Automorphism Groups of Cayley Graphs

Sabrina Lato
Carthage College
slato@carthage.edu

September 28, 2017

Abstract

In this paper, we develop ideas in algebraic graph theory to look at the Cayley graphs of groups, and the automorphism groups of graphs. A Cayley graph can be defined using a group and a set; for a given group, a group automorphism between the sets implies isomorphic Cayley graphs, but a graph isomorphism between two Cayley graphs does not always imply a group automorphism between the two sets. When a graph isomorphism implies a group automorphism between the sets, a Cayley graph is called a Cayley Isomorphic graph (CI-graph) and the question of when a Cayley graph is a CI-graph is an open one. In this paper, we look at when a Cayley graph with specific automorphism groups will be a CI-graph, in particular proving that for a Cayley graph for a group G with $4k$ elements and automorphism group $\mathbb{Z}/4\mathbb{Z} \wr S_k$, the Cayley graph is a CI-graph if it has no elements of order 4, and is not a CI-graph if it contains a non-cylic subgroup of order 2^k and an element of order 4.

1 Introduction

There are a number of different connections between graph theory and algebra. In particular, there are ways to create graphs based on groups, or groups based on graphs. In this paper, we look at Cayley graphs, which are graphs based on groups, and the automorphism groups of graphs. By studying Cayley graphs with certain automorphism groups, we can learn more about that graph, and the underlying group for the Cayley graph.

2 Definitions and Development

2.1 Graph Theory

The definitions below come from [5].

Definition 1. A **graph** is a collection of vertices connected by edges. The set of vertices of a graph G is denoted $V(G)$, and the set of edges is denoted $E(G)$.

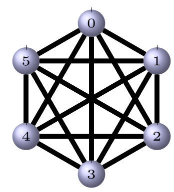


Figure 1: Complete graph on 6 vertices

Definition 2. Vertex v is **adjacent** to vertex w when there is an edge between v and w.

Definition 3. A **walk** between vertex v and vertex w is a sequence of adjacent vertices starting at v and ending at w.

Definition 4. A graph G is **connected** if between any two vertices v and w in $V(G)$, there exists a walk from v to w. A graph that is not connected is **disconnected**.

Definition 5. A **subgraph** H of a graph G is a graph with vertex set $V(H) \subseteq V(G)$ and edge set $E(H) \subseteq E(G)$.

Definition 6. An **induced subgraph** H of a graph G is a subgraph H with vertex set $V(H) \subseteq V(G)$ and edge set $E(H)$ such that for all vertices $v, w \in V(H)$, the edge $vw \in E(H)$ if and only if $vw \in E(G)$. We can also speak of a graph being induced by a vertex subset $S \subseteq V(G)$.

Definition 7. A **component** of a graph G is a maximal connected induced subgraph of G; that is, the subgraph induced by a vertex set $S \in V(G)$ is connected, but for any set such that $S \subsetneq S'$, the subgraph induced by S' is disconnected.

Definition 8. The **degree** of a vertex v is the number of vertices which are adjacent to v, or the number of edges that begin or end at v.

Definition 9. A **regular** graph is a graph where every vertex has the same degree.

Definition 10. Graph G is **isomorphic** to graph H when there exists a bijection f from $V(G) \to V(H)$ such that $f(u)$ and $f(v)$ are adjacent if and only if u and v are adjacent.

Definition 11. An **automorphism** is an isomorphism from $V(G) \to V(G)$.

2.1.1 Special Kinds of Graphs

Definition 12. The **complete** graph on n vertices, also called K_n, is a graph on n vertices such that every vertex is adjacent to every other vertex. See Figure 1.

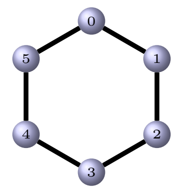


Figure 2: Cycle on 6 vertices

Definition 13. A **cycle** on n vertices, represented C_n, is a graph of the form $v_0, v_1, \ldots, v_{n-1}$ where, for all i such that $0 \leq i \leq n-1, v_i$ is adjacent to only the vertices v_{i+1} and v_{i-1}, where subscripts are read mod n.

Definition 14. Graph H is a **complement** to graph G when, for vertices u, v, u and v are adjacent in H if and only if u and v are not adjacent in G. The complement of G is sometimes written $\overline{G}$.

Becuase finite graphs are both easier to work with and better understood than infinite graphs, we will restrict ourselves to finite graphs for this paper.

