected case.

This definition extends to a definition for groups.

Definition 1.2. A group G is a *(D)CI-group* if every Cayley (di)graph on G is a (D)CI-graph.

These definitions (in the undirected case) as well as the following equivalent condition for a graph to be a (D)CI-graph, first appeared in work by Babai [3], extending a research problem posed by Adám for cyclic groups [1]. There has been a large body of work on this topic, and Li published a survey paper [14] outlining many of the results.

Theorem 1.3 ([3]). *A Cayley (di)graph Γ on the group G is a (D)CI-graph if and only if any two regular copies of G in $\text{Aut}(\Gamma)$ are conjugate.*

In the infinite case, it is natural to consider locally-finite (di)graphs: that is, (di)graphs whose valency is finite. When studying Cayley (di)graphs, this means that the set S is finite. However, restricting our consideration to this case complicates matters, as the complement of a locally-finite (di)graph is not locally-finite. For this reason, the standard argument made above that reduces the finite problem to the case of connected (di)graphs, does not apply to infinite (di)graphs that are locally-finite. In other words, if one wishes to study this problem in the context of locally-finite (infinite) (di)graphs, it is necessary to consider disconnected as well as connected (di)graphs.

For this reason, we give two new definitions. In the case of finite (di)graphs, both of these definitions coincide with the definition of a (D)CI-group, but in the infinite case they do not, and are themselves (we believe) worthy of study as natural generalisations of finite (D)CI-groups.

Definition 1.4. A finitely-generated group G is a *(D)CI_f-group* if every connected locally-finite Cayley (di)graph on G is a (D)CI-graph.

Note that it is not possible to have a connected locally-finite Cayley (di)graph on a group that is not finitely-generated, so the requirement that the group be finitely-generated only serves to avoid a situation where all non-finitely-generated groups are vacuously CI_f-groups.

Definition 1.5. A group G is a *strongly (D)CI_f-group* if every locally-finite Cayley (di)graph on G is a (D)CI-graph.

It should be apparent from these definitions that

$$\text{(D)CI-group} \Rightarrow \text{strongly (D)CI}_f\text{-group}$$

and if we restrict our attention to finitely-generated groups,

$$\text{strongly (D)CI}_f\text{-group} \Rightarrow \text{(D)CI}_f\text{-group}.$$

In this paper we will construct examples of groups that are (D)CI_f-groups but not strongly (D)CI_f-groups (despite being finitely generated) and groups that are strongly (D)CI_f-groups but not (D)CI-groups, so these definitions are interesting. We further study these classes, particularly in the case of infinite abelian groups, including a complete characterisation of the locally-finite graphs on \mathbb{Z}^n that are (D)CI-graphs. We also prove that no infinite abelian group is a (D)CI-group, and that any (D)CI-group must be a torsion group that is not locally finite. We leave open the question of whether or not any infinite (D)CI-groups exist.

The first paper we are aware of that solves a CI problem for infinite graphs was by Möller and Seifert [18]. Since they were actually considering the problem of digraphical regular representations (DRRs) of infinite finitely-generated groups, they considered only connected graphs. In the course of determining the DRRs for \mathbb{Z} , the results they proved imply (in our terms) that \mathbb{Z} is a CI_f-group. In the only prior work that we are aware of that is aimed specifically at solving the CI problem for infinite graphs, Ryabchenko [29] uses the standard definition (the same one we gave above) for a CI-group, and claims to have proven that every finitely-generated free abelian group is a CI-group. It is clear from his proofs that what he in fact shows is that \mathbb{Z} is a strongly CI_f-group, and \mathbb{Z}^n is a CI_f-group. We will restate the results he actually proves in that paper using our terminology, as well as pointing out several consequences of his proofs that he did not mention. We also show that \mathbb{Z}^n is not a strongly (D)CI_f-group if $n > 1$. Ryabchenko cites a paper by Chuesheva as the main motivation for his paper, but the journal is obscure and the url he provides no longer exists, so we were not able to obtain a copy of this paper. Löh has published a paper [16] on the related question of when a graph can be represented as a Cayley graph on more than one finitely-generated infinite abelian group.

We will proceed from the strongest property to the weakest. In Section 2, we will consider infinite (D)CI-groups, and prove that various large families of infinite groups cannot be (D)CI-groups; specifically, we show that any infinite CI-group must be a torsion group that is not locally finite. (Since every DCI-group is a CI-group, this result carries over to the directed case.) In Section 3, we consider strongly CI_f-groups. We construct an infinite family of such groups, but also prove that \mathbb{Z}^n is not a strongly CI_f-group for $n > 1$. We show that every finitely-generated subgroup of a strongly CI_f-group is a CI_f-group, but leave open the question of whether or not all subgroups of strongly CI_f-groups are strongly CI_f-groups. In Section 4, we consider CI_f-groups. We show that without the condition of local-finiteness, connectedness is not sufficient to ensure that a Cayley graph on \mathbb{Z}^n is a CI-graph. We note that \mathbb{Z}^n is a CI_f-group for every n . In Section 5, we include the results from [29], the first of which is also attributable to [18]. We have slightly generalised as well as correcting the statements from [29] (which can be done using the same proofs), and include some easy corollaries of his proofs, showing that every locally-finite Cayley (di)graph on \mathbb{Z}^n is a normal Cayley (di)graph, and in fact has a unique regular subgroup isomorphic to \mathbb{Z}^n . Finally, in Section 6, we completely

characterise the locally-finite Cayley graphs on \mathbb{Z}^n that are CI-graphs. In particular, we show that if $n \neq 2$ then a (nonempty) locally-finite Cayley graph on \mathbb{Z}^n is a (D)CI-graph if and only if it is connected, and that a (nonempty) locally-finite Cayley graph on \mathbb{Z}^2 is a (D)CI-graph if and only if it either

- is connected, or
- has exactly two connected components, and the connection set S is invariant under some automorphism of order 3 of $\langle S \rangle$.

2 CI-groups

In this section of the paper, we demonstrate that various families of infinite groups are not CI-groups. Since all DCI-groups are also CI-groups, this implies that these groups are not DCI-groups. We also discuss the open questions that remain.

Remark 2.1 ([4]). We observe that the property of being a CI-group is inherited by subgroups.

There is a standard construction for the above fact, used for finite groups, that works equally well for infinite groups if we are not requiring that graphs be locally finite. That is: if $H < G$ is not a CI-group, take a connected Cayley graph $\Gamma = \text{Cay}(H; S)$ that is not a CI-graph (use a complement if necessary to ensure that the graph is connected). Let $\Gamma' = \text{Cay}(H; S')$ be an isomorphic graph that is not isomorphic via an automorphism of H . Then $\text{Cay}(G; S)$ and $\text{Cay}(G; S')$ are clearly isomorphic, but any isomorphism must take connected components to connected components, so would restrict to an isomorphism from Γ to Γ' that cannot come from a group automorphism of H .

We now show that \mathbb{Z} is not a CI-group. Together with the preceding remark, this has strong consequences.

Proposition 2.2. *The group \mathbb{Z} is not a (D)CI-group.*

Proof. We prove this by finding a Cayley graph on \mathbb{Z} that is not a CI-graph. Let $S = \{i \in \mathbb{Z} : i \equiv 1, 4 \pmod{5}\}$. We will show that $\Gamma = \text{Cay}(\mathbb{Z}; S)$ is not a CI-graph.

Let $S' = \{i \in \mathbb{Z} : i \equiv 2, 3 \pmod{5}\}$, and let $\Gamma' = \text{Cay}(\mathbb{Z}; S')$. We claim that if we define $\phi : \Gamma \rightarrow \Gamma'$ by

$$\phi(i) = \begin{cases} i & \text{if } i \equiv 0 \pmod{5} \\ i + 1 & \text{if } i \equiv 1 \pmod{5} \\ i + 2 & \text{if } i \equiv 2 \pmod{5} \\ i - 2 & \text{if } i \equiv 3 \pmod{5} \\ i - 1 & \text{if } i \equiv 4 \pmod{5} \end{cases},$$

then ϕ is a graph isomorphism. Clearly ϕ is one-to-one and onto, so we need only show that xy is an edge of Γ if and only if $\phi(x)\phi(y)$ is an edge of Γ' .

Suppose that xy is an edge of Γ ; equivalently, $y - x \equiv 1, 4 \pmod{5}$. A case-by-case analysis of the possible residue classes for x and y shows that this always forces $\phi(y) - \phi(x) \equiv 2, 3 \pmod{5}$; equivalently, $\phi(x)\phi(y)$ is an edge of Γ' .

