Eulerian and Hamiltonian Cycles in Cayley Graphs

Michael Cavaliere

April 22, 2023

Contents

1 Introduction

Groups are a fundamental area of study in mathematics, in part due to their versatility; whilst they can be studied as purely algebraic objects, groups can also be endowed with additional structure and viewed from the perspective of a vastly different area of mathematics. One such structure that can be given to a group is that of a graph, where the relationships between the elements and the generators of a group can be encoded as vertices and edges respectively. These graphs are called Cayley graphs, and are one of the main objects of study in geometric group theory.

Firstly, I will introduce the group theoretic and graph theoretic background needed start studying Cayley graphs. This will allow me to state and prove some key properties of them. After a brief aside exploring the idea of a minimal generating set, I will move to considering cycles in Cayley graphs; this will include Eulerian cycles, for which I provide a full characterisation of the Cayley graphs which admit them, and Hamiltonian cycles, which are significantly more challenging to characterise and are a current area of research. Finally, I will outline some of the active areas of research relating to Cayley graphs.

2 Introduction to Cayley Graphs

2.1 Generating Sets and Group Presentations

Central to the study of Cayley graphs is the idea of a generating set for a group, as given in the abstract algebra courses [11] and [20].

Definition 2.1.1 **Word**

For a group G with $X \subset G$, a word in X is an expression of the form

$$\prod_{i=1}^{n} x_i^{\varepsilon_i}$$

where $x_1, \dots, x_n \in X$ and $\varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\}$.

Definition 2.1.2 **Reduced Form**

For a group G with $X \subset G$, a word in X is in reduced form if every pair xx^{-1} or $x^{-1}x$ has been replaced by the identity element.

By convention, the identity element is represented by the empty word, so every pair xx^{-1} or $x^{-1}x$ is removed from the word. Note that this does not change the group element it represents.

Definition 2.1.3 **Subgroup Generated by a Subset**

For a group G with $X \subset G$, the subgroup generated by X, denoted $\langle X \rangle$, is the subgroup consisting of all possible words in X.

It is clear that $\langle X \rangle$ is a subgroup of G from the definition, as it consists of all finite products of elements in X and their inverses.

Definition 2.1.4 **Generating Set**

For a group G, $X \subset G$ is a generating set of G if $G = \langle X \rangle$.

If a group has a finite generating set, then it is called finitely generated. In particular, every finite group is finitely generated, as the generating set can be taken to be the whole group, but not every finitely generated group is finite; for example, the additive group of the integers has $\{1\}$ or $\{a, b\}$ for coprime integers a and b, by Bézout's lemma, as possible generating sets.

A generalisation of this counterexample is a family of finitely generated infinite groups called free groups [6, p. 215].

Definition 2.1.5 **Free Group**

For a set X, the free group $F(X)$ generated by a set X is the group consisting of all reduced words in X with concatenation of words followed by reduction as the binary operation.

The intuition behind this definition is that a free group is a group where there are no relations between any of the generators. It is clear from the definition that $F(X)$ is indeed a group, and that a non-trivial finite group cannot be free as the non-identity elements of X must have infinite order.

The additive group of the integers is a free group of rank one, where the rank of a free group is the minimal cardinality of a generating set for the group [6, p. 218]. This generating set with minimum cardinality is called the free generating set of the group.

From the definition of a free group, the definition of a group presentation can be formalised [6, p. 218].

Definition 2.1.6 **Normal Closure**

For a group G, the normal closure of $X \subset G$ is

$$\bigcap_{X \subset N \trianglelefteq G} N$$

Definition 2.1.7 **Group Presentation**

A group G has presentation $\langle X \mid R \rangle$, where $X \subset G$ and $R \subset F(X)$, if $G \cong F(X)/N$, where N is the normal closure of R.

If G has presentation $\langle X \mid R \rangle$, then X is a generating set for G such that for every word $r \in R$, $r = 1$ when r is viewed as an element of G. Typically, the words in R are rewritten as relations in the presentation of G; for example, $C_n = \langle a \mid a^n = 1 \rangle$, $D_{2n} = \left\langle a, b \mid a^n = 1, b^2 = 1, ba = a^{-1}b \right\rangle$ and $\mathrm{Dic}_{4n} = \left\langle a, b \mid a^{2n} = 1, a^n = b^2, ba = a^{-1}b \right\rangle$ are some standard presentations of common families of finite groups.[1]

Every group has a presentation, as the kernel of the homomorphism $\phi : F(G) \to G$ where the restriction to G is the identity map is normal in $F(G)$, and so by the first isomorphism theorem, $F(G)/\ker(\phi) \cong \mathrm{im}(\phi) = G$. The free group $F(X) \cong F(X)/\{1\}$ must have presentation $\langle X \mid \emptyset \rangle$, and this is generally notated as $\langle X \mid \, \rangle$. This fits with the intuition of the free group having no relations between its generators.

However, not every group has a finite presentation, where both the generating set X and the set of relations R are finite; finite groups always have a finite presentation, as the whole group can be taken as the generating set with at most $|G|^2$ relations, as every possible product can be taken as a relation.

[1] The dicyclic group Dic_8 is more commonly known as the quaternion group Q_8.

2.2 Graph Theoretic Definitions

Before stating the definition of a Cayley graph, I first review some basic graph theoretic definitions, as stated in the combinatorics course [18].[2]

Definition 2.2.1 **Graph**
A graph (V, E) consists of a set of vertices V and a set of edges E such that every edge is given by the unordered pair $\{u, v\}$ for some $u, v \in V$.

A subgraph of a graph (V, E) is a graph (V', E') such that $V' \subset V$ and $E' \subset E$, where V' must contain all endpoints of edges in E'. A spanning subgraph is a subgraph containing all the vertices of the original graph.

Definition 2.2.2 **Degree**
For a graph (V, E), the degree of a vertex $v \in V$, denoted $\deg v$, is the number of edges $e \in E$ such that $v \in e$.

Definition 2.2.3 **Paths and Cycles**
For a graph (V, E), a path between vertices $u, v \in V$ is a sequence $\{e_0, e_1, \ldots, e_n\} \subset E$ such that $e_i = \{w_i, w_{i+1}\}$ for $i \in [0, n]$ with $w_0 = u$, $w_{n+1} = v$ and $i \neq j \implies w_i \neq w_j$ for $i, j \in [1, n]$. A cycle is a path where $u = v$.

A graph containing at least one cycle is called cyclic, and a graph with no cycles is called acyclic.

Definition 2.2.4 **Connected**
A graph (V, E) is connected if $\forall u, v \in V$, there is a path between u and v.

A subgraph is a connected component if it is connected and is not a subgraph of any larger connected subgraph.

Definition 2.2.5 **Tree**
A graph Γ is a tree if it is connected and acyclic.

The definition of a graph can be adapted to allow for directed graphs, which can encode additional information about relationships between vertices and edges, as in the following definitions adapted from [9, pp. 2–11]:

Definition 2.2.6 **Directed Graph**
A directed graph (V, E) consists of a set of vertices V and a set of edges E such that every edge is given by the ordered pair (u, v) for some $u, v \in V$.

In practice, rather than a purely directed graph, I will consider a mixed graph where an undirected edge $\{u, v\}$ will be used in the graph if $(u, v), (v, u) \in E$. This simplifies the presentation of the graph and is the convention when considering Cayley graphs [15, p. 21].

For a directed edge (u, v), the vertex u is the tail of (u, v) and the vertex v is the head of (u, v).

[2] The definition of a graph used here is that of a simple graph; this differs from a multigraph, which allows for multiple edges between the same pair of vertices and loops connecting vertices to themselves. Similarly, directed graphs are assumed to be simple, with no multiple edges between the same vertices with the same direction or loops.

Definition 2.2.7 **Underlying Graph**
The underlying graph of a directed graph (V, E) is the undirected graph (V, E') such that $E' = \{\{u, v\} : (u, v) \in E\}$.

The concept of the degree of a vertex can be adapted for directed graphs by considering the in-degree and out-degree, which characterises the incoming and outgoing directed edges for a vertex.

Definition 2.2.8 **In-Degree and Out-Degree**
For a directed graph (V, E), the in-degree of a vertex $v \in V$, denoted $\deg^- v$, is the number of edges $e \in E$ such that $e = (u, v)$ for some $u \in V$. The out-degree of a vertex $v \in V$, denoted $\deg^+ v$, is the number of edges $e \in E$ such that $e = (v, u)$ for some $u \in V$.

Similarly, the notion of connectivity can be extended to directed graphs, using the following definitions given in [9, pp. 57–58].

Definition 2.2.9 **Weakly Connected**
A directed graph is weakly connected if its underlying graph is connected.

Definition 2.2.10 **Paths and Cycles in Directed Graphs**
For a directed graph (V, E), a path between vertices $u, v \in V$ is a sequence $\{e_0, e_1, \ldots, e_n\} \subset E$ such that $e_i = (w_i, w_{i+1})$ for $i \in [0, n]$ with $w_0 = u$, $w_{n+1} = v$ and $i \neq j \implies w_i \neq w_j$ for $i, j \in [1, n]$. A cycle is a path where $u = v$.

As in the undirected case, a directed graph containing at least one cycle is called cyclic, and a directed graph with no cycles is called acyclic. The definition of a tree extends to directed graphs, where a directed graph is a tree if its underlying graph is a tree. This is a stronger condition than simply being acyclic, as an acyclic directed graph could have a cyclic underlying graph as cycles in directed graphs are directed.

In a similar way, there is a stronger notion of connectivity in directed graphs:

Definition 2.2.11 **Strongly Connected**
A directed graph (V, E) is strongly connected if $\forall u, v \in V$, there is a path from u to v and a path from v to u.

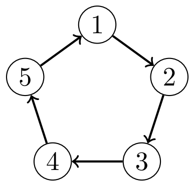
The definition of connected components generalises to weakly connected components and strongly connected components in directed graphs.

It is clear from the definition that a directed graph being strongly connected implies that it is weakly connected, but that the two concepts are not equivalent.