2.2 Algebra

In this section, we will explore some algebraic ideas, with the ulitmate goal of applying it to graph theory. As such, the groups and sets we're working with will be finite, so we may assume that all of the sets and groups in this section are also finite, even though some of the definitions and theorems apply for infinite groups as well.

The definitions below come from [1].

Definition 15. A **group action** of a group G on a set A is a map $G \times A \to A$, written $g \cdot a$ for $g \in G, a \in A$ satisyfing the following:

i. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ where $g_1 g_2$ is the group operation computed in G;

ii. $1 \cdot a = a$ for all $a \in A$, where 1 is the identity in G.

Example 16. Any group can act on itself by defining $g_1 \cdot g_2 = g_1 g_2$.

Example 17. Let S_n be the symmetric group on n symbols, and let A be a set with n elements. There is clearly a bijection between the elements of A and $1, \ldots, n$, and we can use this bijection to let S_n act in a natural way on the elements of A. For example, the permutation element $(1, 2)$ would switch the labellings of the elements corresponding to 1 and 2 and map every other element to itself. We can see that the identity in S_n will map every element of $a \in A$ to itslef, and that for $g_1, g_2 \in S_n$, $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $a \in A$. Thus this isindeed a group action.

Example 18. Let A be a set, and let H be a group. We define B as the set of functions from A into H. We can thus think of an element in B as a n-tuple, where n is the number of elements in A. There is a natural correspondance between B and the $H \times H \times \cdots \times H$, the direct product of H with itself n times. We can see that B is a group under pointwise multplication, that is, if $f, g \in B$ then for $a \in A$, $(fg)(a) = f(a)g(a)$. Specifically, B is the group created by the direct product of n copies of H.

Now let G be a group acting on A. This action induces an action of G on B. Given $f \in B$ and $x \in G$, then we can define f^x on A as $f^x(a) = f(a \cdot x^{-1})$ for all $a \in A$. We note that for $x_1, x_2 \in G$, $f^{x_1 x_2}(a) = f(a \cdot (x_1 x_2)^{-1}) = (f(a \cdot x_2^{-1} x_1^{-1})) = f((a \cdot x_2^{-1}) \cdot x_1^{-1})$. Further, if 1 is the identity of G then $f^1(a) = f(a \cdot 1) = f(a)$. Thus f^x is indeed a group action of G on B.

Definition 19. Let G be a group acting on a set A. The equivalence class $\{g \cdot a \mid g \in G\}$ is called the **orbit** of G containing a.

Definition 20. The action of G on A is called **transitive** if there is only one orbit, that is, given any two elements $a, b \in A$, there is some $g \in G$ such that $a = g \cdot b$.

Definition 21. Let G be a permutation group acting transitively on a finite set A. Then G is **regular** if $\|G\| = \|A\|$.

Lemma 22. *Let G be a transitive permutation group acting on a finite set A. Then the following are equivalent.*

i. The group G is regular.

ii. For any $a, b \in A$, there is a unique element $g \in G$ satisfying $g \cdot a = b$.

iii. The only element of G that fixes an element of A is the identity.

Proof. We will show that $(i) \Leftrightarrow (ii)$ and $(ii) \Leftrightarrow (iii)$, and by transitivity we can conclude that $(i) \Leftrightarrow (ii)$.

Let G be a regular group acting on A, and let a, b be arbitrary elements of A. Since the action of G is transitive, we know that this action is surjective, and since we're looking at finite groups of the same size, it must be injective too, so there is a unique g such that $g \cdot a = b$. Conversely, suppose that G is a group acting on A such that for every $a, b \in A$, there is a unique $g \in G$ such that $g \cdot a = b$. If we fix a, then we have for every $b_i \in A$, there is a unique g_i such that $g_i \cdot a = b_i$, so the number of elements of G must be the same as the number of elements of A; in other words, G is regular.

Now suppose that given any two elements $a, b \in A$, there is some $g \in G$ such that $a = g \cdot b$. Then clearly, the only element of G that fixes an element of A is the identity. Conversely, suppose that the only element of G that fixes an element of A is the identity. Let $g_1, g_2 \in G$ such that $g_1 \cdot a = b$ and $g_2 \cdot a = b$. Then $g_1^{-1} \cdot (g_1 \cdot a) = g_1^{-1} \cdot b = g_1^{-1} \cdot (g_2 \cdot a)$. So $a = 1 \cdot a = (g_1^{-1} g_1) \cdot a = (g_1^{-1} g_2) \cdot a$ and, since the identity is unique, $g_1^{-1} g_2 = 1$, which means g_1^{-1} is the inverse of g_2, so $g_2 = g_1$. Thus there is a unique element $g \in G$ satisfying $g \cdot a = b$. $\square$