Since the only automorphisms of \mathbb{Z} fix sets that are closed under taking negatives (which S and S' are), and $S \neq S'$, we conclude that Γ is not a CI-graph. \square

This of course has very strong consequences.

Corollary 2.3. *No infinite group containing an element of infinite order is a CI-group. That is, infinite CI-groups must be torsion groups.*

Proof. If G contains an element τ of infinite order, then $\langle \tau \rangle \cong \mathbb{Z}$. By Proposition 2.2, this subgroup is not a CI-group, and by Remark 2.1, G cannot be a CI-group. \square

We now consider infinite abelian p -groups.

Proposition 2.4. *No infinite abelian p -group is a CI-group.*

Proof. By Remark 2.1, any subgroup of a CI-group is a CI-group. By Corollary 2.3, any infinite CI-group must be a torsion group (i.e., every element has finite order). Elspas and Turner [8] showed that \mathbb{Z}_{16} is not a CI-group, and this was generalised in [4] to \mathbb{Z}_{n^2} for $n \geq 4$, so any infinite abelian p -group would have to be elementary abelian (or contain an infinite elementary abelian subgroup). But Muzychuk [22] showed that elementary abelian p -groups of sufficiently high rank are not CI-groups. (Muzychuk's rank requirement was later improved by Spiga [32] and Somlai [31], but we only require a finite bound.) \square

The following simple lemma will allow us to eliminate all infinite abelian groups. This idea has been used in the finite case, but we provide the proof here since it is short, to show that it works equally well in the infinite case.

Lemma 2.5. *Suppose that G is a CI-group. If $H_1, H_2 \leq G$ with $|H_1| = |H_2|$ and $|G : H_1| = |G : H_2|$, then some automorphism of G carries H_1 to H_2 . In particular, $H_1 \cong H_2$.*

Proof. We have $\text{Cay}(G; H_1 - \{e\}) \cong \text{Cay}(G; H_2 - \{e\})$ since both consist of $|G : H_1|$ disjoint copies of the complete graph on $|H_1|$ vertices. So there is an automorphism of G that carries H_1 to H_2 . \square

Using the above results, we can now show that no infinite abelian group is a CI-group. In fact the idea of this proof does not really require the assumption that the infinite group is abelian, but that is certainly more than sufficient, and results in the strong corollary that follows.

Theorem 2.6. *No infinite abelian group is a CI-group.*

Proof. Suppose that G were an infinite abelian CI-group. By Corollary 2.2, we can assume that every element of G has finite order. By Proposition 2.4 (and Remark 2.1), we can assume that G does not contain an infinite p -group (applying Proposition 2.4 requires the assumption that G is abelian). Thus every p -subgroup of G is a finite CI-group, and

there are nontrivial p -subgroups of G for infinitely many primes. Fix some prime p for which the p -subgroups of G are nontrivial. Let H_1 be any infinite subgroup of G that has infinite order and infinite index in G , and has no elements of order p . (Such an H_1 exists since the Sylow p -subgroup of G is finite. For example, if P_1, P_2, \dots are all of the nontrivial Sylow subgroups of G with the exception of the Sylow p -subgroup, we could take $\langle P_i : i \text{ is odd} \rangle$.) Let H_2 be generated by H_1 together with an element of order p from G . Clearly, H_1 and H_2 are non-isomorphic since only one contains an element of order p , but this contradicts Lemma 2.5. \square

A locally-finite group is a group in which every finitely-generated subgroup is finite. The preceding theorem has the following consequence.

Corollary 2.7. *No infinite locally-finite group is a CI-group.*

Proof. Hall and Kulatilaka [11] and Kargapolov [13] independently proved that every infinite locally-finite group contains an infinite abelian group. Both proofs rely on the Feit-Thompson Theorem. Together with Remark 2.1, Theorem 2.6 therefore yields the desired conclusion. \square

Given the above results, it would be tempting to conjecture that no infinite group is a CI-group, but this is by no means clear, particularly in the case of unusual groups such as the Tarski Monsters (see below). We leave this as a problem for future research, first summarising what we can say about such a group.

Corollary 2.8. *Every subgroup of a CI-group must be a CI-group. Furthermore, every infinite CI-group must be:*

1. *a torsion group; and*
2. *not locally-finite.*

In addition, if there is an infinite CI-group, there is one that is finitely generated.

Proof. The first statement is Remark 2.1. Conclusion (1) is Corollary 2.3. Conclusion (2) is Corollary 2.7.

Suppose now that G is an infinite CI-group. Since G is not locally-finite, it must have a subgroup that is finitely generated but infinite, and is still a CI-group (by Remark 2.1). \square

In determining whether or not there is an infinite CI-group, one possible family of candidates that needs to be considered carefully is the family of so-called ‘‘Tarski Monsters’’. These are infinite groups whose only proper subgroups have order p for some fixed (but dependent upon the group) large prime p . Thus, every element of the group has order p , while any two elements in different cyclic subgroups generate the entire group. Clearly, if a Tarski monster G were to be a CI-group, then there would have to be at most two orbits of non-identity elements under $\text{Aut}(G)$. More precisely, for any two elements $g, h \in G$, g would have to be in the same orbit as either h or h^{-1} (otherwise, if there is

no automorphism taking g to either h or h^{-1} , then $\text{Cay}(G; \{g, g^{-1}\}) \cong \text{Cay}(G; \{h, h^{-1}\})$ but there is no automorphism of G taking $\{g, g^{-1}\}$ to $\{h, h^{-1}\}$, so there must be either a single orbit, or two orbits Ω and Ω^{-1} . We found discussions on the internet [17] indicating that for some Tarski monsters, any two of the subgroups are conjugate, but did not find an answer as to whether or not the stronger condition we are interested in is true for some Tarski monsters. Even if it were true, this is not enough to guarantee that such a group is a CI-group. We leave this as an open question.

Question 2.9. Does there exist an infinite CI-group? In particular, is any Tarski monster a CI-group?

3 Strongly CI_f -groups

In contrast to the class of CI-groups, we were able to find infinite groups that are strongly CI_f -groups. To begin this section, we note that Ryabchenko [29] proved that \mathbb{Z} is a strongly CI_f -group. This result is stated in Section 5 of this paper, as Corollary 5.2.

This naturally leads to the question of \mathbb{Z}^n . We show that \mathbb{Z}^n is not a strongly CI_f -group for any $n > 1$. We in fact prove a stronger result, for use later in this paper when we precisely characterise locally-finite graphs in Theorem 6.1.

Proposition 3.1. *Let $n > 1$, and let $\Gamma = \text{Cay}(\mathbb{Z}^n; S)$ be any Cayley (di)graph on \mathbb{Z}^n such that the number of connected components of (the underlying graph of) Γ is either infinite, or is divisible by p^2 for some prime p . Then Γ is not a (D)CI-graph.*

Proof. For this proof, we use the formulation of the CI problem given in Theorem 1.3.

Let $G = \langle S \rangle$, and let $\Gamma_0 = \text{Cay}(G; S)$ (so this is connected). Then $\text{Aut}(\Gamma)$ will either be $S_{\mathbb{Z}} \wr \text{Aut}(\Gamma_0)$, or $S_n \wr \text{Aut}(\Gamma_0)$, where n is finite and there is some prime p such that $p^2 \mid n$. Consider the subgroup of the appropriate symmetric group that is induced by the natural action of \mathbb{Z}^n on the connected components of Γ . Clearly this will be a regular abelian subgroup that is either countably infinite, or of order n . There are many nonisomorphic countably infinite regular abelian subgroups of $S_{\mathbb{Z}}$ (\mathbb{Z} and $\mathbb{Z}_2 \times \mathbb{Z}$, for example). Likewise, there are at least two nonisomorphic regular subgroups of S_n ($\mathbb{Z}_p \times \mathbb{Z}_{n/p}$ and $\mathbb{Z}_{p^2} \times \mathbb{Z}_{n/p^2}$). Since $n > 1$, each of these can be expanded to a regular action isomorphic to \mathbb{Z}^n in $\text{Aut}(\Gamma)$. Since the subgroups are nonisomorphic, they are not conjugate in the appropriate symmetric group, so the expanded actions on Γ are not conjugate in $\text{Aut}(\Gamma)$. Thus Γ is not a (D)CI-graph. \square

Corollary 3.2. *The group \mathbb{Z}^n is not a strongly CI_f -group for $n > 1$.*

Proof. When $n > 1$, it is easy to construct finitely-generated Cayley graphs on \mathbb{Z}^n for which the number of connected components is either countably infinite, or divisible by a square. For example, $\Gamma_1 = \text{Cay}(\mathbb{Z}^n; \{\pm(1, 0, \dots, 0)\})$ has a countably infinite number of connected components, while Γ_2 , the Cayley graph on \mathbb{Z}^n whose connection set is the standard generating set for \mathbb{Z}^n (together with inverses) with the first generator (and its

inverse) replaced by $\pm(p^2, 0, \dots, 0)$, will have p^2 connected components. So Proposition 3.1 is sufficient.