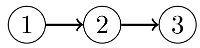
The Cartesian product on sets can be generalised to the Cartesian product of graphs, as given in [9, pp. 105–106].[3]

Definition 2.2.12 **Cartesian Product**
The Cartesian product of two (directed) graphs $\Gamma = (V_1, E_1)$ and $\Gamma' = (V_2, E_2)$ is the graph $\Gamma \times \Gamma' = (V_1 \times V_2, E)$, where

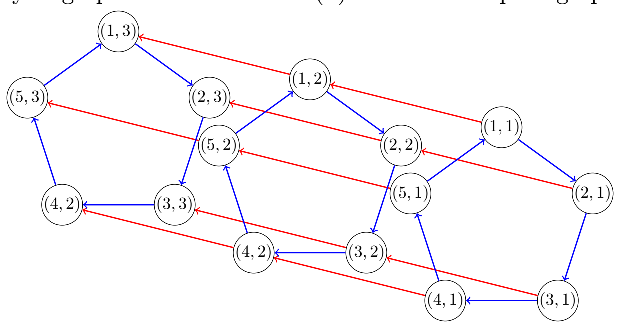
$$E = \{((u, v), (u, w)) : u \in V_1, (v, w) \in E_2\} \cup \{((u, w), (v, w)) : w \in V_2, (u, v) \in E_2\}$$



(a) The directed cycle graph on five vertices.



(b) The directed path graph on three vertices.



(c) The Cartesian product of the two directed graphs.

Figure 1: The Cartesian product of a directed cycle and a directed path, with the component factors highlighted in blue and red respectively.

Whilst the definition may seem unintuitive, when visualised, the Cartesian product of graphs is a natural definition, as seen in Figure 1.[4]

The idea of a graph isomorphism can also be defined for both undirected and directed graphs, with the two definitions being analogous [9, p. 65].

Definition 2.2.13 **Isomorphic**

Two (directed) graphs (V_1, E_1) *and* (V_2, E_2) *have an isomorphism* $\phi : V_1 \to V_2$ *between them if* ϕ *is a bijection such that* $(u, v) \in E_1 \iff (\phi(u), \phi(v)) \in E_2$*. Then,* (V_1, E_1) *and* (V_2, E_2) *are isomorphic with* $(V_1, E_1) \cong (V_2, E_2)$*.*

Isomorphisms $V \to V$ for a directed graph $\Gamma = (V, E)$ are known as automorphisms and the set of all automorphisms on Γ is notated as $\mathrm{Aut}(\Gamma)$. The set of automorphisms of a graph can be thought of as the set of all symmetries of the graph, and this gives a group with respect to composition of functions.

Proposition 2.2.14

For a (directed) graph Γ*,* $\mathrm{Aut}(\Gamma)$ *is a group with composition of functions.*

Proof. Let $\Gamma = (V, E)$. For any $\phi, \psi \in \mathrm{Aut}(\Gamma)$, $\phi : V \to V$ and $\psi : V \to V$ are both bijections so $\psi \circ \phi : V \to V$ is a bijection. As ϕ and ψ are isomorphisms, $(u, v) \in E \iff (\phi(u), \phi(v)) \in E \iff (\psi(\phi(u)), \psi(\phi(v))) \in E$, so $\psi \circ \phi \in \mathrm{Aut}(\Gamma)$ and hence $\circ$ is a binary operation on $\mathrm{Aut}(\Gamma)$.

The map $I : V \to V$ where $v \mapsto v$ is clearly an automorphism, so $I \in \mathrm{Aut}(\Gamma)$. Since for $\phi \in \mathrm{Aut}(\Gamma)$, $I \circ \phi = \phi \circ I = \phi$ by definition, I is an identity element for $\mathrm{Aut}(\Gamma)$.

[3] All the following definitions and results regarding directed graphs also hold in the undirected case with very similar proofs.

[4] Often, the Cartesian product of graphs Γ and Γ' is denoted $\Gamma \square \Gamma'$ and referred to as the graph box product to avoid confusion with the graph tensor product. However, in this essay the tensor product will not be used so $\Gamma \times \Gamma'$ is used unambiguously.

For $\phi \in \mathrm{Aut}(\Gamma)$, as ϕ is a bijection, ϕ^{-1} exists and is a bijection. As $(u,v) \in E \iff (\phi(u),\phi(v)) \in E$, by definition of an inverse function, $\big(\phi^{-1}(u),\phi^{-1}(v)\big) \in E \iff (u,v) \in E$, so $\phi^{-1} \in \mathrm{Aut}(\Gamma)$.

For any $\phi,\psi,\pi \in \mathrm{Aut}(\Gamma)$, $\phi \circ (\psi \circ \pi) = (\phi \circ \psi) \circ \pi$ by definition of composition of functions, so associativity holds.

Hence, $\mathrm{Aut}(\Gamma)$ is a group with composition of functions. □

The automorphism group of a directed graph can be used to characterise certain graphs, including a useful property of Cayley graphs using the following definition [8, p. 33]:

Definition 2.2.15 **Vertex Transitive**
A (directed) graph $\Gamma = (V,E)$ is vertex transitive if its automorphism group $\mathrm{Aut}(\Gamma)$ acts transitively on its vertices.

An intuitive description of a directed graph that is vertex transitive is that it is a graph where structurally there is no way to differentiate the vertices of the graph from each other if they are unlabelled, as for the action to be transitive - meaning it has only one orbit - there must be for all vertices $u,v \in V$ some $\phi \in \mathrm{Aut}(\Gamma)$ such that $\phi(u) = v$.

2.3 Definition and Properties of Cayley Graphs

Cayley graphs are a representation of the structure of a group inspired by the following famous theorem in group theory [15, p. 4, 19–20]:

Theorem 2.3.1 **Cayley's Theorem**
Every group G is isomorphic to a subgroup of the symmetric group $\mathrm{Sym}(G)$.

Proof. Consider the operation $\cdot : G \times G \to G$ defined by $g \cdot x = gx$. Clearly $1 \cdot x = x$ and $g \cdot (h \cdot x) = g \cdot (hx) = (gh)x = (gh) \cdot x$, so $\cdot$ is an action.

As $\cdot$ is an action, the map $\phi : G \to \mathrm{Sym}(G)$, where $\phi(g)$ is the function $x \mapsto g \cdot x$, is a homomorphism. Since $g \cdot x = x \iff g = 1$, $\cdot$ is faithful and so $G/\ker(\phi) \cong G$. By the first isomorphism theorem, this implies that $G \cong \mathrm{im}(\phi) \leq \mathrm{Sym}(G)$. □

Cayley's Theorem shows that every group can be represented by a group of permutations of its elements. This result can be extended to show that every group is isomorphic to a subgroup of the symmetry group of a particular directed graph.

Corollary 2.3.2
Every group G is isomorphic to a subgroup of the automorphism group $\mathrm{Aut}(\Gamma)$ for a directed graph Γ with vertex set equal to G.

Proof. For $X \subset G$, consider the directed graph $\Gamma_{G,X}$ with vertex set G and edge set $E = \{(g,gx) : g \in G, x \in X\}$. Since G acts on itself by left multiplication, $\cdot : G \times E \to E$ defined by $h \cdot (g,gx) = (hg,hgx)$ is an action.

Note that $(g,gx) \mapsto h \cdot (g,gx)$ is in $\mathrm{Aut}(\Gamma_{G,X})$ by the cancellation law, as $(g,k) \in E \iff k = gx \iff hk = hgx \iff (hg,hk) \in E$ for $g,h,k \in G$ and $x \in X$.

As $\cdot$ is an action, the map $\phi : G \to \mathrm{Aut}(\Gamma_{G,X})$, where $\phi(h)$ is the function $(g,gx) \mapsto h \cdot (g,gx)$, is a homomorphism. Since $h \cdot (g,gx) = (g,gx) \iff h = 1$ as left multiplication is a faithful action, $\cdot$ is faithful and so $G/\ker(\phi) \cong G$. By the first isomorphism theorem, this implies that $G \cong \mathrm{im}(\phi) \leq \mathrm{Aut}(\Gamma_{G,X})$. □

This shows that every group can be represented by a group of permutations of a directed graph with vertex set equal to the group. This graph is known as a Cayley graph of the group [15, p. 21].

Definition 2.3.3 **Cayley Graph**
For a group G and $X \subset G$, the Cayley graph of G with respect to X is the directed graph $\mathrm{Cay}(G, X)$ with vertex set equal to G and edge set $\{(g, gx) : g \in G, x \in X\}$.

When discussing Cayley graphs, an edge (g, gx) is said to be generated by $x \in X$. When drawn out, Cayley graphs are often edge-coloured, where each edge is coloured based on its generator.

As I am only considering simple graphs, X is assumed throughout to be a proper subset of G with $1 \notin X$. Furthermore, as mentioned above, Cayley graphs are typically mixed graphs rather than purely directed, where an undirected edge is used if (g, gx) and (gx, g) are both edges generated by the same element; that is, when $|x| = 2$.

Many authors choose to define Cayley graphs as requiring a generating set rather than any subset of the group, but as seen in Figure 2, any subset of the group can be used. The following two results, which are generalisations of a result stated in [21, p. 132] for finite groups without proof, justify this convention.

Proposition 2.3.4
For a group G and $X \subset G$, $\mathrm{Cay}(G, X)$ is weakly connected if and only if $G = \langle X \rangle$.

Proof. Suppose that $\mathrm{Cay}(G, X)$ is weakly connected. By definition, this means there is a path between h and g in the underlying graph for any $g, h \in G$. In particular, this holds for all $g \in G$ and $h \in X$. By definition of a Cayley graph, every edge in the underlying graph is of the form $\{k, kx\}$ for some $k \in G$ and $x \in X$. This implies, using the definition of a path, that there is some $x_1, \ldots, x_n \in X$ and $\varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}$ such that

$$g = h \prod_{i=1}^{n} x_i^{\varepsilon_i}$$

As $h \in X$, this implies that $g \in \langle X \rangle$, and hence $G = \langle X \rangle$.

Suppose that $G = \langle X \rangle$. For any $g, h \in G$, $g^{-1}h \in G$ so there is some $x_1, \ldots, x_n \in X$ such that

$$g^{-1}h = \prod_{i=1}^{n} x_i^{\varepsilon_i} \iff h = g \prod_{i=1}^{n} x_i^{\varepsilon_i}$$

where $\varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}$. By definition of a Cayley graph, every edge in the underlying graph is of the form $\{k, kx\}$ for some $k \in G$ and $x \in X$, so this product describes a path in the underlying graph between g and h. Since this holds for any $g, h \in G$, this implies that $\mathrm{Cay}(G, X)$ is weakly connected. □

Corollary 2.3.5
For a group G and $X \subset G$ where every element of X has finite order, if $\mathrm{Cay}(G, X)$ is weakly connected, then $\mathrm{Cay}(G, X)$ is strongly connected.