	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)	(3,0)	(3,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)	(3,0)	(3,1)
(0,1)	(0,1)	(0,0)	(3,1)	(3,0)	(2,1)	(2,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(2,0)	(2,1)	(3,0)	(3,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)	(3,1)	(3,0)	(2,1)	(2,0)
(2,0)	(2,0)	(2,1)	(3,0)	(3,1)	(0,0)	(0,1)	(1,0)	(1,1)
(2,1)	(2,1)	(2,0)	(1,1)	(1,0)	(0,1)	(0,0)	(3,1)	(3,0)
(3,0)	(3,0)	(3,1)	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)
(3,1)	(3,1)	(3,0)	(2,1)	(2,0)	(1,1)	(1,0)	(0,1)	(0,0)

Table 1: The Cayley table of $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

Definition 23. The **automorphism group** of a group G, written $\text{Aut}(G)$, is the set of all automorphisms of that group. It is a permutation group on the elements of the group.

Definition 24. Let H and K be groups and let φ be a homomorphism from K into $\text{Aut}(H)$. Let $\cdot$ denote the left-action of K on H determined by φ. Let G be the set of ordered pairs (h, k) with $h \in H$ and $k \in K$. We note that G is a group under the operation $(h_1, k_1)(h_2, k_2) = (h_1(k_1 \cdot h_2), k_1k_2)$. We write that $G = H \rtimes_\varphi K$, where $\rtimes_\varphi$ is the **semidirect product** of H and K with regard to φ. When φ is assumed to be clear from context, this will be written as simply $H \rtimes K$.

Example 25. If φ is the trivial homomorphism that maps everything in K to the identity map, then $H \rtimes_\varphi K = H \times K$, since $(h_1, k_1)(h_2, k_2) = (h_1(k_1 \cdot h_2), k_1k_2) = (h_1h_2, k_1k_2)$, which is the definition of the direct product.

Example 26. What is $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$?

We begin by noting that the only automorphisms of $\mathbb{Z}/4\mathbb{Z}$ are the identity automorphism and the function $f : 0 \mapsto 0, 1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 1$. Thus the only homomorphisms from $\mathbb{Z}/2\mathbb{Z}$ to $\text{Aut}(\mathbb{Z}/4\mathbb{Z})$ are the trivial homomorphism and $\varphi : \varphi(0) \mapsto$ identity, $\varphi(1) \mapsto f$. Since the automorphism wasn't specified, we can assume that it's referring to the non-trivial φ.

With φ and our two groups defined, we can use these to compute each of the elements in $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. This information is represented in the form of a Cayley Table in Table 1. This is isomorphic to the Cayley Table for D_4, so we know that $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_4$.

Definition 27. Let K and L be groups, and let A be a set that is acted on by K. Recall from Example 18 that if H is the group of functions from A to L, K acts on H. The **wreath product** of L by K, denoted $L \wr K$, is $H \rtimes K$ with regard to this action.

	((0,0),0)	((0,0),1)	((0,1),0)	((0,1),1)	((1,0),0)	((1,0),1)	((1,1),0)	((1,1),1)
((0,0),0)	((0,0),0)	((0,0),1)	((0,1),0)	((0,1),1)	((1,0),0)	((1,0),1)	((1,1),0)	((1,1),1)
((0,0),1)	((0,0),1)	((0,0),0)	((1,0),1)	((1,0),0)	((0,1),1)	((0,1),0)	((1,1),1)	((1,1),0)
((0,1),0)	((0,1),0)	((0,1),1)	((0,0),0)	((0,0),1)	((1,1),0)	((1,1),1)	((1,0),0)	((1,0),1)
((0,1),1)	((0,1),1)	((0,1),0)	((1,1),1)	((1,1),0)	((0,0),1)	((0,0),0)	((1,0),1)	((1,0),0)
((1,0),0)	((1,0),0)	((1,0),1)	((1,1),0)	((1,1),1)	((0,0),0)	((0,0),1)	((0,1),0)	((0,1),1)
((1,0),1)	((1,0),1)	((1,0),0)	((0,0),1)	((0,0),0)	((1,1),1)	((1,1),0)	((0,1),1)	((0,1),0)
((1,1),0)	((1,1),0)	((1,1),0)	((1,0),0)	((1,0),1)	((0,1),0)	((0,1),1)	((0,0),0)	((0,0),1)
((1,1),1)	((1,1),1)	((1,1),0)	((0,1),1)	((0,1),0)	((1,0),1)	((1,0),0)	((0,0),1)	((0,0),0)

Table 2: The Cayley table of $\mathbb{Z}/2\mathbb{Z} \wr S_2$

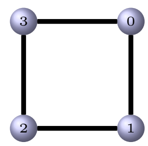


Figure 3: A cycle on four vertices.