Had we only wanted to show that \mathbb{Z}^n is not a strongly CI_f -group for $n > 1$, we could have pointed out that $\Gamma_1 \cong \text{Cay}(\mathbb{Z}^n; \{\pm(2, 0, \dots, 0)\})$ but not via a group automorphism of \mathbb{Z}^n , or similarly that Γ_2 is isomorphic to the Cayley graph on \mathbb{Z}^n whose connection set is the standard generating set for \mathbb{Z}^n (together with inverses) with the first generator (and its inverse) replaced by $\pm(p, 0, \dots, 0)$, and the second generator (and its inverse) replaced by $\pm(0, p, \dots, 0)$, but not via a group automorphism of \mathbb{Z}^n . \square

Having determined the status of free abelian groups, we turn our attention to the opposite end of the spectrum of infinite abelian groups and consider torsion groups. First we prove a restriction on torsion groups that are strongly CI_f -groups (dropping the abelian constraint for the time being).

Lemma 3.3. *Suppose that G is a locally-finite torsion group that is a strongly CI_f -group. Then every finite subgroup of G is a CI-group.*

Furthermore, for $p \geq 5$ the Sylow p -subgroups of G are elementary abelian, and the Sylow 3-subgroups are either cyclic of order at most 27, or elementary abelian.

Proof. Since G is a strongly CI_f -group, an argument similar to that of Remark 2.1 shows that every finite subgroup must be a CI-group.

Babai and Frankl [4] showed that for $p \geq 5$ the only finite p -groups that are CI-groups are elementary abelian, and the finite 3-groups that are CI-groups are either cyclic of order at most 27, or elementary abelian. Furthermore, Muzychuk [22] proved that elementary abelian groups of sufficiently high rank are not CI-groups. Since G is locally-finite and the results just stated imply that every finite p -subgroup has bounded order, there must be a finite number of generators that contribute to any p -group in G . In particular, this means that the p -groups in G must all be finite. Thus by [4] again, we obtain the desired conclusion. \square

In addition to \mathbb{Z} which seems to be a sporadic example, we have been able to find an infinite family of groups that are strongly CI_f -groups.

Theorem 3.4. *Let G be a countable abelian torsion group. Then G is a strongly (D) CI_f -group if and only if every finite subgroup of G is a (D)CI-group.*

Proof. Abelian torsion groups are locally-finite, so necessity is shown in Lemma 3.3.

For the converse, suppose that G is a countable abelian torsion group, and every finite subgroup of G is a (D)CI-group.

By Lemma 3.3, when $p \geq 3$ the Sylow p -subgroups of G are elementary abelian, or cyclic of order at most 27. To understand the Sylow 2-subgroups and to improve our understanding of the Sylow 3-subgroups, we use Lemma 3.3 to note that they must be Sylow 2-subgroups of finite (D)CI-groups. Aside from some finite exceptional groups whose order does not exceed $2^5 3^2 = 288$, it is known that in any finite abelian (D)CI-group H , every Sylow p -subgroup of H must be either \mathbb{Z}_4 , or elementary abelian. This strengthening of the work of Babai and Frankl [4] for $p = 2$ and $p = 3$ is mentioned in

[15]. Since G has arbitrarily large finite subgroups all of which are (D)CI-groups, this implies that every Sylow p -subgroup of G must be either \mathbb{Z}_4 , or elementary abelian.

Let $\Gamma = \text{Cay}(G; S) \cong \Gamma' = \text{Cay}(G; S')$, with S finite. Since G is an abelian torsion group, $\langle S \rangle$ must be finite, and $\langle S' \rangle$ has the same finite order, so $H = \langle S, S' \rangle$ is a finite subgroup of G , so is a (D)CI-group. Clearly $\text{Cay}(H; S) \cong \text{Cay}(H; S')$, so as H is a (D)CI-group, there is an automorphism α of H taking S to S' .

Since G is countable, list the elements of G : g_1, g_2, \dots , so that $H = \{g_1, \dots, g_{|H|}\}$ (the rest of the list can be arbitrary). For $i \geq |H|$, define $G_i = \langle g_1, \dots, g_i \rangle$ (so $G_{|H|} = H$).

We claim that for $i \geq |H|$, there is an automorphism α_i of G_i that takes S to S' (so is an isomorphism from $\text{Cay}(G_i; S)$ to $\text{Cay}(G_i; S')$) such that for every $j \in \{|H|, |H|+1, \dots, i\}$, the restriction of α_i to G_j is α_j . We prove this claim by induction. The base case of $i = |H|$ has been established. By induction, we can assume that we have α_{i-1} such that the restriction of α_{i-1} to G_j is α_j for every $|H| \leq j \leq i-1$, so we need only find α_i such that the restriction of α_i to G_{i-1} is α_{i-1} . Since G_i is abelian, it is the direct product of its Sylow p -subgroups, so if we show that the action of α_{i-1} on any Sylow p -subgroup of G_{i-1} is the restriction of the action of α_i on the corresponding Sylow p -subgroup of G_i , this will suffice. Let P_i be a Sylow p -subgroup of G_i , and P_{i-1} the corresponding Sylow p -subgroup of G_{i-1} . If $P_{i-1} = P_i$ then we define $\alpha_i(g) = \alpha_{i-1}(g)$ for every $g \in P_i = P_{i-1}$. If P_i is elementary abelian and $P_i \neq P_{i-1}$, then since $G_i = \langle G_{i-1}, g_i \rangle$ is abelian, we must have $P_i \cong P_{i-1} \times \mathbb{Z}_p$. In this case use this representation, and for any $(g, h) \in P_i = P_{i-1} \times \mathbb{Z}_p$, define $\alpha_i(g, h) = (\alpha_{i-1}(g), h)$. The only remaining possibility is that $p = 2$, $P_i = \mathbb{Z}_4$, and $P_{i-1} = \mathbb{Z}_2$. In this case, define $\alpha_i(g) = g$ for every $g \in P_i$. Since α_{i-1} must act as the identity on $P_{i-1} \cong \mathbb{Z}_2$, the restriction of α_i to P_{i-1} is again α_{i-1} .

Now we define α' , which will be an automorphism of G that takes S to S' . For ease of notation, first define $\alpha_i = \alpha$ for $1 \leq i \leq |H|$. Now for any $g_i \in G$, define $\alpha'(g_i) = \alpha_i(g_i)$. We show that the map α' is an automorphism of G . Let $g_i, g_j \in G$ with $i \leq j$. First, notice that because the restriction of α_j to G_i is α_i (where $G_i = H$ for every $1 \leq i \leq |H|$), we have $\alpha_j(g_i) = \alpha_i(g_i)$. Now, $g_i, g_j, g_i g_j \in G_j$ and

$$\alpha'(g_i)\alpha'(g_j) = \alpha_i(g_i)\alpha_j(g_j) = \alpha_j(g_i)\alpha_j(g_j) = \alpha_j(g_i g_j) = \alpha'(g_i g_j). \quad \square$$

While the finite abelian (D)CI-groups have not been completely determined, elementary abelian groups of rank at most 4 are known to be DCI-groups [7, 10, 12, 20, 33]. So the preceding theorem gives us an infinite class of infinite strongly (D)CI $_f$ -groups: namely, pick any infinite set of primes Q . For each $p \in Q$, take a cyclic p -group. Define G to be the direct product of the chosen groups. Then G is a strongly (D)CI $_f$ -group. (It would be nice to be able to select an elementary abelian p -group of rank higher than one for at least some of the primes in Q ; unfortunately, the question of whether or not finite direct products of most such groups are (D)CI-groups remains open.)