Proof. By Proposition 2.3.4, $G = \langle X \rangle$. For any $g, h \in G$, $g^{-1}h \in G$ so there is some $x_1, \ldots, x_n \in X$ such that

$$g^{-1}h = \prod_{i=1}^{n} x_i^{\varepsilon_i} \iff h = g \prod_{i=1}^{n} x_i^{\varepsilon_i}$$

where $\varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}$. Since every $x_i \in X$ has finite order n_i,

$$h = g \prod_{i=1}^{n} x_i^{k_i}$$

where $k_i \in \{0, \ldots, n_i - 1\}$ by taking $k_i \equiv \varepsilon_i \pmod{n_i}$. This means that h can be written as a product of g and a product of elements of X.

By definition of a Cayley graph, every edge is of the form (k, kx) for some $k \in G$ and $x \in X$, so this product describes a path from g to h. Since this holds for any $g, h \in G$, this implies that $\mathrm{Cay}(G, X)$ is strongly connected. $\square$

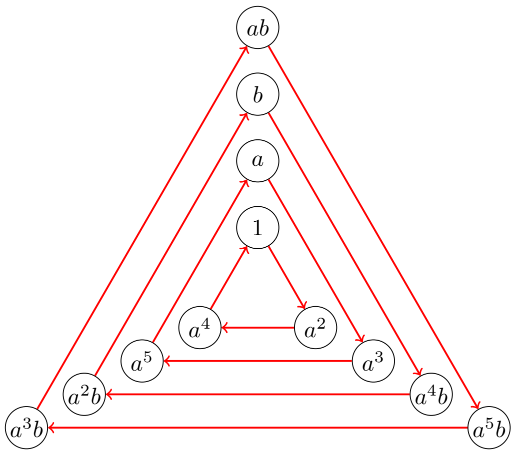


Figure 2: The Cayley graph $\mathrm{Cay}\big(\mathrm{Dic}_{12}, \{a^2\}\big)$ with respect to a non-generating subset.

This shows that Cayley graphs generated by a generating set for the group are exactly those which are weakly connected. For sets where the elements have finite order, the Cayley graphs generated by a generating set for the group are exactly those which are strongly connected.

The notion of connectivity in Cayley graphs can be extended to considering the connected components of $\mathrm{Cay}(G, X)$ where $G \neq \langle X \rangle$, which represent the cosets with respect to $\langle X \rangle$, as seen in the following result from [21, p. 134].

Proposition 2.3.6
For a group G with $g, h \in G$ and $X \subset G$, g and h are in the same coset of $\langle X \rangle$ in G if and only if g and h are vertices in the same weakly connected component of $\mathrm{Cay}(G, X)$.

Proof. Suppose that $g, h \in k\langle X \rangle$ for some $k \in G$. Then, $g = kx_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n}$ and $h = ky_1^{\mu_1} \ldots y_m^{\mu_m}$ for some $x_1, \ldots, x_n, y_1, \ldots, y_m \in X$ and $\varepsilon_1, \ldots, \varepsilon_n, \mu_1, \ldots, \mu_m \in \{\pm 1\}$. Hence,

$$\begin{aligned} g^{-1}h &= x_n^{-\varepsilon_n} \ldots x_1^{-\varepsilon_1} k^{-1} k y_1^{\mu_1} \ldots y_m^{\mu_m} \\ &= x_n^{-\varepsilon_n} \ldots x_1^{-\varepsilon_1} y_1^{\mu_1} \ldots y_m^{\mu_m} \\ \implies h &= g x_n^{-\varepsilon_n} \ldots x_1^{-\varepsilon_1} y_1^{\mu_1} \ldots y_m^{\mu_m} \end{aligned}$$

By definition of a Cayley graph, every edge in the underlying graph is of the form $\{a, ax\}$ for some $a \in G$ and $x \in X$, so this product describes a path in the underlying graph between g and h. Hence, every element in the coset $k\langle X\rangle$ belongs to a weakly connected component.

Suppose that $g, h \in G$ belong to the same weakly connected component of $\mathrm{Cay}(G, X)$ and that $h \in k\langle X\rangle$ for some $k \in G$. By definition, this means there is a path between h and g in the underlying graph for any $g, h \in G$. In particular, this holds for all $g \in G$ and $h \in X$. By definition of a Cayley graph, every edge in the underlying graph is of the form $\{a, ax\}$ for some $a \in G$ and $x \in X$. This implies, using the definition of a path, that there is some $x_1, \ldots, x_n \in X$ and $\varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}$ such that

$$g = h \prod_{i=1}^{n} x_i^{\varepsilon_i}$$

As $h \in k\langle X\rangle$, this implies that $g \in k\langle X\rangle$. □

The results regarding connectivity in Cayley graphs with respect to generating sets can then be used to prove the following corollary:

Corollary 2.3.7
For a group G with $g, h \in G$ and $X \subset G$ where every element of X has finite order, g and h are in the same coset of $\langle X\rangle$ in G if and only if g and h are vertices in the same strongly connected component of $\mathrm{Cay}(G, X)$.

Proof. By Proposition 2.3.6, g and h are in the same coset of $\langle X\rangle$ if and only if g and h are vertices in the same weakly connected component of $\mathrm{Cay}(G, X)$. Hence, each weakly connected component of $\mathrm{Cay}(G, X)$ can be considered as the graph $\mathrm{Cay}(\langle X\rangle, X)$ up to relabelling of vertices. By Corollary 2.3.5, $\mathrm{Cay}(\langle X\rangle, X)$ is therefore strongly connected, and so g and h are in the same coset of $\langle X\rangle$ if and only if g and h are vertices in the same strongly connected component of $\mathrm{Cay}(G, X)$. □

The definition of a Cayley graph does allow for infinite groups and infinite generating sets; for example, Figure 3 shows the Cayley graph of the free group of rank one and the free group of rank two with respect to their free generating sets.

It follows from the definition of a Cayley graph that cycles represent the relations satisfied by the generators of the graph. Based on this, I propose and prove the following characterisation of Cayley graphs:[5]

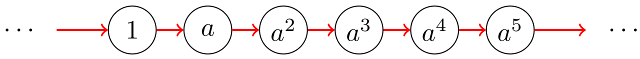
Proposition 2.3.8
For a group G with $G = \langle X\rangle$ and $|G| > 2$, $\mathrm{Cay}(G, X)$ *is a tree if and only if $G \cong F(X)$.*

Proof. Suppose that $\mathrm{Cay}(G, X)$ has a cycle $C = \{\{g_0, g_1\}, \ldots, \{g_{n-1}, g_n\}\}$ in its underlying graph, where $g_0 = g_n$. By definition of a Cayley graph, every edge in the underlying graph is of the form $\{g, gx\}$ for some $g \in G$ and $x \in X$, so

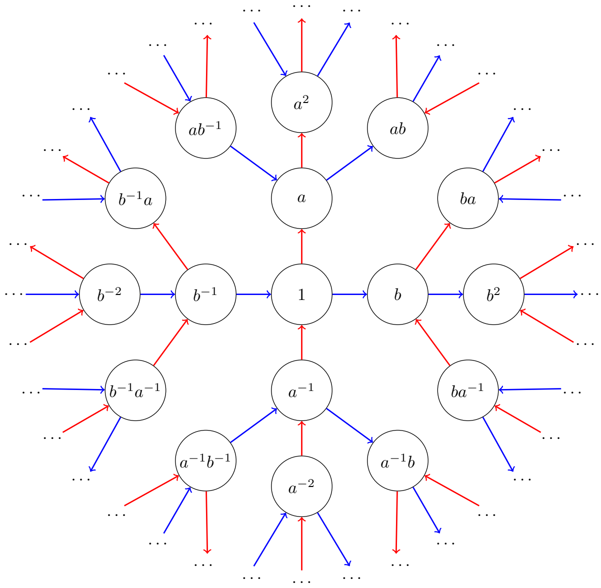
$$g_n = g_0 \prod_{i=1}^{n} x_i^{\varepsilon_i} \iff \prod_{i=1}^{n} x_i^{\varepsilon_i} = 1$$

for some $x_1, \ldots, x_n \in X$ and $\varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}$. This implies that G has presentation $\langle X \mid R\rangle$ where $x_1 \ldots x_n \in R \subset F(X)$. Hence, $R \neq \emptyset$ and so $G \ncong F(X)$.

[5]Note that $|G| = 2 \iff G \cong C_2$ and so the Cayley graph of G with respect to the only possible generating set has two vertices and one undirected edge between them as the single generator has order two, so it is a tree. When $|G| = 1$, $G \cong \{1\} \cong F(\{1\})$ and the Cayley graph has one vertex and no edges since the generating set of a Cayley graph cannot contain the identity, so it is a tree.



(a) The Cayley graph $\mathrm{Cay}(F(\{a\}), \{a\})$



(b) The Cayley graph $\mathrm{Cay}(F(\{a,b\}), \{a,b\})$

Figure 3: Cayley graphs of the free groups of rank one and rank two with respect to their free generating sets.

Suppose that G is not a free group. Then, G has presentation $\langle X \mid R\rangle$ where $R \neq \emptyset$. For $r \in R$, since r is a word in X,

$$r = \prod_{i=1}^{n} x_i^{\varepsilon_i} \iff gr = g\prod_{i=1}^{n} x_i^{\varepsilon_i}$$

for some $x_1, \ldots, x_n \in X$ and $\varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}$. By definition of a Cayley graph, every edge in the underlying graph is of the form $\{g, gx\}$ for some $g \in G$ and $x \in X$, so this product describes a cycle in the underlying graph of $\mathrm{Cay}(G, X)$, so the graph is not a tree. □

It follows from this that Cayley graphs generated by elements with finite order must be cyclic.

Corollary 2.3.9
For a group G with $G = \langle X\rangle$ and $|G| > 2$, if every element of X has finite order, then $\mathrm{Cay}(G, X)$ is cyclic.

Proof. By Proposition 2.3.8, the underlying graph of $\mathrm{Cay}(G, X)$ is cyclic. Consider a cycle $C = \{\{g_0, g_1\}, \ldots, \{g_{n-1}, g_n\}\}$ in the underlying graph, where $g_0 = g_n$. By definition of a Cayley graph, every edge in the underlying graph is of the form $\{g, gx\}$ for some $g \in G$ and $x \in X$, so

$$g_n = g_0 \prod_{i=1}^{n} x_i^{\varepsilon_i}$$

for some $x_1, \dots, x_n \in X$ and $\varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\}$. Since each element $x_i \in X$ has finite order n_i,

$$g_n = g_0 \prod_{i=1}^{n} x_i^{k_i}$$

where $k_i \in \{0, \dots, n_i - 1\}$ by taking $k_i \equiv \varepsilon_i \pmod{n_i}$. This means that g_n can be written as a product of g_0 and a product of elements of X, which corresponds to a path from g_0 to $g_n = g_0$, and hence a cycle in the directed graph $\mathrm{Cay}(G, X)$. □

In practice, most study of Cayley graphs concerns finite groups, including this essay. When working with finite groups, Cayley graphs with respect to any generating set are strongly connected and cyclic, as every element in a group with finite order must have finite order.