Example 28. Let K be $\mathbb{Z}/2\mathbb{Z}$ and let L be S_2, or equivalently $\mathbb{Z}/2\mathbb{Z}$, and let A be a set with two elements acted on by K. Now, we can define H as the group of functions from A to L to compute $L \wr K$. Thus any element of $L \wr K$ is of the form $((x_1, x_2), x_3)$ where $x_1, x_2, x_3 \in \mathbb{Z}/2\mathbb{Z}$. Obviously, $0 \cdot (x_1, x_2) = (x_1, x_2)$, and we can think of (x_1, x_2) as $(f(a), f(b))$ for $a, b \in A$. Then we know that $1 \cdot (x_1, x_2) = (f^1(f(a), f(b))) = (f(1 \cdot a), f(1 \cdot b)) = (f(b), f(a)) = (x_2, x_1)$. Using this, we get the Cayley Table in Table 2, which is once again isomorphic to D_4.

2.3 Algebraic Graph Theory

The definitions below come from [2] and [6].

Definition 29. The **automorphism group** of a graph G, written $\mathrm{Aut}(G)$, is the set of all automorphisms of a graph. It is a permutation group on the vertices of the graph, $V(G)$.

Example 30. Consider the graph in Figure 3. To most people, this is a square. To a graph theorist, it is a C_4. Either way, the symmetries are the same. This is true for any polygon, so $D_n = \mathrm{Aut}(C_n)$.

Lemma 31.

i. *$Aut(K_n)$=S_n.*

ii. *$Aut(G)$=$Aut(\overline{G})$*

iii. *Let G be an unconnected graph where the connected components consist of n_1 copies of G_1, n_2 copies of $G_2, \ldots n_k$ copies of G_k, where $G_1, G_2, \ldots, G_k$ are pairwise non-isomorphic. Then*

$$Aut(G) = (Aut(G_1) \wr S_{n_1}) \times (Aut(G_2) \wr S_{n_2}) \times \ldots \times (Aut(G_k) \wr S_{n_k})$$

Proof.

i. Let K_n be a graph on n vertices. Clearly $\mathrm{Aut}(K_n) \subseteq S_n$. To show that $S_n \subseteq \mathrm{Aut}(K_n)$, let f be a bijection on n elements. We can think of this bijection as a bijective map sending vertices of G to itself. Since every vertex is adjacent to every other vertex, this map must be an automorphism, and thus $f \in \mathrm{Aut}(K_n)$ so $\mathrm{Aut}(K_n) = S_n$.

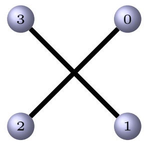
ii. Let $f \in \mathrm{Aut}(G)$. This means that $f(u)$ and $f(v)$ are adjacent exactly when u and v are adjacent, and that $f(u)$ and $f(v)$ are not adjacent when u and v are not adjacent. Thus f is an automorphism of $\mathrm{Aut}(\overline{G})$ as well, so $f \in \mathrm{Aut}(\overline{G})$, and thus $\mathrm{Aut}(G) \subseteq \mathrm{Aut}(\overline{G})$. Reverse inclusion can be shown the same way, establishing that $\mathrm{Aut}(G) = \mathrm{Aut}(\overline{G})$.

iii. Let G be a disconnected graph that consists entirely of n copies of the connected component G'. Let A be the set of components of the graph; we note that S_n acts on A in a natural way. Define H as the group of functions from A to $\mathrm{Aut}(G')$, in other words, it the set of functions that send every component of G to an automorphism of G'. We note that every automorphism of G must send each copy of G' to a copy of G', which can be described by assigning each G' component an automorphism of G' and a component in the graph to map to, which can be written as the tuple (h, k) for $h \in H, k \in S_n$. When composing two automorphisms (h_1, k_1) and (h_2, k_2), we can compose the permutation of components (k_1 and k_2) normally, but when determining what automorphism of G' each component has, we need to account for the permutation of components, which we can do by allowing S_n to act H. Thus we get $(h_1, k_1)(h_2, k_2) = (h_1(k_1 \cdot h_2), k_1k_2)$, which is the definition of the semidirect product. Thus $\mathrm{Aut}(G) = H \rtimes S_n = \mathrm{Aut}(G') \wr S_n$.
Now, let G be a disconnected graph with non-isomorphic components H and J. Clearly any automorphism must send H to $\mathrm{Aut}(H)$ and J to $\mathrm{Aut}(J)$, so $\mathrm{Aut}(G) = \mathrm{Aut}(H) \times \mathrm{Aut}(J)$.
Combining these two parts together, we see that if G is an unconnected graph where the connected components consist of n_1 copies of G_1, n_2 copies of $G_2, \ldots n_k$ copies of G_k, where $G_1, G_2, \ldots, G_k$ are pairwise non-isomorphic, then