It is, unfortunately, not clear whether the property of being a strongly (D)CI $_f$ -group is necessarily inherited by subgroups of strongly (D)CI $_f$ -groups. In the examples that we have found, it is inherited, since the only infinite subgroup of \mathbb{Z} is \mathbb{Z} , and if G is any group in the family of strongly (D)CI $_f$ -groups described in Theorem 3.4, and H is any infinite subgroup of G , then (by our structural characterisation of the family) H is in the family,

so H is a strongly (D)CI $_f$ -group. In general, though, we do not see why the following situation might not arise: G is a strongly (D)CI $_f$ -group, and for some infinite subgroup H and some finite subsets S, S' of G , $\text{Cay}(G; S) \cong \text{Cay}(G; S')$, but for every automorphism α of G that takes S to S' , we have $\alpha(H) \neq H$, and in fact no automorphism of H takes S to S' .

Question 3.5. Is it true that every subgroup of a strongly (D)CI $_f$ -group is a strongly (D)CI $_f$ -group?

Note the answer to Question 3.5 is yes in the case of countable abelian torsion groups that are (D)CI $_f$ -groups. If G is such a group and $H \leq G$, then H is also a countable abelian torsion group (possibly finite) and by Theorem 3.4, every finite subgroup of both G and H is a (D)CI-group, so that H is a strongly (D)CI $_f$ -group.

We can at least say that when a subgroup of a strongly (D)CI $_f$ -group is finitely-generated, it must be a (D)CI $_f$ -groups.

Proposition 3.6. *A finitely-generated subgroup of a strongly (D)CI $_f$ -group is always a (D)CI $_f$ -group.*

Proof. Let G be a strongly (D)CI $_f$ -group, and let $H \leq G$ be finitely generated. Suppose that $\langle S \rangle = H$, and $\text{Cay}(H; S) \cong \text{Cay}(H; S')$ for some subset S' of H . Since $\text{Cay}(H; S)$ (or the underlying undirected graph) is connected, we also have $\langle S' \rangle = H$. Clearly, $\text{Cay}(G; S) \cong \text{Cay}(G; S')$ since each is the disjoint union of $|G : H|$ copies of the original (di)graph. Since G is a strongly (D)CI $_f$ -group, there is an automorphism α of G such that $\alpha(S) = S'$. Since $H = \langle S \rangle = \langle S' \rangle$, we must have $\alpha(H) = H$, so the restriction of α to H is an automorphism of H that takes S to S' . \square

4 CI $_f$ -groups

Although it was not the statement he gave, Ryabchenko [29] proved that \mathbb{Z}^n is a CI $_f$ -group for every n ; that is, every finitely-generated free abelian group is a CI $_f$ -group. We include a slight generalisation of his proof in Section 5, as Corollary 5.4. Currently, these are the only infinite (D)CI $_f$ -groups that we know of, since the family of strongly (D)CI $_f$ -groups determined in Theorem 3.4 has no finitely-generated members.

An interesting observation is that although connectedness is enough to ensure that a locally-finite Cayley graph on \mathbb{Z}^n is a (D)CI-graph, it is not sufficient if the graph is not locally-finite.

Corollary 4.1. *Let $n > 1$. Amongst connected Cayley (di)graphs on \mathbb{Z}^n that are not locally finite, some will be (D)CI-graphs and some will not.*

Proof. Corollary 5.4 tells us that any such (di)graph for which the complement is locally finite and connected will be (D)CI, while Proposition 3.1 tells us that any such (di)graph for which the complement is locally finite with a number of connected components that is infinite or is not square-free, will not be (D)CI. In fact, later in Theorem 6.1, we will

see that any such (di)graph for which $n > 2$ and the complement is locally finite and disconnected, or for which $n = 2$ and the complement is locally finite and has more than 2 connected components, will not be (D)CI. \square

Since subgroups of finitely-generated groups need not be finitely-generated, it is again not at all evident whether or not the property of being a (D)CI $_f$ -group is inherited by subgroups. Amongst other things, we would need to determine that all subgroups of (D)CI $_f$ -groups are finitely generated. Setting this aside, it is not evident whether or not finitely generated subgroups of (D)CI $_f$ -groups are (D)CI $_f$ -groups. Since for a (D)CI $_f$ -group we only know that connected, locally-finite Cayley (di)graphs are (D)CI-graphs, it is hard to see even how, given two locally-finite, isomorphic Cayley (di)graphs on $H \leq G$, one might construct suitable Cayley (di)graphs on G that are locally-finite and connected, to use the (D)CI $_f$ -property. One possible approach would involve proving that every Cayley colour graph on G actually has the CI-property, and then using a second colour of edges on a finite number of generators to connect cosets of H . We leave this as another question. To prove any result along these lines (e.g. with the additional condition that $|G : H|$ be finite) would be interesting, we believe.

Question 4.2. If G is a (D)CI $_f$ -group and $H \leq G$ is finitely-generated, is H a (D)CI $_f$ -group?

5 Ryabchenko's results

In this section we state the results from Ryabchenko's paper, and some closely-related results.

Although Ryabchenko does not consider digraphs, his proofs in fact cover the more general situation, and have a number of easy and interesting consequences that he does not make note of.

Theorem 5.1 ([18], Theorem 1.2; also [29], Theorem 1). *Let $S \subset \mathbb{Z}$ be finite. If $\text{Cay}(\mathbb{Z}; S') \cong \text{Cay}(\mathbb{Z}; S)$ then $S' = \pm S$.*

The statement of Möller and Seifert's result [18, Theorem 1.2] looks much like this, but they assume that S is a generating set for \mathbb{Z} (so that the graphs are connected), since they were looking for DRRs. The general statement given above is an easy consequence of the connected case. Two isomorphic disconnected Cayley graphs on \mathbb{Z} will have the same number of connected components, which determines the index of the subgroup generated by S (and S'); each connected component is isomorphic to a Cayley graph on \mathbb{Z} to which the result for connected graphs applies.

The statements of Theorem 5.1 and of Theorem 5.3 look quite different from the versions in Ryabchenko's paper, so for the reader's convenience and confidence complete proofs (based on Ryabchenko's proofs, which are quite different from the Möller-Seifert proofs) are provided in the arXiv version of this paper, [21].

This has the following immediate consequence.

Corollary 5.2. *The group \mathbb{Z} is a strongly $(D)CI_f$ -group.*

Proof. If $\text{Cay}(\mathbb{Z}; S)$ and $\text{Cay}(\mathbb{Z}; S')$ are isomorphic and S is finite, then by Theorem 5.1, $S' = \pm S$, so either the identity or the automorphism of \mathbb{Z} that takes every integer to its negative will act as an isomorphism from $\text{Cay}(\mathbb{Z}; S)$ to $\text{Cay}(\mathbb{Z}; S')$. \square

The next result does not look at all like the statement of Theorem 2 from [29], but is the clearest and most precise statement of the proof he gives for that theorem.

Theorem 5.3 ([29], Theorem 2). *Let S be a finite generating set for \mathbb{Z}^n , and let $\Gamma = \text{Cay}(\mathbb{Z}^n; S)$. Then if $\Gamma' = \text{Cay}(\mathbb{Z}^n; S')$ and there is an isomorphism $\phi : \Gamma \rightarrow \Gamma'$ such that ϕ takes the identity of \mathbb{Z}^n to the identity of \mathbb{Z}^n , then ϕ is a group automorphism of \mathbb{Z}^n .*

Again, a complete proof of this is provided in [21].

This has an easy corollary, which is (except for his omission of his assumption that the graphs are locally-finite) the result that was stated in [29], Theorem 2.

Corollary 5.4. *The group \mathbb{Z}^n is a $(D)CI_f$ -group.*

Proof. Let $\Gamma = \text{Cay}(\mathbb{Z}^n; S)$ and $\Gamma' = \text{Cay}(\mathbb{Z}^n; S')$ with $\phi : \Gamma \rightarrow \Gamma'$ an automorphism. Let $\mathbf{0}$ represent the identity element of \mathbb{Z}^n . If c is the element of \mathbb{Z}^n that corresponds to the vertex $\phi(\mathbf{0})$, then $\phi' = \phi - c$ is an isomorphism from Γ to Γ' that takes $\mathbf{0}$ to $\mathbf{0}$. By Theorem 5.3, ϕ' must be an automorphism of \mathbb{Z}^n . \square

The following corollary was not mentioned in Ryabchenko's paper but is an immediate consequence of his proof.