Just as the direct product of groups can be used to construct new groups, the Cartesian product of Cayley graphs can be used to construct new Cayley graphs, as is immediate from the definitions.

Proposition 2.3.10
If G and H are groups with $G = \langle X \rangle$ and $H = \langle Y \rangle$, then $Z = (X \times \{1\}) \cup (\{1\} \times Y)$ is a generating set for $G \times H$ and $\mathrm{Cay}(G \times H, Z) \cong \mathrm{Cay}(G, X) \times \mathrm{Cay}(H, Y)$.

Proof. For any $(g, h) \in G \times H$, $(g, 1) \in \langle X \times \{1\} \rangle$ and $(1, h) \in \langle Y \times \{1\} \rangle$. Since $(g, h) = (g, 1)(1, h)$, any element of $G \times H$ can be written as the product of a word in $X \times \{1\}$ and a word in $\{1\} \times Y$. Hence, $G \times H = \langle (X \times \{1\}) \cup (\{1\} \times Y) \rangle$.

By definition of the direct product of groups, the vertex set of $\mathrm{Cay}(G \times H, Z)$ is $V = \{(g, h) : g \in G, h \in H\}$ and the edge set of $\mathrm{Cay}(G \times H, Z)$ is

$$E = \{((g, h), (gx, h)) : g \in G, h \in H, x \in X\} \cup \{((g, h), (g, hy)) : g \in G, h \in H, y \in Y\}$$

This is precisely the definition of the vertex and edge sets of $\mathrm{Cay}(G, X) \times \mathrm{Cay}(H, Y)$, by definition of the Cartesian product of graphs. □

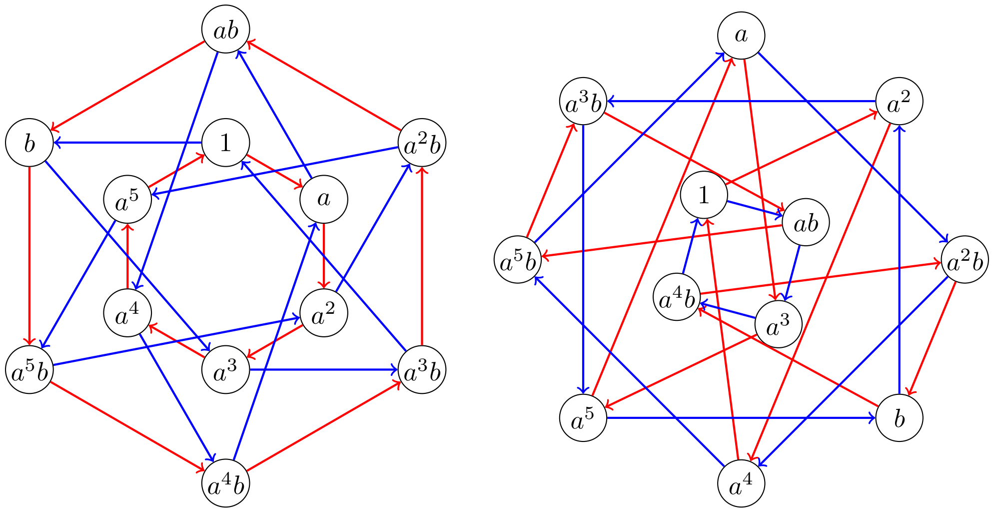
The Cayley graph of a group is not unique; different generating sets for a given group will produce different Cayley graphs. For example, in Figure 4, it is clear that $\mathrm{Cay}(\mathrm{Dic}_{12}, \{a, b\})$ has a cycle of length 6 but $\mathrm{Cay}\big(\mathrm{Dic}_{12}, \{a^2, ab\}\big)$ does not. This is why specifying the generating set for a given Cayley graph is crucial.

Furthermore, although Proposition 2.3.10 shows that Cayley graphs of direct products of groups can be constructed using the Cartesian product, not every Cayley graph of a direct product of groups $G \times H$ will be isomorphic to some Cartesian product of Cayley graphs of G and H. For example, $C_2 \times C_3 \cong C_6$ and so $\mathrm{Cay}(C_2 \times C_3, \{(a, b)\})$ is a connected Cayley graph for $C_2 = \langle a \rangle$ and $C_3 = \langle b \rangle$, but it is not isomorphic to any Cartesian product of Cayley graphs of C_2 and C_3.

The following result is taken from [8, p. 35] and gives another important property of Cayley graphs.

Theorem 2.3.11
For a group G and $X \subset G$, $\mathrm{Cay}(G, X)$ is vertex transitive.

Proof. As shown in Corollary 2.3.2, $\phi(g) : G \to G$ defined by $x \mapsto gx$ is an automorphism of $\mathrm{Cay}(G, X)$. The set $\{\phi(g) : g \in G\}$ is a subgroup of $\mathrm{Aut}(\Gamma)$ as it contains the identity map and for all $g, h \in G$, $(\phi(h))^{-1} \circ \phi(g) = \phi\big(h^{-1}\big) \circ \phi(g) = \phi\big(h^{-1}g\big)$ so $(\phi(h))^{-1} \circ \phi(g) \in \mathrm{Aut}(\Gamma)$. This subgroup acts transitively on G as for all $g, h \in G$, $\big(\phi\big(g^{-1}h\big)\big)(g) = g\big(g^{-1}h\big) = h$. Hence, $\mathrm{Cay}(G, X)$ is vertex transitive. □



(a) $\mathrm{Cay}(\mathrm{Dic}_{12}, \{a, b\})$ (b) $\mathrm{Cay}\big(\mathrm{Dic}_{12}, \{a^2, ab\}\big)$

Figure 4: Cayley graphs of Dic_{12} with respect to different generating sets.

Although all Cayley graphs are vertex transitive, not all vertex transitive graphs are Cayley graphs for some group. For example, the Petersen graph P is vertex transitive but cannot be a Cayley graph for any group [8, p. 35]. I prove this result using the Kneser graph labelling of P, where every vertex is labelled by a two-element subset of $\{1, \ldots, 5\}$ such that vertices are connected by an edge if and only if their labels are disjoint.

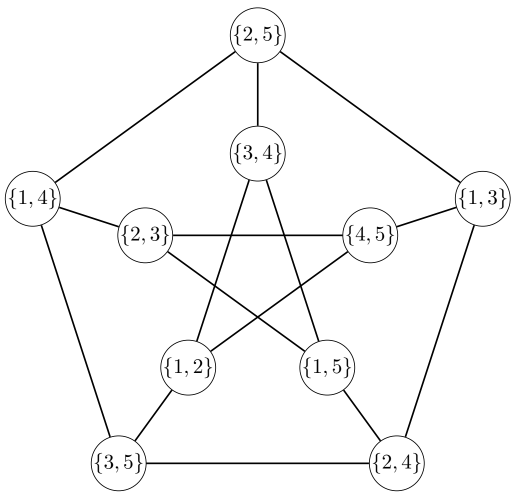


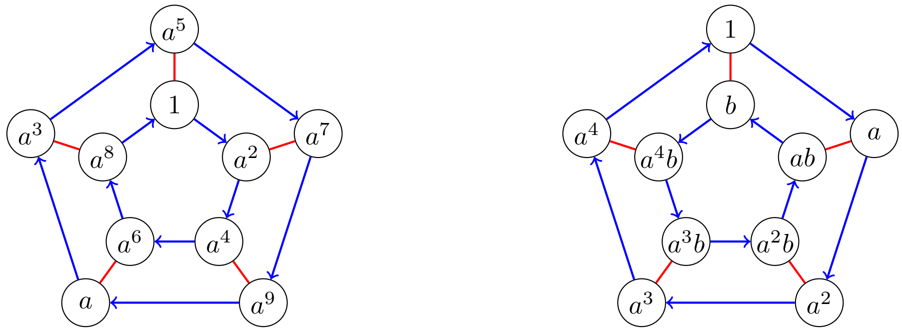
Figure 5: The Petersen graph depicted using its Kneser graph labelling.

Proposition 2.3.12
The Petersen graph P is vertex transitive but not a Cayley graph.

Proof. P is vertex transitive as, using the Kneser graph labelling of the vertices given in Figure 5, any permutation in S_5 induces a permutation of the vertices with $\{a, b\} \cap$

$\{c,d\} = \emptyset \iff \{\sigma(a),\sigma(b)\} \cap \{\sigma(c),\sigma(d)\} = \emptyset$ for $\sigma \in S_5$, so $S_5 \le \mathrm{Aut}(P)$, which implies that P is vertex transitive.

As all groups of order 10 are isomorphic to either C_{10} or D_{10}, if $P = \mathrm{Cay}(G,X)$, then $G \cong C_{10}$ or $G \cong D_{10}$. As all vertices of P have degree 3, $X = \{x,y\} \subset G$ where $|x| = 2$ and $|y| > 2$. If $G \cong C_{10}$, then G is abelian and so $xy^{-1}xy = 1$. This implies that $xy^{-1}xy$ gives a cycle of length 4 in the underlying graph of $\mathrm{Cay}(G,X)$, but P has no such cycles. If $G \cong D_{10}$, then $|y| = 5$ by Lagrange's theorem. As $D_{10} = \langle x, y \mid y^5 = 1, x^2 = 1, xy = y^{-1}x \rangle$, $(xy)^2 = 1$ and so there is again a cycle of length 4 in $\mathrm{Cay}(G,X)$. As these are the only two options for a group of order 10, P cannot be a Cayley graph. □



(a) $\mathrm{Cay}\big(C_{10}, \{a^2, a^5\}\big)$ (b) $\mathrm{Cay}(D_{10}, \{a, b\})$

Figure 6: Examples of Cayley graphs of groups with order ten for generating sets of size two and one generator of order two.

Vertex transitivity provides a stronger characterisation of exactly which directed graphs are Cayley graphs. The following theorem is taken from [17, p. 802], although the proof has been omitted from this essay.