$$\mathrm{Aut}(G) = (\mathrm{Aut}(G_1) \wr S_{n_1}) \times (\mathrm{Aut}(G_2) \wr S_{n_2}) \times \ldots \times (\mathrm{Aut}(G_k) \wr S_{n_k}).$$

$\square$

Example 32. As we saw in Example 30, $\mathrm{Aut}(C_4) \cong D_4$. We note that the complement of a four cycle is the disconnected graph of two edges on four vertices, and by Lemma 31, we know that $\mathrm{Aut}(C_4) \cong \mathrm{Aut}(\overline{C_4})$. At the same time, by the same theorem we know that $\mathrm{Aut}(\overline{C_4}) = \mathrm{Aut}(K_2) \wr S_2 \cong \mathbb{Z}/2\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$. In Example 28 we saw that this was congruent to D_4, as expected.



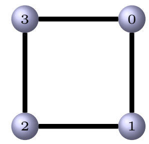


Figure 4: $\text{Cay}(\mathbb{Z}/4\mathbb{Z}; \{2\})$ and $\text{Cay}(\mathbb{Z}/4\mathbb{Z}; \{1, 3\})$

Automorphism groups are important from a graph theory perspective, because many of the more interesting graphs display some kind of symmetry, and this symmetry is reflected in the automorphism group. It is also important from a group theory perspective.

Theorem 33. *[Frucht] Every group is the automorphism group of some graph. Furthermore, if the group is finite, then the graph can be taken to be finite as well.*

Frucht's proof uses Cayley graphs, and can be found in [4].

Definition 34. Let G be a finite group, and let S be a non-empty subset of G such that the identity is not in S and, if $s \in S, s^{-1} \in S$. The **Cayley graph** $\text{Cay}(G; S)$ is defined as the graph where the vertices are elements of G and there is an edge between two vertices u and v exactly when $u = sv$ or $v = su$ for some $s \in S$. The set of all Cayley graphs of a group is denoted $\text{Cay}(G)$.

Example 35. Figure 4 depicts the Cayley graph of $\mathbb{Z}/4\mathbb{Z}$, with sets, respectively, $\{2\}$ and $\{1, 3\}$.

Definition 36. A graph G is **vertex transitive** if there exists $\gamma \in \text{Aut}(G)$ such that γ acts transitively on the vertex set $V(G)$.

Besides coming up with Cayley graphs, Arthur Cayley was also famous for his theorem that every group is isomorphic to a permutation group. Specifically, for a finite group G and $g \in G$, we can define g_R acting on G by $g_R \cdot h = hg$ for all $h \in G$. Then the group $G_R = \{g_R | g \in G\}$ is a permutation group. We can use this to show that every Cayley graph is vertex transitive.

Lemma 37. *The graph Cay($G; S$) is a vertex transtive graph for all groups G and allowed sets S.*

Proof. To show this, it suffices to show that g_R is an automorphism of any Cayley graph on G and that G_R acts transitively on the elements of G.

To begin, let u, v be adjacent vertices in $\text{Cay}(G, S)$ for some suitable set S. Since G_R is transitive, we know that $g_R \cdot u$ and $g_R \cdot v$ are each vertices in $\text{Cay}(G, S)$. By definition $u = sv$ for some $s \in S$, and thus $ug = svg$, so $g_R \cdot u = s(g_R \cdot v)$, and thus $g_R \cdot u$ and $g_R \cdot v$ must be adjacent. Conversely, if $g_R \cdot u$ and $g_R \cdot v$ are adjacent than vertices ug and vg are adjacent, meaning we can write $ug = s(vg) = (sv)g$. This implies $u = ugg^{-1} = svgg^{-1} = sv$,