Corollary 5.5. *If $\Gamma = \text{Cay}(\mathbb{Z}^n; S)$ for some finite generating set S of \mathbb{Z}^n , then Γ is a normal Cayley (di)graph of \mathbb{Z}^n .*

Proof. Let $\mathbf{0}$ be the vertex of Γ corresponding to the identity element of \mathbb{Z}^n . Let γ be any automorphism of Γ . If c is the element of \mathbb{Z}^n that corresponds to the vertex $\gamma(\mathbf{0})$, then $\gamma' = \gamma - c$ is an automorphism of Γ that fixes $\mathbf{0}$. By Theorem 5.3, γ' must be an automorphism of \mathbb{Z}^n , so normalises \mathbb{Z}^n . Since translation by c also normalises \mathbb{Z}^n , we see that $\mathbb{Z}^n \triangleleft \text{Aut}(\Gamma)$. \square

The final corollary presented in this section is slightly less obvious, but is still essentially a consequence of the proof in [29].

Corollary 5.6. *If $\Gamma = \text{Cay}(\mathbb{Z}^n; S)$ for some finite generating set S of \mathbb{Z}^n , then $\text{Aut}(\Gamma)$ has a unique regular subgroup isomorphic to \mathbb{Z}^n .*

Proof. Let Z_1 and Z_2 be two regular subgroups isomorphic to \mathbb{Z}^n in $\text{Aut}(\Gamma)$ (with $Z_1 = \langle S \rangle$). Let $\alpha' \in Z_2$ be arbitrary; we plan to show that $\alpha' \in Z_1$. Let $\alpha \in Z_1$ such that $\alpha'(\mathbf{0}) = \alpha(\mathbf{0})$, where $\mathbf{0}$ is the vertex corresponding to the identity of \mathbb{Z}^n . Then $\beta = \alpha^{-1}\alpha'$ is an automorphism of Γ that fixes $\mathbf{0}$, so by Theorem 5.3, $\beta \in \text{Aut}(Z_1)$.

Since S is finite, Z_1 and Z_2 each have finite index in $\text{Aut}(\Gamma)$. It is well-known that the intersection of two groups of finite index, itself has finite index (c.f. Problem 6, Section

5.1, [2]). Let $Z = Z_1 \cap Z_2$. Clearly, since Z_1 and Z_2 are abelian, β commutes with every element of Z . But since $\beta \in \text{Aut}(Z_1)$, it can only commute with the elements of Z if it fixes all of them. This means that β fixes a finite-index subgroup of Z_1 pointwise, so since $\beta \in \text{Aut}(Z_1)$, we must have $\beta = 1$. Hence $\alpha' = \alpha \in Z_1$, as claimed. Since α' was arbitrary, $Z_2 = Z_1$ is the unique regular subgroup isomorphic to \mathbb{Z}^n in $\text{Aut}(\Gamma)$. \square

6 Characterisation of locally-finite (D)CI-graphs on \mathbb{Z}^n

We have already seen that \mathbb{Z} is a strongly (D)CI_f-group, and that for $n > 1$, \mathbb{Z}^n is a (D)CI_f-group but not a strongly (D)CI-group. The following theorem gives a simple characterisation of the locally-finite Cayley (di)graphs on \mathbb{Z}^n that are (D)CI-graphs (where $n > 1$):

Theorem 6.1. *Let $\Gamma = \text{Cay}(\mathbb{Z}^n, S)$ be nonempty and locally finite. Then Γ is a (D)CI-graph if and only if either:*

1. Γ is connected, or
2. $n = 1$, or
3. $n = 2$, Γ has only two connected components, and S is invariant under some automorphism ϕ of the group $\langle S \rangle$, such that ϕ has order 3.

The proof of the above theorem will occupy the rest of this section. The proof of the main lemma (Lemma 6.4) will use the following well-known consequence of Smith normal form (cf. 4.6.1 of [2]).

Theorem 6.2 (Simultaneous Basis Theorem). *Let M be a free abelian group of finite rank $n \geq 1$ over \mathbb{Z} , and let H be a subgroup of M of rank r . Then there is a basis $\{y_1, \dots, y_n\}$ for M and nonzero elements $a_1, \dots, a_r \in \mathbb{Z}$ such that $r \leq n$, a_i divides a_{i+1} for all i , and $\{a_1 y_1, \dots, a_r y_r\}$ is a basis for H .*

Corollary 6.3. *Let $H = b_1 \mathbb{Z} \times \dots \times b_n \mathbb{Z}$ for some $b_1, \dots, b_n \in \mathbb{Z}$ with $\prod_{i=1}^n b_i = k$, where k is finite and square-free. Then there is an automorphism σ of \mathbb{Z}^n such that $H^\sigma = k\mathbb{Z} \times \mathbb{Z}^{n-1}$.*

Proof. By Theorem 6.2, there is a basis $\{y_1, \dots, y_n\}$ for \mathbb{Z}^n and nonzero integers a_1, \dots, a_n such that a_i divides a_{i+1} for all i , and $\{a_1 y_1, \dots, a_n y_n\}$ is a basis for H . Notice that the index of H in \mathbb{Z}^n is clearly $a_1 a_2 \dots a_n$, so for this product to be the square-free integer k (given that a_i divides a_{i+1} for every i), the only possibility is that $a_1 = \dots = a_{n-1} = 1$ and $a_n = k$. Thus, there is a basis $\{y_1, \dots, y_n\}$ for \mathbb{Z}^n such that $\{y_1, \dots, y_{n-1}, k y_n\}$ is a basis for H , so taking σ to be the automorphism of \mathbb{Z}^n that takes y_n to e_1 , y_1 to e_n , and y_i to e_i for $2 \leq i \leq n-1$, where e_1, \dots, e_n is the standard basis for \mathbb{Z}^n , establishes the desired result. \square

The following technical result is the foundation of the proof of Theorem 6.1.

Lemma 6.4. *Let $\Gamma = \text{Cay}(\mathbb{Z}^n, S)$ be nonempty and locally finite, with $n > 1$. Then Γ is a (D)CI-graph if and only if:*

- Γ (or its underlying graph) has a finite, square-free number of components; and
- $\text{Aut}(H) = \text{Aut}(H)_{\mathbb{Z}^n} \cdot \text{Stab}_{\text{Aut}(H)}(S)$,

where $H = \langle S \rangle$, $\text{Stab}_{\text{Aut}(H)}(S)$ is the group of all automorphisms of H that fix S setwise, and $\text{Aut}(H)_{\mathbb{Z}^n} := \{\phi|_H : \phi \in \text{Aut}(\mathbb{Z}^n), \phi(H) = H\}$, where $\phi|_H$ denotes the restriction of ϕ to its action on H .

Proof. (\Rightarrow) We assume that Γ is a (D)CI-graph. By Proposition 3.1, Γ must have a finite, square-free number of components.

Take any automorphism β of H . Then $\text{Cay}(\mathbb{Z}^n, \beta(S)) \cong \Gamma$, so since Γ is a (D)CI-graph, there must be some $\gamma \in \text{Aut}(\mathbb{Z}^n)$ such that $\gamma(S) = \beta(S)$. So $\gamma^{-1}\beta|_H \in \text{Aut}(H)$ and fixes S setwise. Hence $\gamma^{-1}\beta|_H \in \text{Stab}_{\text{Aut}(H)}(S)$. Also since $\beta \in \text{Aut}(H)$, $H = \langle S \rangle$, and $\beta(S) = \gamma(S)$, we have $\gamma(H) = \beta(H) = H$, so $\gamma|_H \in \text{Aut}(H)$. Hence $\gamma|_H \in \text{Aut}(H)_{\mathbb{Z}^n}$. Therefore $\beta = (\gamma|_H)(\gamma^{-1}\beta|_H) \in \text{Aut}(H)_{\mathbb{Z}^n} \cdot \text{Stab}_{\text{Aut}(H)}(S)$. This shows that $\text{Aut}(H) \leq \text{Aut}(H)_{\mathbb{Z}^n} \cdot \text{Stab}_{\text{Aut}(H)}(S)$; since both of the groups in the product are subgroups of $\text{Aut}(H)$, the other inclusion is immediate.

(\Leftarrow) Suppose that $\Gamma \cong \Gamma' = \text{Cay}(\mathbb{Z}^n, S')$. Let $H = \langle S \rangle$ and $H' = \langle S' \rangle$. Let k be the number of connected components of Γ (and therefore of Γ'), so by assumption k is finite and square-free. Then $|\mathbb{Z}^n : H| = |\mathbb{Z}^n : H'| = k$. Since k is finite, the rank of H (and of H') is also n .

By Corollary 6.3, we can conjugate both H and H' to $k\mathbb{Z} \times \mathbb{Z}^{n-1}$ using an element of $\text{Aut}(\mathbb{Z}^n)$, so H and H' are conjugate to each other in $\text{Aut}(\mathbb{Z}^n)$. Thus, replacing S' by a conjugate if necessary, we may assume without loss of generality that $H' = H$.