Theorem 2.3.13 **Sabidussi's Theorem**
An unlabelled directed graph $\Gamma = (V,E)$ is isomorphic to a Cayley graph $\mathrm{Cay}(G,X)$ for some $X \subset G$ if and only if there is some $H \le \mathrm{Aut}(\Gamma)$ such that $|H| = |V|$ and H acts transitively on V. In this case, $G \cong H$.

2.4 Minimal Generating Sets

The following definition is taken from [10, p. 355]:

Definition 2.4.1 **Minimal Generating Set**
For a group G, a minimal generating set is $X \subset G$ such that no proper subset of X is a generating set of G.

Note that a group can have multiple minimal generating sets of different cardinalities; for example, considering again the additive group of the integers, both the generating sets $\{1\}$ and $\{2,3\}$ would be minimal. This is not unique to infinite groups; in fact, most groups have minimal generating sets of different cardinalities. For example, the cyclic group $C_{10} = \langle a \mid a^{10} = 1 \rangle$ has both $\{a\}$ and $\{a^2, a^5\}$ as minimal generating sets. The maximal cardinality of a minimal generating set for a group G is denoted $m(G)$ and the minimal cardinality is denoted $d(G)$. If a group is finite, then there exists a minimal generating set of minimal cardinality; for infinite groups, minimal generating sets are either finite or of the same cardinality as the group [10, p. 356].

A result from universal algebra provides a surprising insight into the phenomenon of minimal generating sets having different cardinalities. Although the result is stated in a more general form in [3, p. 33], which applies to minimal generating sets for all sets with n-ary closure operators for $n \geq 2$, this has been adapted here to address the specific case of finitely generated groups.

Theorem 2.4.2 **Tarkski's Irredundant Basis Theorem**
For a finite group G, for any $n \in \mathbb{N}$ such that $d(G) \leq n \leq m(G)$, G has a minimal generating set X such that $|X| = n$.

This shows that not only do many groups have minimal generating sets of different cardinalities, but that finite groups must have at least one minimal generating set of every size between $d(G)$ and $m(G)$.

In light of the difficulty of finding all the minimal generating sets of a given group, many of the results surrounding minimal generating sets of groups instead focus on bounding the cardinalities of such sets, and in particular there are several existing results regarding $d(G)$. For example, the following result for direct products of finite groups follows directly from the definition of $d(G \times H)$.

Lemma 2.4.3
For a finite group $G \times H$, $\max\{d(G), d(H)\} \leq d(G \times H) \leq d(G) + d(H)$.

Proof. If $G \times H = \langle X \rangle$, then $G = \langle \phi(X) \rangle$ where $\phi : G \times H \to G$ is the canonical surjective homomorphism $(g, h) \mapsto g$. This implies that $|X| \geq d(G)$. By the same argument using $\phi : G \times H \to H$, $|X| \geq d(H)$ and hence $d(G \times H) \geq \max\{d(G), d(H)\}$.

If $G = \langle X_G \mid R_G \rangle$ and $H = \langle X_H \mid R_H \rangle$ for minimal generating sets X_G and X_H with $|X_G| = d(G)$ and $|X_H| = d(H)$, then $G \times H = \langle X_G \cup X_H \mid R_G \cup R_H \cup [X_G, X_H] \rangle$.[6] As $|X_G \cup X_H| \leq d(G) + d(H)$, $d(G \times H) \leq d(G) + d(H)$. □

A similar result can also be derived for quotient groups.

Lemma 2.4.4
For a finite group G with $N \trianglelefteq G$, $d(G/N) \leq d(G)$.

Proof. Let $d(G) = n$ and $X = \{x_1, \ldots, x_n\}$ be a minimal generating set of G. Since every $g \in G$ can be written as a word in X, every $gN \in G/N$ can be written as a product of the cosets $\{x_1N, \ldots, x_nN\}$. Hence, $d(G/N) \leq d(G)$. □

Many properties of minimal generating sets seem counter-intuitive; for example, the minimum cardinality of minimal generating sets does not necessarily preserve subgroup ordering. For example, by Cayley's Theorem, every finite group with $|G| = n$ is isomorphic to a subgroup of S_n, which has minimal generating set $\{(1, 2), (1, \ldots, n)\}$. However, there are finite groups with $d(G) > 2$, as will be seen in Proposition 2.4.10, so $H \leq G \not\Rightarrow d(H) \leq d(G)$.

There are certain families of finite groups for which it is much easier to determine the minimal generating sets of; one example of such a family are the finite p-groups, where $d(G) = m(G)$. This uses the following definition and result, taken from [16, pp. 122–123].[7]

[6] This presentation is stated without proof here, but it can be proved by showing that $(g, h) \mapsto gh$ is an isomorphism from $G \times H$ to the group given by the presentation.

[7] Note that Proposition 2.4.6 holds in the case that G is infinite, but involves invoking Zorn's lemma to find a maximal subgroup.

Definition 2.4.5 **Frattini Subgroup**

For a group G, the Frattini subgroup $\Phi(G)$ is the intersection of all maximal subgroups of G, where $H \leq G$ is maximal if and only if $H \leq K \leq G \implies K = H$ or $K = G$. If G has no maximal subgroups, then $\Phi(G) = G$.

Proposition 2.4.6

For a finite group G, the Frattini subgroup $\Phi(G)$ is the set of all elements $g \in G$ such that there is no minimal generating set of G containing g.

Proof. Suppose that g is not an element of any minimal generating set of G. For a maximal subgroup $H \leq G$, if $g \notin H$, then as $H \leq \langle \{g\} \cup H \rangle$, $\langle \{g\} \cup H \rangle = G$. As g cannot be an element of any minimal generating set of G, this implies that H is a generating set of G and hence $H = G$, which is a contradiction. As $g \in H$ for any maximal subgroup H, this implies that $g \in \Phi(G)$.

Suppose that $g \in \Phi(G)$. If $\{g\} \cup X$ is a minimal generating set of G for some $X \subset G$, then as $G \neq \langle X \rangle$, there must exist a maximal subgroup $H \leq G$ such that $\langle X \rangle \leq H$. As $g \in H$, this implies that $\langle \{g\} \cup X \rangle \leq H$, which is a contradiction. Hence, g is not an element of any minimal generating set of G. □

Although the proof will be omitted from this essay, this property of the Frattini subgroup can be used alongside results about nilpotent groups to prove the following theorem, which is taken from [16, p. 124]:

Theorem 2.4.7 **Burnside Basis Theorem**

If G is a finite p-group, then $G/\Phi(G)$ is a vector space over $\mathbb{Z}/p\mathbb{Z}$ and $d(G) = m(G) = \dim(G/\Phi(G))$.

The Burnside Basis Theorem can be used to classify the Cayley graphs of some types of p-group with respect to minimal generating sets up to isomorphism. I first propose and prove the following proposition:

Proposition 2.4.8

For a finite group G with $G = \langle X \mid R \rangle$ and $Y \subset G$, if there is a bijection $\phi : X \to Y$ such that $x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} \in R \iff \phi(x_1)^{\varepsilon_1} \dots \phi(x_n)^{\varepsilon_n} = 1$, then $\mathrm{Cay}(G, X)$ and $\mathrm{Cay}(G, Y)$ are isomorphic.

Proof. Consider the map $\psi : F(Y) \to G$ defined by

$$\psi\left(\prod_{i=1}^{n} y_i^{\varepsilon_i}\right) = \prod_{i=1}^{n} \phi^{-1}(y_i)^{\varepsilon_i}$$

for $y_1, \dots, y_n \in Y$ and $\varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\}$. By definition of $F(Y)$ and the fact that ϕ is a bijection, ψ is well-defined. As

$$\begin{aligned}
\psi\left(\prod_{i=1}^{n+k}\right) &= \prod_{i=1}^{n+k} \phi^{-1}(y_i)^{\varepsilon_i} \\
&= \prod_{i=1}^{n} \phi^{-1}(y_i)^{\varepsilon_i} \prod_{i=n+1}^{n+k} \phi^{-1}(y_i)^{\varepsilon_i} \\
&= \psi\left(\prod_{i=1}^{n} y_i^{\varepsilon_i}\right) \psi\left(\prod_{i=n+1}^{n+k} y_i^{\varepsilon_i}\right)
\end{aligned}$$

ψ is a homomorphism. For every $g \in G$, as

$$\begin{aligned} g &= \prod_{i=1}^{n} x_i^{\varepsilon_i} \\ \implies g &= \psi\left(\prod_{i=1}^{n} \phi(x_i)^{\varepsilon_i}\right) \end{aligned}$$

for some $x_1, \dots, x_n \in X$ and $\varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\}$, ψ is surjective. Hence, $F(Y)/\ker(\psi) \cong G$ by the first isomorphism theorem and so $G = \langle Y \mid \ker(\psi)\rangle$. By construction, $r \in \ker(\psi) \iff \psi(r) \in R$.

Let $\overline{\psi} : G \to G$ be defined as $\overline{\psi}(g) = \psi(y_1^{\varepsilon_1} \dots y_n^{\varepsilon_n})$ where $g = y_1^{\varepsilon_1} \dots y_n^{\varepsilon_n}$. As

$$\begin{aligned} \overline{\psi}(g) &= \overline{\psi}(h) \\ \iff \overline{\psi}\left(\prod_{i=1}^{n} y_i^{\varepsilon_i}\right) &= \overline{\psi}\left(\prod_{i=n+1}^{n+k} y_i^{\varepsilon_{n+k}}\right) \\ \iff \prod_{i=1}^{n} \phi^{-1}(y_i)^{\varepsilon_i} &= \prod_{i=n+1}^{n+k} \phi^{-1}(y_i)^{\varepsilon_i} \\ \iff \left(\prod_{i=n+1}^{n+k} \phi^{-1}(y_i)^{\varepsilon_i}\right)^{-1} \prod_{i=1}^{n} \phi^{-1}(y_i)^{\varepsilon_i} &= 1 \\ \iff \prod_{i=-(n+k)}^{-(n+1)} \phi^{-1}(y_i)^{\varepsilon_i} \prod_{i=1}^{n} \phi^{-1}(y_i)^{\varepsilon_i} &= 1 \\ \iff \prod_{i=-(n+k)}^{-(n+1)} y_i^{\varepsilon_i} \prod_{i=1}^{n} y_i^{\varepsilon_i} &= 1 \\ \iff \left(\prod_{i=n+1}^{n+k} y_i^{\varepsilon_i}\right)^{-1} \prod_{i=1}^{n} y_i^{\varepsilon_i} &= 1 \\ \iff h^{-1}g &= 1 \\ g &= h \end{aligned}$$

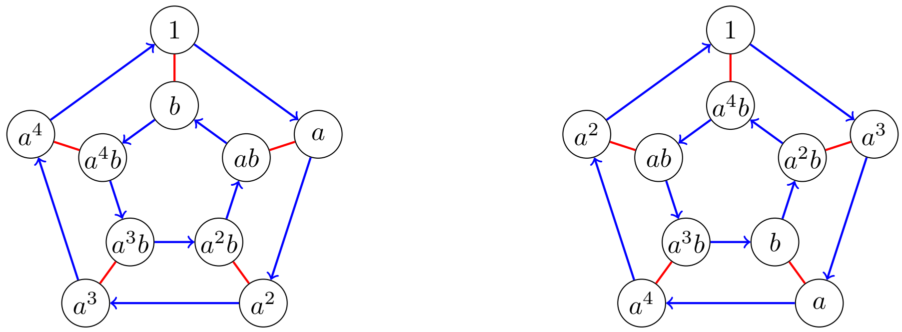
$\overline{\psi}$ is injective and hence an automorphism.