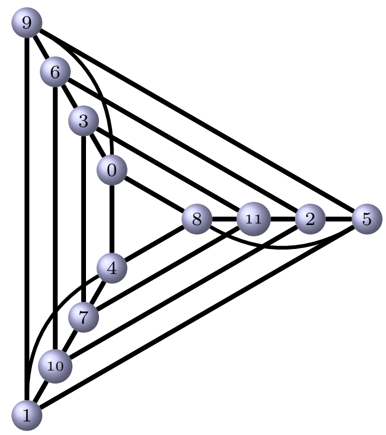


Figure 5: $\mathrm{Cay}(\mathbb{Z}/12\mathbb{Z}; \{3, 4, 8, 9\})$

so u and v are adjacent. Those g_R is a bijection that preserves adjacency, so $g_R \in \mathrm{Aut}(G)$, and $G_R \subseteq \mathrm{Aut}(G)$.

Now, let $a, b \in G$. We note that $a = bb^{-1}a$, so letting $g_R = b^{-1}a$ we have $g_R \cdot b = a$, and thus by definition G_R is transitive. This means that G_R is a subgroup of $\mathrm{Aut}(G)$ acting transitively on the vertices of $\mathrm{Cay}(G; S)$, so $\mathrm{Cay}(G; S)$ must be vertex transitive. □

Definition 38. A graph G is **edge transitive** if there exists $\gamma \in \mathrm{Aut}(G)$ such that γ acts transitively on the edge set $E(G)$.

However, not all Cayley graphs are edge transitive, as shown by Figure 5. The edge between vertex 0 and vertex 4 is clearly part of a cycle of length 3, but the ege between vertex 0 and vertex 3 is not, so there cannot be an automorphism between the two.

A natural question that arises from Definition 34 is when the Cayley graphs of the same group are isomorphic for different sets.

Clearly, if there exists an automorphism α such that $S' = S\alpha$ for sets S, S', then $\mathrm{Cay}(G; S) \cong \mathrm{Cay}(G; S')$, since we can use the automorphism α to relabel the vertices of $\mathrm{Cay}(G, S;)$ to get a graph isomorphic to $\mathrm{Cay}(G; S')$. However, not all isomorphic Cayley graphs have an automorphism between the sets.

Example 39. The Cayley graphs in Figure 6 are clearly isomorphic, as they are each two disjoint cycles on four vertices. However, there can't be any automorphism betweeen $\{7, 9\}$ and $\{1, 3\}$ in $U(16)$ since the former consists entirely of points of order 2 and the latter contains of points of order 4.

From this observation, we get the next two definitions.

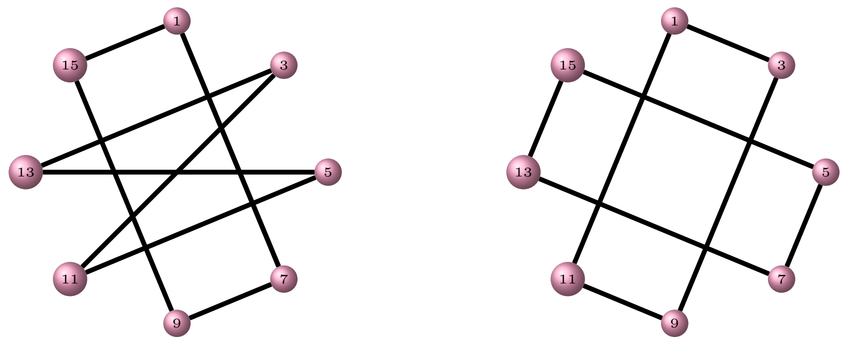


Figure 6: $\mathrm{Cay}(U(16); \{7,9\})$ and $\mathrm{Cay}(U(16); \{1,3\})$

Definition 40. A group is a **CI-group** if $\mathrm{Cay}(G; S)$ and $\mathrm{Cay}(G; S')$ on G are isomorphic if and only if there exists a group automorphism α such that $S' = S\alpha$.

Definition 41. A graph is a **CI-graph** if $\mathrm{Cay}(G; S) \cong \mathrm{Cay}(G; S')$ implies there exists an automorphism α satisfying $S' = S\alpha$.

Classifying groups as CI-groups or their Cayley graphs as CI-graphs is an open problem, although work has been done on the Cayley graphs of cyclic groups. In this paper, we will look at the automorphism group of the Cayley graph of Abelian groups to try and better understand under what conditions a graph will be a CI-graph.