Now since $H' = H \cong \mathbb{Z}^n$ and since $\text{Cay}(H, S) \cong \text{Cay}(H', S') = \text{Cay}(H, S')$ is connected, Corollary 5.4 tells us that this is a (D)CI-graph, so there is some $\tau \in \text{Aut}(H)$ such that $\tau(S) = S'$. By assumption, $\tau = \tau_1\tau_2$ where $\tau_1 \in \text{Aut}(H)_{\mathbb{Z}^n}$ and $\tau_2 \in \text{Stab}_{\text{Aut}(H)}(S)$. Now, since τ_2 fixes S setwise, we have $\tau_1(S) = \tau\tau_2^{-1}(S) = \tau(S) = S'$. By definition of $\text{Aut}(H)_{\mathbb{Z}^n}$, there is some $\sigma' \in \text{Aut}(\mathbb{Z}^n)$ such that $\sigma'|_H = \tau_1$, so since $S \subseteq H$, we have $\sigma'(S) = \tau_1(S) = S'$. This has shown that there is an automorphism of \mathbb{Z}^n taking S to S' , so Γ is a (D)CI-graph. \square

The proof of Theorem 6.1 will also use a bit of number theory and a classical fact from group theory.

Definition 6.5 ([9]). Let $(q, n) \in \mathbb{Z} \times \mathbb{Z}$ with $q, n > 1$. A prime number p is a *large Zsigmondy prime* for (q, n) if $p \mid (q^n - 1)$, but $p \nmid (q^i - 1)$ for $1 \leq i < n$, and either $p > n + 1$ or $p^2 \mid (q^n - 1)$.

Remark 6.6 ([9]). If p is a large Zsigmondy prime for (q, n) , then q has order n in the multiplicative group of units modulo p (which has order $p - 1$), so $n \leq p - 1$.

Lemma 6.7 (Feit [9, Thm. A]). *If $(q, n) \in \mathbb{Z} \times \mathbb{Z}$ with $q, n > 1$, then there is a large Zsigmondy prime for (q, n) , unless either*

1. $n = 2$, or
2. $n = 4$ and $q \in \{2, 3\}$, or
3. $n = 6$ and $q \in \{2, 3, 5\}$, or
4. $n \in \{10, 12, 18\}$ and $q = 2$.

Lemma 6.8 (Minkowski [30, Thm. 1(i), p. 3]). *Let F be a finite subgroup of $\mathrm{GL}(n, \mathbb{Q})$ for some n , and let p be a prime.*

1. *If $|F|$ is divisible by p , then $n \geq p - 1$.*
2. *If $|F|$ is divisible by p^2 , then $n \geq 2(p - 1)$.*

Proof of Theorem 6.1. (\Rightarrow) Assume Γ is (D)CI, but is not connected, and $n > 1$. We will show that the conditions in part 3 of the statement of the theorem are satisfied. Let $H = \langle S \rangle$, and let $k = |\mathbb{Z}^n : H|$ be the number of connected components of Γ . Then $k > 1$, and Proposition 3.1 tells us that k is square-free (and finite, so $H \cong \mathbb{Z}^n$). Therefore, Corollary 6.3 allows us to assume $H = k\mathbb{Z} \times \mathbb{Z}^{n-1}$, after conjugating S by an element of $\mathrm{Aut}(\mathbb{Z}^n) = \mathrm{GL}(n, \mathbb{Z})$.

Let

$$\sigma = \begin{pmatrix} 1/k & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Then σ is an isomorphism from H to \mathbb{Z}^n . Now

$$\mathrm{Aut}(H)_{\mathbb{Z}^n} = \left\{ \phi|_H : \phi = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \dots & b_{nn} \end{pmatrix} \in \mathrm{GL}(n, \mathbb{Z}) \text{ and } b_{12}, \dots, b_{1n} \equiv 0 \pmod{k} \right\},$$

so

$$A_H^\sigma := \sigma \cdot \mathrm{Aut}(H)_{\mathbb{Z}^n} \cdot \sigma^{-1} = \left\{ \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \dots & b_{nn} \end{pmatrix} \in \mathrm{GL}(n, \mathbb{Z}) : b_{21}, \dots, b_{n1} \equiv 0 \pmod{k} \right\}.$$

Lemma 6.4 tells us $\mathrm{Aut}(H) = \mathrm{Aut}(H)_{\mathbb{Z}^n} \cdot \mathrm{Stab}_{\mathrm{Aut}(H)}(S)$. Conjugating both sides by σ yields $\mathrm{GL}(n, \mathbb{Z}) = A_H^\sigma F$, where $F = \mathrm{Stab}_{\mathrm{Aut}(\mathbb{Z}^n)}(\sigma(S))$ is a finite subgroup of $\mathrm{GL}(n, \mathbb{Z})$.

Let q be a prime divisor of k , and let π be the natural homomorphism from $\mathrm{GL}(n, \mathbb{Z})$ to $\mathrm{GL}(n, \mathbb{Z}_q)$. Letting $\mathrm{SL}^\pm(n, \mathbb{Z}_q) = \{g \in \mathrm{GL}(n, \mathbb{Z}_q) \mid \det g = \pm 1\}$, we have

$$\mathrm{SL}^\pm(n, \mathbb{Z}_q) = \pi(\mathrm{GL}(n, \mathbb{Z})) = \pi(A_H^\sigma) \cdot \pi(F).$$

Since $\mathrm{SL}^\pm(n, \mathbb{Z}_q)$ is transitive on the finite projective space $\mathrm{PG}(n-1, q)$, and $\pi(A_H^\sigma)$ is the stabilizer in $\mathrm{SL}^\pm(n, \mathbb{Z}_q)$ of a point in this space, this implies that $\pi(F)$ is transitive on $\mathrm{PG}(n-1, q)$. In particular,

$$|\pi(F) : \pi(F) \cap \pi(A_H^\sigma)| \text{ is divisible by } |\mathrm{PG}(n-1, q)| = (q^n - 1)/(q - 1).$$

(And the same is true when F is replaced by any of its conjugates in $\mathrm{GL}(n, \mathbb{Z})$.)

The remainder of the proof is a slight extension of an argument suggested by G. Robinson [28]. Let p be a prime factor of $(q^n - 1)/(q - 1)$, so $p \mid |F|$. From Lemma 6.8(1), we see that $p \leq n + 1$. Furthermore, if $p = n + 1$, then, since F has an element of order p (by Cauchy's Theorem) and the cyclotomic polynomial $(x^p - 1)/(x - 1)$ is irreducible over \mathbb{Q} , the representation of F on \mathbb{Q}^n is irreducible (over \mathbb{Q}).

We claim that p is not a large Zsigmondy prime for (q, n) . Otherwise, Remark 6.6 tells us that $p \geq n + 1$, so Lemma 6.8(2) implies that $p^2 \nmid |F|$, so $p^2 \nmid (q^n - 1)/(q - 1)$. If p is a large Zsigmondy prime, then $p \nmid (q - 1)$, so we conclude that $p^2 \nmid (q^n - 1)$. The claim now follows by combining this with the fact (in the preceding paragraph) that $p \leq n + 1$.

We now know that there are no large Zsigmondy primes for (q, n) . We conclude from Lemma 6.7 that

$$n \in \{2, 4, 6, 10, 12, 18\}$$

(and for each n , there are only a few possible values of q , unless $n = 2$). We consider each possible value of n as a separate case.

Case 1. Assume $n = 2$. It is well known that every finite subgroup of $\mathrm{GL}(2, \mathbb{Z})$ is conjugate to a subgroup of either

$$D_8 = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle \text{ or } D_{12} = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \right\rangle.$$

(A list of all the finite subgroups of $\mathrm{GL}(2, \mathbb{Z})$, up to conjugacy, can be found in [23, pp. 179–180].) Thus, we may assume, after passing to a conjugate, that $F \subseteq D_m$, with $m \in \{8, 12\}$. Note that $|D_m| = m \leq 12$. Then, since

$$\left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\} \subseteq D_8 \cap A_H^\sigma \text{ and } \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq D_{12} \cap A_H^\sigma,$$

we have

$$q + 1 = \frac{q^2 - 1}{q - 1} = \frac{q^n - 1}{q - 1} \leq \frac{|\pi(F)|}{|\pi(F) \cap \pi(A_H^\sigma)|} \leq \frac{|D_m|}{|D_m \cap A_H^\sigma|} \leq \frac{12}{4} = 3.$$

So $q = 2$. This means $k > 1$ is a square-free positive integer whose only prime divisor is 2. So $k = 2$. In other words, Γ has only two connected components.