Let E_X be the edge set of $\mathrm{Cay}(G, X)$ and E_Y the edge set of $\mathrm{Cay}(G, Y)$. Then,

$$\begin{aligned} (g, h) \in E_Y &\iff h = gy \text{ for some } y \in Y \\ &\iff \overline{\psi}(h) = \overline{\psi}(gy) \\ &\qquad = \overline{\psi}(g)\overline{\psi}(y) \\ &\qquad = \overline{\psi}(g)\phi^{-1}(y) \\ &\qquad = \overline{\psi}(g)x \text{ for some } x \in X \\ &\iff \big(\overline{\psi}(g), \overline{\psi}(h)\big) \in E_X \end{aligned}$$

Hence, $\mathrm{Cay}(G, X)$ and $\mathrm{Cay}(G, Y)$ are isomorphic. □

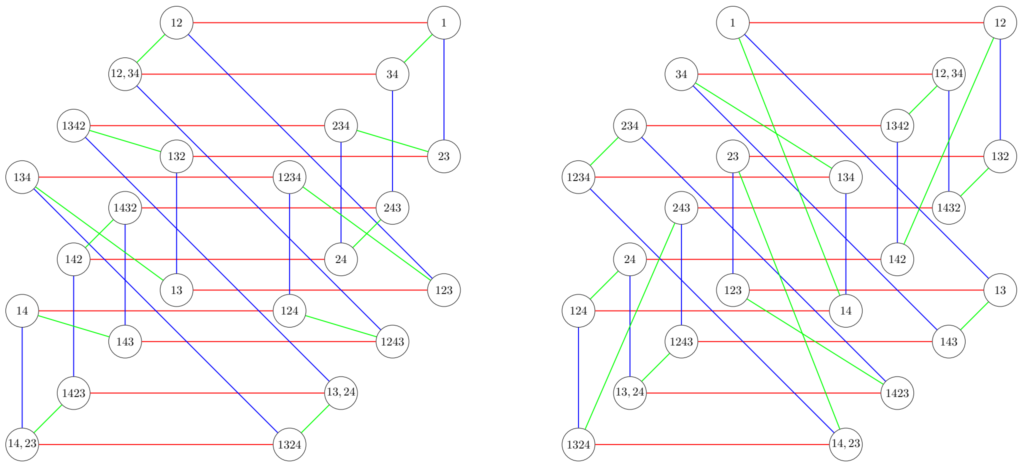
For example, if $\{a, b\} \subset D_{2n}$ is such that $|a| = n$, $|b| = 2$ and $|ba| = 2$, then $\{a, b\}$ generates D_{2n}. As seen in Figure 7, this implies that, for example, $\mathrm{Cay}(D_{10}, \{a, b\})$ and $\mathrm{Cay}\big(D_{10}, \{a^3, a^4b\}\big)$ are isomorphic.



(a) $\mathrm{Cay}(D_{10}, \{a, b\})$ (b) $\mathrm{Cay}\big(D_{10}, \{a^3, a^4b\}\big)$

Figure 7: Cayley graphs of the dihedral group D_{10} with respect to different minimal generating sets that satisfy the same relations.

Although in the example of D_{2n}, Proposition 2.4.8 implies that any minimal generating set with the same number of elements and same orders of the elements have isomorphic Cayley graphs, Figure 8 shows that this does not always hold; both have a generating set with three order two elements, but $\mathrm{Cay}(S_4, \{(1, 2), (2, 3), (3, 4)\})$ has a cycle of length 4 where $\mathrm{Cay}(S_4, \{(1, 2), (1, 3), (1, 4)\})$ does not.



(a) $\mathrm{Cay}(S_4, \{(1, 2), (2, 3), (3, 4)\})$ (b) $\mathrm{Cay}(S_4, \{(1, 2), (1, 3), (1, 4)\})$

Figure 8: Cayley graphs of the symmetric group S_4 with respect to different minimal generating sets; they are not isomorphic to each other despite both having three order two generators.

The classification of the Cayley graphs of cyclic p-groups follows directly from this result:

Proposition 2.4.9
For a group $G \cong C_{p^n}$ for some prime p and $n \in \mathbb{N}$, all Cayley graphs of G with respect to a minimal generating set of G are isomorphic.

Proof. By the Burnside Basis Theorem, as G is cyclic, the minimal generating sets of G are all of the form $\{g\}$ for some $g \in G$ where $|g| = p^n$. By Proposition 2.4.8, this implies that all Cayley graphs of G with respect to a minimal generating set of G are isomorphic. □

In particular, Proposition 2.4.9 proves that all Cayley graphs of prime order cyclic groups with respect to minimal generating sets are isomorphic. This can be generalised to all elementary abelian groups - as defined in [6, p. 136], these are the abelian groups where every non-trivial element has order p for a given prime p. It follows from Cauchy's theorem that an elementary abelian group must be a p-group, and by the fundamental theorem of finite abelian groups, there is a unique elementary abelian group of order p^n up to isomorphism, namely $\prod_{i=1}^{n} C_p$.[8]

Proposition 2.4.10
For an elementary abelian group G, all Cayley graphs of G with respect to a minimal generating set are isomorphic.

Proof. If G is elementary abelian, then $G \cong \prod_{i=1}^{n} C_p$ where $|G| = p^n$. As $G = \langle a_1 \rangle \times \cdots \times \langle a_k \rangle$, $\{(g_1, \ldots, g_k) : g_i = a_i, g_j = 1, i \neq j\}$ is a minimal generating set of G. By the Burnside Basis Theorem, the minimal generating sets of G all contain n elements. Since by definition, every non-trivial element of G has order p and $G = \langle g_1, \ldots, g_n \mid g_i^p = 1, g_i g_j = g_j g_i \rangle$, every minimal generating set of G must satisfy these relations and so, by Proposition 2.4.8, all Cayley graphs of G with respect to a minimal generating set of G are isomorphic. □

The classification of all Cayley graphs with respect to minimal generating sets for arbitrary finite abelian groups is significantly harder, due to the number of minimal generating sets. The following two results are stated as an exercise in [6, p. 166] to give $d(G)$ for any abelian group G. They follow from the fundamental theorem of finite abelian groups and the Burnside Basis Theorem.

Lemma 2.4.11
For a finite abelian group $G \cong \prod_{i=1}^{k} C_{d_i}$ where $d_i \mid d_{i+1}$ for $i \in \{1, \ldots, k-1\}$ such that $|G| = d_1 \ldots d_k$, if P_j is the Sylow p_j-subgroup in G for a prime $p_j \mid |G|$, then $k = \max_{p_j \mid |G|}\{d(P_j)\}$.

Proof. If $p \mid d_1$, then $p \mid d_i$ for all $i \in \{1, \ldots, k\}$. For each d_i, as $d_i = p^{n_i} m_i$ where $p \nmid m_i$, $P \cong \prod_{i=1}^{k} C_{p^{n_i}}$ is a Sylow p-subgroup of G. As G is abelian, every subgroup of G is normal and so P is the only Sylow p-subgroup of G. As $P = \langle g_1 \rangle \times \cdots \times \langle g_k \rangle$, $\{(p_1, \ldots, p_k) : p_i = g_i, p_j = 1, i \neq j\}$ is a minimal generating set of P. By the Burnside Basis Theorem, as P is a p-group, this implies that $d(P) = k$. This holds for any prime $p \mid d_1$. If $p \mid |G|$ but $p \nmid d_1$, then $d(P) < k$, so the result holds. □

Proposition 2.4.12
For a finite abelian group $G \cong \prod_{i=1}^{k} C_{d_i}$ where $d_i \mid d_{i+1}$ for $i \in \{1, \ldots, k-1\}$ such that $|G| = d_1 \ldots d_k$, $d(G) = k$.

Proof. By Lemma 2.4.3, $d(G) \leq k$. Using Lemma 2.4.11, let P be a Sylow p-subgroup of G with $d(P) = k$ and let $P_1, \ldots, P_r$ be the other Sylow p_i-subgroups of G corresponding each prime $p_i \mid G$ where $p_i \neq p$.

Since G is a finite abelian group, every Sylow p-subgroup of G is normal in G and so $G \cong P \times P_1 \times \cdots \times P_r \cong P \times \prod_{i=1}^{r} P_i$. By definition of the direct product, $N = \prod_{i=1}^{r} P_i \trianglelefteq G$ and $G/N \cong P$. By Lemma 2.4.4, $d(P) = d(G/N) \leq d(G)$ and so $d(G) \geq k$. Hence, $d(G) = k$. □

[8] Often additive notation is used for abelian groups, such as writing $\bigoplus_{i=1}^{n} C_p$. I have however generally expressed the cyclic group C_p multiplicatively and I will only use additive notation for abelian groups where the group operation is a form of addition, such as when considering $\mathbb{Z}/n\mathbb{Z}$.

3 Cycles in Cayley Graphs

3.1 Eulerian Cycles

One of the most famous types of cycle in graph theory are Eulerian cycles, with the definition revised from the combinatorics course [18].

Definition 3.1.1 **Eulerian Cycle**
An Eulerian cycle in a finite graph is a cycle that uses every edge exactly once.

Eulerian cycles in directed graphs are defined in the same way, with the key difference being the stronger condition that the cycle must be directed; hence, not every directed graph with an Eulerian cycle in its underlying graph will have an Eulerian cycle.

For both undirected and directed graphs, there is a simple characterisation of precisely which graphs contain Eulerian cycles. This first uses the following lemma, which was stated in [4, p. 44] without proof.