3 Results

Theorem 42. *Let G be a group with n elements. If $Aut(Cay(G; S)) = S_n$, then $Cay(G; S)$ is a CI-graph.*

Proof. Since $\mathrm{Cay}(G; S)$ is a graph on n vertices with automorphism group S_n, any possible relabelling of the vertices must preserve adjacency. This is only possible if the graph is complete or completely disconnected. Since a completely disconnected graph would imply S was empty, $\mathrm{Cay}(G; S)$ must be complete. This means every vertex has degree $n - 1$, so S must contain every element except the identity. For a given graph G, there is only one distinct S, so if $\mathrm{Aut}(\mathrm{Cay}(G; S)) = S_n$, $\mathrm{Cay}(G; S)$ must be a CI-graph. □

Lemma 43. *A graph $Cay(G; S)$ is a CI-graph if and only if $\overline{Cay}(G; S)$ is a CI-graph.*

Proof. Let $\mathrm{Cay}(G, S)$ be a CI-graph. We note that $\overline{\mathrm{Cay}}(G; S) = \mathrm{Cay}(G; \overline{S})$ where $\overline{S}$ is the complement of S in $G \setminus \{1\}$, so it is in fact a Cayley graph. Now suppose that $\mathrm{Cay}(G; \overline{S}) \cong \mathrm{Cay}(G; \overline{S}')$ for some suitable set $\overline{S}'$. Then by definition, $\mathrm{Cay}(G; S') \cong \mathrm{Cay}(G; S)$. Since $\mathrm{Cay}(G; S)$ is a CI-graph, we know there is an automorphism α such that $S = S'\alpha$. Obviously, $\alpha(1) = 1$, so α can be restricted to a bijection from $G \setminus \{1\}$ to $G \setminus \{1\}$. Since α is a bijection from S to S', this implies that it must also be a bijection from $\overline{S} = G \setminus \{1\} \setminus S$ to $\overline{S}' = G \setminus \{1\} \setminus S'$. Thus $\overline{S} = \overline{S}'\alpha$, so $\mathrm{Cay}(G; \overline{S})$ is a CI-graph. The reverse direction works the same way. □

Remark 44. Suppose that G and H are two graphs with the same automorphism group. Each automorphism is a permutation of vertices of the corresponding graph, so it follows that there must be a way to label the vertices of G $g_1, \cdots, g_n$ and the vertices of H $h_1, \cdots, h_n$ such that if σ_g is an automorphism of G and for any $1 \leq i, j \leq n$, $g_j = \sigma_g(g_i)$, then σ_h is the corresponding automorphism of H and $h_j = \sigma_h(h_i)$.

Lemma 45. *The only graphs on $4k$ vertices with automorphism group $D_4 \wr S_k$ are the graph of k disconnected 4-cycles and its complement.*

Proof. Let G be a graph on $4k$ vertices with automorphism group $D_4 \wr S_k$. By Remark 44, we know that we can label the vertices as elements of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ such that if φ is an automorphism sending vertex $(0,0)$ to (i,j), we know that $\{\varphi(1,0), \varphi(3,0)\} \mapsto \{(i+1,j), (i-1,j)\}$, $\varphi(2,0) \mapsto (i+2,j)$, and the only constraint on the other vertices is that they can't map to a vertex with j as the second coordinate. Thus if there is an edge between $(0,0)$ and $(1,0)$ there must be an edge between $(0,0)$ and $(3,0)$ and no edges between $(0,0)$ and (i,j) for all $0 \leq i \leq 3$ and $1 \leq i \leq k$; conversely, if there is no edge between $(0,0)$ and $(1,0)$ there must be no edge between $(0,0)$ and $(3,0)$ but edges between $(0,0)$ and (i,j) for all $j \neq 0$. Because every automorphism sending $(0,0)$ to (i,j) sends $(2,0)$ to $(i+2,j)$, all of the existing automorphims work regardless of whether or not there is an edge between $(0,0)$ and $(2,0)$. However, if there is an edge between $(0,0)$ and $(2,0)$ and between $(0,0)$ and $(1,0)$, it follows by the vertex-transitivity of Cayley graphs that the graph in question must be k disconnected copies of K_4, which has automorphism group $S_4 \wr S_k$, a contradiction. The same reasoning holds for the lack of edge between $(0,0)$ and $(2,0)$ and between $(0,0)$ and $(1,0)$ and the complement of k disconnected copies of K_4. Thus the only graphs on $4k$ vertices with automorphism group $D_4 \wr S_k$ must be k disconnected 4-cycles and its complement. □