Furthermore, $|F|$ is divisible by $(q^n - 1)/(q - 1) = (2^2 - 1)/(2 - 1) = 3$, so F has an element of order 3. Therefore $\mathrm{Stab}_{\mathrm{Aut}(H)}(S) = \sigma^{-1}F\sigma$ also has an element ϕ of order 3. So the conditions in (3) are satisfied.

Case 2. Assume $n = 4$. From Lemma 6.7, we have $q \in \{2, 3\}$, so $|F|$ must be divisible by either $(2^4 - 1)/(2 - 1) = 15$ or $(3^4 - 1)/(3 - 1) = 40$. Therefore, F is

contained in a maximal finite subgroup M of $\mathrm{GL}(4, \mathbb{Z})$ whose order is divisible by 5. The nine maximal finite subgroups of $\mathrm{GL}(4, \mathbb{Z})$ are listed in [6, Thm. 4.27] (up to conjugacy), and, by inspection, the only two whose order is divisible by 5 are Sx_4 and Py_4 . So (after passing to a conjugate) M is either Sx_4 or Py_4 .

However, for each maximal subgroup M , the proof in [6] provides a finite M -invariant subset S that contains a basis of \mathbb{Z}^4 . For Py_4 , we have $|S| = 10$, so M has an orbit of cardinality ≤ 10 on $\mathrm{PG}(3, q)$; therefore M is not transitive. For Sx_4 , we have $|S| = 20$, and M is transitive on S ; therefore, the cardinality of some orbit on $\mathrm{PG}(3, q)$ must be a divisor of 20, and is therefore neither 15 nor 40. Once again, M is not transitive. Since $F \subseteq M$, this is a contradiction.

Case 3. Assume $n = 6$. From Lemma 6.7, we have $q \in \{2, 3, 5\}$. However, if $q \in \{3, 5\}$, then $(q^6 - 1)/(q - 1)$ is divisible by either $p = 13$ or $p = 31$, which contradicts the fact that $p \leq n + 1 = 7$. Therefore, we must have $q = 2$, so $(q^6 - 1)/(q - 1) = 3^2 \cdot 7$ is divisible by $p = 7$.

Let M be a maximal finite subgroup of $\mathrm{GL}(6, \mathbb{Z})$ that contains F . We note that M is absolutely irreducible, not merely irreducible over \mathbb{Q} . For example, it is implicit in [25, Thm. IV.5 and p. 117] (and stated explicitly, but without proof, on page 483 of [26]) that if a maximal finite subgroup of $\mathrm{GL}(6, \mathbb{Z})$ is irreducible (over \mathbb{Q}), then it is absolutely irreducible. G. Robinson [28] has provided two (short) alternative arguments. Begin by noting that if M is not absolutely irreducible, then it is (isomorphic to) a finite subgroup of $\mathrm{GL}(d, \mathbb{C})$, with $d \leq 3 = (p - 1)/2$. One argument simply notes that the finite subgroups of $\mathrm{GL}(3, \mathbb{C})$ have been classified. The other argument uses a theorem of R. Brauer [5], which implies that either M is isomorphic to $\mathrm{PSL}(2, p) = \mathrm{PSL}(2, 7)$ (which is of order 168), or the Sylow p -subgroup of M is normal (which implies $|M|$ is a divisor of $2(p - 1)p = 84$); in either case, $|M|$ is not divisible by $|\mathrm{PG}(n - 1, 2)| = 63$.

The seventeen absolutely irreducible maximal finite subgroups of $\mathrm{GL}(6, \mathbb{Z})$ are listed in [27, Thm. 4.1] (up to conjugacy), and, by inspection, the only three whose order is divisible by 7 are $\mathrm{Aut}(F_{12})$, $\mathrm{Aut}(F_{13})$, and $\mathrm{Aut}(F_{14})$. The order of $\mathrm{Aut}(F_{14}) \cong \mathrm{PGL}(2, 7) \times \{\pm 1\}$ is 672, which is not divisible by $|\mathrm{PG}(n - 1, 2)| = 63$.

Therefore, M is either $\mathrm{Aut}(F_{12})$ or $\mathrm{Aut}(F_{13})$. These are both isomorphic to $S_p \times \{\pm 1\}$, and they are conjugate over \mathbb{Q} to the automorphism group of the root lattice \mathcal{A}_{p-1} . In the notation of [6], this automorphism group is Sx_{p-1} . Specifically, note that S_p acts on \mathbb{Z}^p by permuting the standard basis vectors e_1, \dots, e_p . The embedding of $Sx_{p-1} = S_p \times \{\pm 1\}$ in $\mathrm{GL}(n, \mathbb{Z})$ is obtained by identifying $\mathbb{Z}^n = \mathbb{Z}^{p-1}$ with the \mathbb{Z} -span of the S_p -invariant set $\Phi = \{e_i - e_j : i \neq j\}$. Choose $g \in \mathrm{GL}(n, \mathbb{Q})$ that conjugates M to Sx_{p-1} , so $g\Phi$ is an M -invariant subset of \mathbb{Q}^n . After multiplying g by a scalar, we may assume $g\mathbb{Z}^n \subseteq \mathbb{Z}^n$, and (since Φ contains a basis of \mathbb{Z}^n) that there exists $v \in g\Phi \setminus 2\mathbb{Z}^n$. Then v represents a point $[v]$ in $\mathrm{PG}(n - 1, 2)$, and, since $g\Phi$ is M -invariant, we have

$$|M \cdot [v]| \leq |g\Phi| = |\Phi| = p \cdot (p - 1) < (2^{p-1} - 1)/(2 - 1),$$

which contradicts the fact that M is transitive on $\mathrm{PG}(n - 1, 2)$ (with $n = p - 1$).

Case 4. Assume $n = 10$. From Lemma 6.7, we have $q = 2$, so $(q^n - 1)/(q - 1) =$

$2^{10} - 1 = 3 \cdot 11 \cdot 31$, so letting $p = 31$ contradicts the fact that $p \leq n + 1 = 11$.

Case 5. Assume $n = 12$. From Lemma 6.7, we have $q = 2$. So $|F|$ must be divisible by $(2^{12} - 1)/(2 - 1) = 3^2 \cdot 5 \cdot 7 \cdot 13$. Let $p = 13$. Since $p > 11$, we know from [24, Thm. V.10(iii), p. 31] that any finite subgroup of $\text{GL}(p - 1, \mathbb{Z})$ whose order is divisible by p is either isomorphic to a subgroup of $\text{PGL}_2(p) \times \{\pm 1\}$, or conjugate in $\text{GL}(p - 1, \mathbb{Q})$ to a subgroup of Sx_{p-1} , the automorphism group of the root lattice \mathcal{A}_{p-1} . However, we know, from the argument in the last paragraph of Case 3 of the proof, that F cannot be conjugate in $\text{GL}(p - 1, \mathbb{Q})$ to a subgroup of Sx_{p-1} .

Therefore, F must be isomorphic to a subgroup of $\text{PGL}_2(13) \times \{\pm 1\}$. But this, too, is impossible, because

$$|\text{PGL}_2(13) \times \{\pm 1\}| = 13(13^2 - 1) \cdot 2 < (2^{12} - 1)/(2 - 1) = |\text{PG}(11, 2)|.$$

Case 6. Assume $n = 18$. From Lemma 6.7, we have $q = 2$, so $(q^n - 1)/(q - 1) = 2^{18} - 1 = 3^3 \cdot 7 \cdot 19 \cdot 73$, so letting $p = 73$ contradicts the fact that $p \leq n + 1 = 19$.

(\Leftarrow) From Corollaries 5.4 and 5.2, we know that if either (1) or (2) holds, then Γ is a CI-graph. Therefore, we need only consider assumption (3): assume Γ has two connected components, and S is invariant under some automorphism ϕ of the group $\langle S \rangle$, such that ϕ has order 3.