Lemma 3.1.2
If (V, E) is a finite weakly connected directed graph such that $\deg^-(v) = \deg^+(v)$ for all $v \in V$, then (V, E) is strongly connected.

Proof. Let $|V| = 1$. Then, vacuously, (V, E) is weakly connected with $\deg^-(v) = \deg^+(v)$ for all $v \in V$, and also strongly connected.

Suppose that $\forall |V'| < n$ where (V', E') is weakly connected with $\deg^-(v) = \deg^+(v)$ for all $v \in V'$, (V', E') is strongly connected. If $|V| = n$, where the directed graph (V, E) is weakly connected with $\deg^-(v) = \deg^+(v)$ for all $v \in V$, then consider a proper subgraph (V', E') where $|V'| = n - 1$. As $|V'| < n$, the inductive hypothesis holds and so (V', E') is strongly connected. By definition, this means that for any $u, v \in V'$, there is a path from u to v and a path from v to u.

Consider $v \in V - V'$. As (V, E) is weakly connected and $\deg^-(v) = \deg^+(v)$, there are edges $(u, v), (v, w) \in E$ such that $u, w \in V'$. For any $x \in V'$, there is a path from x to u and a path from w to x. Hence, there is a path from x to v and a path from v to x, by appending the given edges to these paths. Since $V' \cup \{v\} = V$, this implies that (V, E) is strongly connected by induction. □

The proof of the characterisation is then adapted from [2, p. 21]:

Theorem 3.1.3 **Euler's Theorem**
A finite directed graph (V, E) has an Eulerian cycle if and only if all vertices $v \in V$ with non-zero degree belong to a single weakly connected component and $\deg^-(v) = \deg^+(v)$.

Proof. Suppose that (V, E) has an Eulerian cycle. Then, every vertex with non-zero degree must belong to a single weakly connected component, as if $u, v \in V$ have non-zero degree, then there must be a path from u to v in the Eulerian cycle. Furthermore, for each $v \in V$, $\deg^-(v) = \deg^+(v)$ as the number of edges starting at v must equal the number of edges leaving v for the Eulerian cycle to use every edge.

Suppose that all vertices $v \in V$ with non-zero degree belong to a single weakly connected component and that $\deg^-(v) = \deg^+(v)$. By Lemma 3.1.2, this implies that all vertices with non-zero degree belong to a single strongly connected component.

To construct an Eulerian cycle C in (V, E), take $u \in V$ where u has non-zero degree. There must therefore be some $v \in V$ such that $(u, v) \in E$, so append (u, v) to C. Since $\deg^-(v) = \deg^+(v)$, there must be some $w \in V$ such that $(v, w) \in E$, so append (v, w)

to C. Continuing in this manner, for each edge e appended to C, the condition that $\deg^-(x) = \deg^+(x)$ implies that there is some edge $e' \in E$ where the tail of e is the head of e' that can be appended to C. This process must terminate, as E is finite, but it only terminates when the last edge appended to C is an edge with tail u and there are no remaining edges in $E - C$ with head u. Hence, when the process terminates, C is a cycle.

If C contains all edges in E, then C is an Eulerian cycle. Suppose that there is some $e \in E - C$. Since all vertices with non-zero degree belong to a single strongly connected component, this implies that there must be some $v \in V$ such that v is the head of e and v is the tail of some $e' \in C$. Shift the cycle C such that e' is the last edge in C, and hence v is the starting and endpoint of the cycle. Append e to C and repeat the process above, which will then terminate when the last edge appended to C is an edge with tail v and there are no remaining edges in $E - C$ with head v. This means that all edges incident on v are in C. As V is finite, this implies that this process can be repeated to ensure that all edges of E are in C, and hence C will be an Eulerian cycle. □

The corresponding result for the undirected case can be derived immediately from this:

Corollary 3.1.4
A finite graph (V, E) has an Eulerian cycle if and only if all vertices $v \in V$ with non-zero degree belong to a single connected component and every vertex has even degree.

Proof. Suppose that (V, E) has an Eulerian cycle. Then, every vertex with non-zero degree must belong to a single strongly connected component, as if $u, v \in V$ have non-zero degree, then there must be a path between u and v in the Eulerian cycle. Furthermore, for each $v \in V$, $\deg v \equiv 0 \pmod 2$ as the number of edges starting at v must equal the number of edges leaving v for the Eulerian cycle to use every edge.

Suppose that all vertices $v \in V$ with non-zero degree belong to a single connected component and every vertex has even degree. For every pair of edges $\{u, v\}, \{w, v\} \in E$ incident on a vertex v, replace them with the directed edges (u, v) and (v, w). Since every vertex has even degree, this gives a directed graph with $\deg^-(v) = \deg^+(v)$. Lemma 3.1.2 implies that the connected component in the underlying graph corresponds to a strongly connected component in the directed graph. By Euler's Theorem, this directed graph therefore has an Eulerian cycle, and hence the underlying graph has an Eulerian cycle. □

3.2 Eulerian Cycles in Cayley Graphs

Euler's Theorem can be used to characterise exactly which Cayley graphs of finite groups admit Eulerian cycles.

Firstly, the following lemma is taken from [21, p. 133]. Here the assumption is made that for vertices incident upon an undirected edge, the contribution to both the in-degree and out-degree of that edge is one.

Lemma 3.2.1
For a group G and $X \subset G$ where X is finite, for all vertices $v \in G$ of $\mathrm{Cay}(G, X)$, $\deg^-(v) = \deg^+(v) = |X|$.

Proof. Since for $x, y \in X$, $vx = vy \iff x = y$ by the cancellation law, by definition of the out-degree and in-degree, $\deg^+(v) = |\{vx : x \in X\}| = |X|$ and $\deg^-(v) = \left|\{vx^{-1} : x \in X\}\right| = |X|$. □

I now propose and prove the following characterisation of the Cayley graphs of finite groups with Eulerian cycles:

Theorem 3.2.2
For a finite group G and $X \subset G$, $\mathrm{Cay}(G, X)$ has an Eulerian cycle if and only if $G = \langle X \rangle$ and X contains an even number of elements of order two.

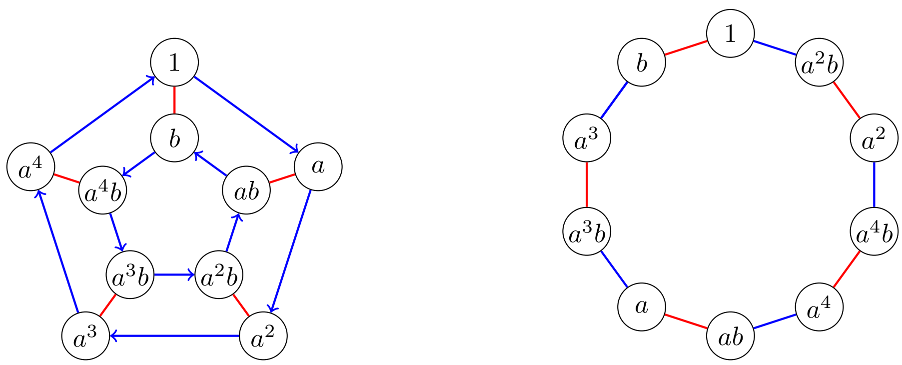
Proof. By Euler's Theorem, a directed graph has an Eulerian cycle if and only if the in-degree and out-degree of every vertex is equal and all vertices with non-zero degree belong to a single weakly connected component.

Since all vertices in a Cayley graph must be incident upon at least one edge by definition, the graph must be weakly connected. By Proposition 2.3.4, $\mathrm{Cay}(G, X)$ is weakly connected if and only if $G = \langle X \rangle$.

By Lemma 3.2.1, the in-degree and out-degree of every vertex in a Cayley graph is equal, where any undirected edges are considered to each be contributing one to both the in-degree and out-degree of vertices incident upon it. However, by definition of an Eulerian cycle, each edge is used exactly once so an undirected edge cannot be used to both enter and exit a vertex. In the context of Eulerian cycles, an undirected edge must be considered as contributing one to exactly one of the in-degree and the out-degree of vertices incident upon it. Hence, there must be an even number of undirected edges. An edge generated by $x \in X$ is undirected if and only if $|x| = 2$.

Hence, $\mathrm{Cay}(G, X)$ has an Eulerian cycle if and only if $G = \langle X \rangle$ and X contains an even number of elements of order two. $\square$

Note that this shows that the existence of Eulerian cycles in Cayley graphs is only dependent on the generating set and hence a group can have both Cayley graphs that have Eulerian cycles and Cayley graphs that do not, as shown in Figure 9.



(a) $\mathrm{Cay}(D_{10}, \{a, b\})$

(b) $\mathrm{Cay}\big(D_{10}, \{a^2b, b\}\big)$

Figure 9: Cayley graphs of $D_{10} = \langle a, b : a^5 = 1, b^2 = 1, ba = a^{-1}b \rangle$ with respect to different generating sets; $\mathrm{Cay}\big(D_{10}, \{a^2b\}\big)$ clearly has an Eulerian cycle, but $\mathrm{Cay}(D_{10}, \{a, b\})$ does not.

3.3 Hamiltonian Cycles

After considering the question of the cycles in a graph that use every edge exactly once, it is natural to consider the cycles in a graph that use every vertex exactly once. This is the definition of a Hamiltonian cycle, as given in the combinatorics course [18].

Definition 3.3.1 **Hamiltonian Cycle**

A Hamiltonian cycle in a finite graph is a cycle that uses every vertex exactly once.

Again, Hamiltonian cycles in directed graphs are defined in the same way, using the stronger condition of the cycle being directed. A generalisation of this definition is that of a Hamiltonian path; a path that uses every vertex exactly once.

Although the characterisation of which graphs contain Eulerian cycles was relatively straightforward, there is no such result for Hamiltonian cycles. For both directed and undirected graphs, the issue of finding a Hamiltonian cycle is NP-complete [7, p. 199]. However, there are many results guaranteeing the existence of Hamiltonian cycles in undirected graphs satisfying certain conditions, usually relating to the degrees or degree sums of vertices. Furthermore, graphs with Hamiltonian cycles can be built from other graphs with Hamiltonian cycles using the Cartesian product, as stated in [5, pp. 51–52].

Theorem 3.3.2

If $\Gamma = (V, E)$ and $\Gamma' = (V', E')$ are graphs with Hamiltonian cycles, then $\Gamma \times \Gamma'$ has a Hamiltonian cycle.