Theorem 46. *Let G be a group with $4k$ elements and S a set closed under inverses such that $Aut(Cay(G; S)) = \mathbb{Z}/4\mathbb{Z} \wr S_k$. Then if G is a group with a non-cyclic subgroup of order 2^k containing an element of order 4, $Cay(G; S)$ is not a CI-graph.*

Proof. Let g be an element with order 4 and a, b distinct elements of order 2. We know that such elements exist by the constraints on G. We begin by noting that $\mathrm{Aut}(\mathrm{Cay}(G; \{g, g^{-1}\})) = \mathbb{Z}/4\mathbb{Z} \wr S_k$, since the graph will be k disjoint cycles of length 4, and by theorem 31, we know that it has automorphism group $\mathbb{Z}/4\mathbb{Z} \wr S_k$. Therefore, by Lemma 45 we know that either $\mathrm{Cay}(G; S)$ or its complement is isomorphic to this graph. We may assume without loss of generality that

$\mathrm{Cay}(G;S) \cong \mathrm{Cay}(G;\{g,g^{-1}\})$, since by Lemma 43 its complement is CI exactly when $\mathrm{Cay}(G;S)$ is. Thus we know that S is a two-element set $\{u,v\}$ closed under inverses such that $u^4 = v^4 = 1$. This is only possible if $u^2 = v^2 = 1$, or if $v = u^3 = u^{-1}$. Thus S must be of one of these two forms.

Now, consider $\mathrm{Cay}(G;\{a,b\})$. By construction, there is an edge between the identity 1 vertex and vertex a, as well as an edge between 1 and b. Since G is abelian, we know there is an edge between a and ab and between b and ab, making a C_4. Since there are only two elements in the set for this Cayley graph, it has degree 2, and since it is vertex transitive $\mathrm{Cay}(G;\{a,b\})$ must also be a graph of k disconnected copies of C_4. So $\mathrm{Cay}(G;S) \cong \mathrm{Cay}(G;\{a,b\})$.

For $\mathrm{Cay}(G;S)$ to be a CI-graph, there would have to be automorphisms α_1 and α_2 such that $\{a,b\} = S\alpha_1$ and $\{g,g^{-1}\} = S\alpha_2$. However, $\{a,b\}$ has two elements of order 2, and $\{g,g^{-1}\}$ has none, so there can't be automorphisms between both sets. Thus $\mathrm{Cay}(G;S)$ is not a CI-graph.

□

Corollary 47. *If G is a group with no elements of order 4 and S is a set closed under inverses such that $Aut(Cay(G;S)) = \mathbb{Z}/4\mathbb{Z} \wr S_k$, $Cay(G;S)$ is a CI-graph.*

Proof. As established above, S must consist of two elements of order 2.
Since G is a finite Abelian group, we know by the fundamental theorem governing such groups it has a direct product composition. Since it doesn't have an element of order 4, it must be of the form $\mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z} \times H$ where H is a group of odd order. From this it is clear that there is an automorphism that switches any two elements of order 2, so we must be able to write $S = \{a,b\}\alpha$ for any $\{a,b\}$ of elements of order 2, and thus $\mathrm{Cay}(G;S)$ is a CI-graph. □

Corollary 48. *If G is a group with a non-cyclic subgroup of order 2^k containing an element of order 4, then G is not a CI-group.*

4 Conclusion and Directions for Further Research

Determining when a Cayley graph is a CI-graph is an interesting open problem at the intersection of group theory and graph theory. Much of the work on this problem, such as the results summarized in [**?**] has been done on cyclic groups. As shown in this paper, the automorphism group of Cayley graphs can be used to create theorems about when a graph is a CI-graph and when it is not. Additional research can explore other automorphism groups to draw more conclusions about CI-graphs.

References

[1] Dummit, D. and Foote, R. *Abstract Algebra Third Edition*, John Wiley and Sons, Inc., Massachussets, 2004.

[2] Cameron, P. Automorphisms of graphs. *Topics in Algebraic Graph Theory* Cambridge University Press, New York, 2005.

[3] Godsil, C.D. GRR's for non-solvable groups. *Colloq. Math. Soc. Jànos Bolyai* **25** (1981), 221-239.

[4] Hetzel, D. *Über reguläre graphische Darstellungen von auflösbare Grupen* Diplomarbeit, Techn. Univer. Berlin, 1976.

[5] Behzad, M. and Chartrand, G. *Introduction to the Theory of Graphs* Allyn and Bacon, Inc., 1971.

[6] Alspach, B. Cayley Graphs. *Topics in Algebraic Graph Theory* Cambridge University Press, New York, 2005.