Since the number of components of Γ is 2, which is a finite, square-free number, we only need to verify the second condition of Lemma 6.4 to see that this is a CI graph. Let $H = \langle S \rangle$. Since Γ has two components, we know $|\mathbb{Z}^2 : H| = 2$, so Corollary 6.3 tells us that we may assume $H = 2\mathbb{Z} \times \mathbb{Z}$, after applying an automorphism of \mathbb{Z}^2 . As in the proof of (\Rightarrow), let

$$\sigma = \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix}.$$

Since $\phi \in \text{Stab}_{\text{Aut}(H)}(S)$, we have $\sigma\phi\sigma^{-1} \in \text{Stab}_{\text{Aut}(\mathbb{Z}^n)}(\sigma(S))$. It is well known that no element of order 3 in $\text{GL}(n, \mathbb{Z})$ acts trivially on $\text{PG}(n, 2)$. (See, for example, Case 1 of the proof of [19, Thm. 4.8.2, pp. 66–67] with $p = 2$ and $k = 3$.) Since $|\text{PG}(2, 2)| = 3$, this implies that $\langle \phi \rangle$ is transitive on $\text{PG}(2, 2)$. Since $\sigma \cdot \text{Aut}(H)_{\mathbb{Z}^2} \cdot \sigma^{-1}$ is the stabilizer in $\text{GL}(2, \mathbb{Z})$ of a point in $\text{PG}(2, 2)$, and $\langle \phi \rangle \subseteq \text{Stab}_{\text{Aut}(\mathbb{Z}^n)}(\sigma(S))$, we conclude that

$$(\sigma \cdot \text{Aut}(H)_{\mathbb{Z}^2} \cdot \sigma^{-1}) \cdot \text{Stab}_{\text{Aut}(\mathbb{Z}^n)}(\sigma(S)) = \text{GL}(2, \mathbb{Z}).$$

Conjugating by σ^{-1} yields the desired conclusion that $\text{Aut}(H) = \text{Aut}(H)_{\mathbb{Z}^n} \cdot \text{Stab}_{\text{Aut}(H)}(S)$. \square

We remark that graphs described in Theorem 6.1(3) (that is, disconnected, nonempty, locally-finite (D)CI-graphs on \mathbb{Z}^2) do arise.

Example 6.9. The graph $\text{Cay}(\mathbb{Z}^2, S)$ where $S = \{\pm(2, 0), \pm(0, 1), \pm(2, 1)\}$ is a CI-graph.

Proof. The matrix

$$\begin{pmatrix} -1 & 2 \\ -\frac{1}{2} & 0 \end{pmatrix}$$

has order 3 (its cube is the identity matrix) and is invariant on S (it maps $\pm(2, 0)$ to $\pm(-2, -1)$ to $\pm(0, 1)$), so is an automorphism of $\langle S \rangle$. Therefore by Theorem 6.1(3), it is a CI-graph. \square

Acknowledgments

I am deeply indebted to Laci Babai for many long conversations about this problem that led to the terminology introduced in this paper. Ideas from these conversations also formed the basis of many of the results and proofs presented here. Thanks are also due to the anonymous referee for careful reading of this paper and a number of helpful suggestions. I am also very grateful to Geoff Robinson, whose insightful answer to a question I posed on mathoverflow [28] led to major improvements in Section 6 of this paper. Finally, Dave Witte Morris helped enormously in formulating and writing up the ideas in Section 6.

References

- [1] A. Adam. Research problem 2–10. *J. Combinatorial Theory*, 2:309, 1967.
- [2] Robert B. Ash. Abstract algebra: The basic graduate year. <http://www.math.uiuc.edu/~r-ash/Algebra.html>, 11 2002.
- [3] L. Babai. Isomorphism problem for a class of point-symmetric structures. *Acta Math. Acad. Sci. Hungar.* 29(3–4):329–336, 1977.
- [4] L. Babai and P. Frankl. Isomorphisms of Cayley graphs. I. *Combinatorics* (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. I, Colloq. Math. Soc. János Bolyai, North-Holland, Amsterdam, 18:35–52, 1978.
- [5] Richard Brauer. On groups whose order contains a prime number to the first power II. *Amer. J. Math.* 64:421–440, 1942.
- [6] E. C. Dade. The maximal finite groups of 4×4 integral matrices. *Illinois J. Math.* 9:99–122, 1965.
- [7] Edward Dobson. Isomorphism problem for Cayley graphs of Z_p^3 . *Discrete Math.*, 147(1–3):87–94, 1995.
- [8] Bernard Elspas and James Turner. Graphs with circulant adjacency matrices. *J. Combinatorial Theory*, 9:297–307, 1970.
- [9] Walter Feit. On large Zsigmondy primes. *Proc. Amer. Math. Soc.*, 102:29–36, 1988.
- [10] C. D. Godsil. On Cayley graph isomorphisms. *Ars Combin.*, 15:231–246, 1983.
- [11] P. Hall and C. R. Kulatilaka. A property of locally finite groups. *J. London Math. Soc.*, 39:235–239, 1964.

- [12] M. Hirasaka and M. Muzychuk. An elementary abelian group of rank 4 is a CI-group. *J. Combin. Theory Ser. A*, 94(2):339–362, 2001.
- [13] M. I. Kargapolov. On a problem of O. Ju. Šmidt. *Sibirsk. Mat. Ž.*, 4:232–235, 1963.
- [14] Cai Heng Li. On isomorphisms of finite Cayley graphs—a survey. *Discrete Math.*, 256(1–2):301–334, 2002.
- [15] Cai Heng Li, Zai Ping Lu, and P. P. Pálffy. Further restrictions on the structure of finite CI-groups. *J. Algebraic Combin.*, 26(2):161–181, 2007.
- [16] Clara Löh. Which finitely generated Abelian groups admit isomorphic Cayley graphs? *Geom. Dedicata*, 164:97–111, 2013.
- [17] Avinoam Mann. Discussion of conjugacy classes of infinite groups. <http://www.math.niu.edu/~rusin/known-math/95/finite.conj>, 09 1995, now available at <https://web.archive.org/web/20120310035855/http://www.math.niu.edu/~rusin/known-math/95/finite.conj>.
- [18] Rögnvaldur G. Möller and Norbert Seifert. Digraphical Regular Representations of Infinite Finitely Generated Groups. *Europ. J. Combinatorics*, 19:597–602, 1998.
- [19] D. W. Morris. *Introduction to arithmetic groups*. Deductive Press, 2015. <https://arxiv.org/src/math/0106063v6/anc/IntroArithGrps-FINAL.pdf>
- [20] J. Morris. Isomorphisms of cayley graphs. *Ph.D. thesis*, Simon Fraser University, 1999.
- [21] J. Morris. The CI problem for infinite groups. [arXiv:1502.06114](https://arxiv.org/abs/1502.06114), 02 2015.
- [22] M. Muzychuk. An elementary abelian group of large rank is not a CI-group. *Discrete Math.*, 264(1–3):167–185, 2003. The 2000 *Com²MaC* Conference on Association Schemes, Codes and Designs (Pohang).
- [23] Morris Newman. *Integral matrices*. Academic Press, New York-London, 1972.
- [24] G. Nebe and W. Plesken. Finite rational matrix groups. *Mem. Amer. Math. Soc.* 116 1995, no. 556.
- [25] Wilhelm Plesken. Bravais groups in low dimensions. *Match* 10:97–119, 1981.
- [26] W. Plesken. Some applications of representation theory. In *Representation theory of finite groups and finite-dimensional algebras (Bielefeld, 1991)*, 477–496, Birkhäuser, Basel, 1991.
- [27] Wilhelm Plesken and Michael Pohst. On maximal finite irreducible subgroups of $GL(n, \mathbf{Z})$ II. The six dimensional case. *Math. Comp.* 31:552–573, 1977.
- [28] Geoff Robinson. Transitive actions of finite subgroups of $GL(n, \mathbf{Z})$ on projective geometries. <http://mathoverflow.net/q/252537>, 10 2016.
- [29] A. A. Ryabchenko. Isomorphisms of Cayley graphs of a free abelian group. *Sibirsk. Mat. Zh. (Translation in Siberian Math. J.)*, 48(5):1142–1146, (Russian); 919–922 (English), 2007.
- [30] Jean-Pierre Serre. Bounds for the orders of the finite subgroups of $G(k)$. [arXiv:1011.0346v1](https://arxiv.org/abs/1011.0346v1), 11 2010.

- [31] Gábor Somlai. Elementary abelian p -groups of rank $2p + 3$ are not CI-groups. *J. Algebraic Combin.*, 34(3):323–335, 2011.
- [32] Pablo Spiga. Elementary abelian p -groups of rank greater than or equal to $4p - 2$ are not CI-groups. *J. Algebraic Combin.*, 26(3):343–355, 2007.
- [33] James Turner. Point-symmetric graphs with a prime number of points. *J. Combinatorial Theory*, 3:136–145, 1967.