Proof. Suppose that $|V| = m$ and $|V'| = n$. As Γ has a Hamiltonian cycle, it has the cycle graph C_m on m vertices as a subgraph; similarly, Γ' has the cycle graph on n vertices C_n as a subgraph. This implies that $C_m \times C_n$ is a spanning subgraph of $\Gamma \times \Gamma'$ by definition of the Cartesian product.

Let C_m have vertex set $\{u_1, \ldots, u_m\}$ and edges $\{u_i, u_{i+1}\}$ for $i \in \{1, \ldots, m-1\}$ and $\{u_m, u_1\}$; similarly, let C_n have vertex set $\{v_1, \ldots, v_n\}$ and edges $\{v_i, v_{i+1}\}$ for $i \in \{1, \ldots, n-1\}$ and $\{v_n, v_1\}$. If m and n are both odd, then the cycle defined by the sequence of vertices

$$\begin{gathered}(u_1, v_1), (u_2, v_1), \ldots, (u_m, v_1), (u_m, v_2), \ldots, (u_2, v_2), (u_2, v_3), \ldots, \\ (u_2, v_{n-1}), (u_2, v_n), (u_m, v_n), (u_1, v_n), (u_1, v_{n-1}), \ldots, (u_1, v_1)\end{gathered}$$

(as shown in Figure 10a) is a Hamiltonian cycle in $C_m \times C_n$. If at least one of m and n is even - suppose without loss of generality that n is even - then the cycle defined by the sequence of vertices

$$\begin{gathered}(u_1, v_1), (u_2, v_1), \ldots, (u_m, v_1), (u_m, v_2), \ldots, (u_1, v_2), (u_2, v_3), \ldots, \\ (u_1, v_{n-1}), (u_1, v_n), (u_m, v_n), \ldots, (u_1, v_n), (u_1, v_1)\end{gathered}$$

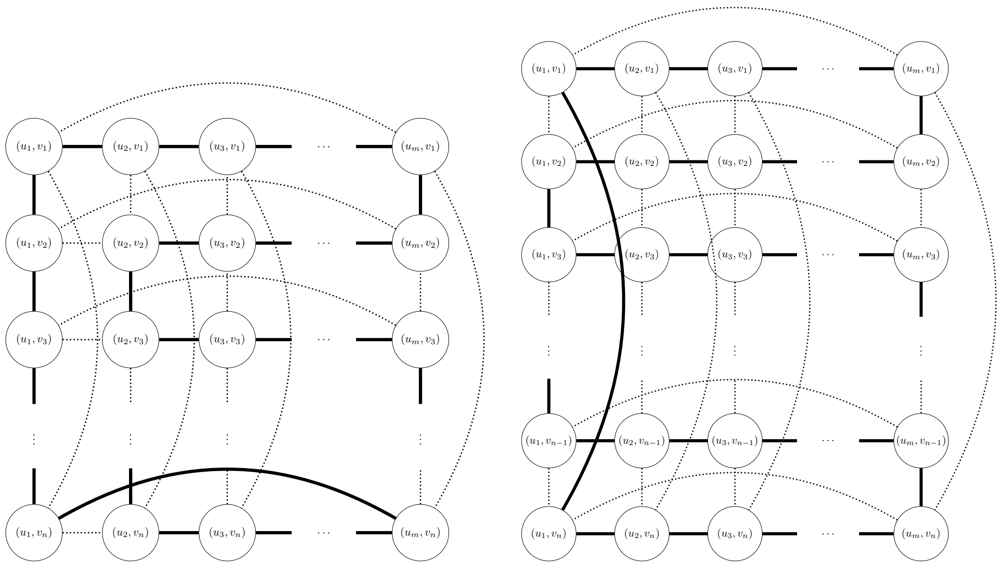
(as shown in Figure 10b) is a Hamiltonian cycle in $C_m \times C_n$.

Hence, $C_m \times C_n$ has a Hamiltonian cycle, which is a Hamiltonian cycle in $\Gamma \times \Gamma'$. $\square$

However, this result does not hold for directed graphs. It is clear from Figure 10 that the argument in the proof of Theorem 3.3.2 would not work in the directed case, as adding the directions to C_m and C_n would cause the given edges to no longer form a cycle. The following result from [12, pp. 138–140] characterises when the Cartesian product of directed cycle graphs has a Hamiltonian cycle, using an intuitive application of the additive group $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, which is isomorphic to the direct product of cyclic groups $C_m \times C_n$.

Lemma 3.3.3

For directed cycle graphs C_m and C_n on m and n vertices respectively, if $\mathrm{hcf}(m, n) \geq 2$ and there exists integers $d_m, d_n > 0$ such that $d_m + d_n = \mathrm{hcf}(m, n)$ and $\mathrm{hcf}(m, d_m) = \mathrm{hcf}(n, d_n) = 1$, then $C_m \times C_n$ has a Hamiltonian cycle.



(a) A Hamiltonian cycle in $C_m \times C_n$ when m and n are odd.

(b) A Hamiltonian cycle in $C_m \times C_n$ when n is even.

Figure 10: Demonstration of the construction of Hamiltonian cycles in Theorem 3.3.2.

Proof. Let $V = \{0, \ldots, m-1\} \times \{0, \ldots, n-1\}$ be the vertex set of $C_m \times C_n$ and E be the edge set. This provides a natural way viewing $C_m \times C_n$ as the additive group $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$; there is an edge $(u, v) \in E$ if and only if either $v = u + (1, 0)$ or $v = u + (0, 1)$.

Using the conditions given, a cycle $(v_1, v_2), \ldots, (v_{mn-1}, v_{mn})$ can be defined in the following way:

$$\begin{aligned}
v_1 &= (0, 0) \\
v_2 &= (1, 0) \\
&\vdots \\
v_{d_m+1} &= (d_m, 0) \\
v_{d_m+2} &= (d_m, 1) \\
v_{d_m+3} &= (d_m, 2) \\
&\vdots \\
v_{d_m+d_n-1} &= (d_m, d_n - 2) \\
v_{\mathrm{hcf}(m,n)} &= (d_m, d_n - 1) \\
v_{\mathrm{hcf}(m,n)+1} &= (d_m, d_n) \\
v_{\mathrm{hcf}(m,n)+2} &= (d_m + 1, d_n) \\
&\vdots \\
v_{\mathrm{hcf}(m,n)+i} &= v_i + (d_m, d_n) \\
&\vdots \\
v_{mn} &= (\mathrm{lcm}(m, n) d_m, \mathrm{lcm}(m, n) d_n - 1)
\end{aligned}$$

$$= (0, n-1)$$

It follows from this that $\big(v_i, v_{i+1 \pmod{mn}}\big) \in E$ and that $v_i \neq v_j$ for every $i, j \in \{1, \ldots, mn\}$ where $i \neq j$. Since $C_m \times C_n$ has mn vertices by definition, this cycle is a Hamiltonian cycle. $\square$

Theorem 3.3.4
If C_m and C_n are directed cycle graphs on m and n vertices respectively, then $C_m \times C_n$ has a Hamiltonian cycle if and only if $\operatorname{hcf}(m,n) \geq 2$ and there exists integers $d_m, d_n > 0$ such that $d_m + d_n = \operatorname{hcf}(m,n)$ and $\operatorname{hcf}(m, d_m) = \operatorname{hcf}(n, d_n) = 1$.

Proof. By Lemma 3.3.3, the given conditions imply that $C_m \times C_n$ has a Hamiltonian cycle and so it suffices to prove the opposite implication.

Again let $V = \{0, \ldots, m-1\} \times \{0, \ldots, n-1\}$ be the vertex set of $C_m \times C_n$ and E be the edge set.

Suppose that there is a Hamiltonian cycle $(v_1, v_2), \ldots, (v_{mn-1}, v_{mn})$ in $C_m \times C_n$, so the v_i are unique for $i \in \{1, \ldots, mn\}$. Without loss of generality, let $v_1 = (0,0)$. Let

$$\begin{aligned} V_1 &= \{v_i \in V : v_{i+1} = v_i + (1,0) \pmod{m}\} \\ V_2 &= \{v_i \in V : v_{i+1} = v_i + (0,1) \pmod{n}\} \end{aligned}$$

so that $V_1, V_2 \neq \emptyset$ and $V_1 \cup V_2 = V$.

For $v_i \in V_1$, if $v_i + (1, n-1) \in V_2$ with $v_j = v_i + (1, n-1)$, then $i \neq j$ but $v_{i+1} = v_i + (1,0) = v_i + (1,n) = v_{j+1}$. This contradicts the assumption that the v_i are unique and so $v_i + (1, n-1) \in V_1$. Conversely, suppose that $v_i + (1, n-1) \in V_1$ and $v_i \in V_2$, with $v_j = v_i + (1,0)$. If $v_{j-1} \in V_2$, then $v_j = v_{j-1} + (0,1)$ and so $v_i + (1, n-1) = v_{j-1}$, contradicting $v_i + (1, n-1) \in V_1$, and if $v_{j-1} \in V_1$, then $v_{j-1} = v_i$, contradicting $v_i \in V_2$. Hence, $v_i \in V_1$ if and only if $v_i + (1, n-1) \in V_1$.

If $H = \langle (1, n-1) \rangle \leq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, then $|H| = \operatorname{lcm}(m,n) = \frac{mn}{\operatorname{hcf}(m,n)}$. Since $v_i \in V_1$ if and only if $v_i + (1, n-1) \in V_1$, it follows that V_1 and V_2 are each the union of distinct cosets of H in $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Since cosets are disjoint, $V_1 \cap V_2 = \emptyset$ and so $\operatorname{hcf}(m,n) \geq 2$.

For each $v_i \in V$, there is some $a \in \{0, \ldots, m-1\}$ and $b \in \{0, \ldots, n-1\}$ such that $a + b = \operatorname{hcf}(m,n)$ and $v_{i+\operatorname{hcf}(m,n)} = v_i + (a,b)$. Let $K = \{(a,b) : a + b = \operatorname{hcf}(m,n)\}$. For any $(a,b) \in K$, $(a,b) = (\operatorname{hcf}(m,n), 0) - b(1, n-1)$ and so to show that $K \subset H$, it suffices to show that $(\operatorname{hcf}(m,n), 0) \in K$. By Bézout's lemma, there exists some $p, q \in \mathbb{Z}$ such that $pm + qn = \operatorname{hcf}(m,n)$. Then,

$$\begin{aligned} (\operatorname{hcf}(m,n), 0) &= (\operatorname{hcf}(m,n) - pm, qn(n-1)) \\ &= (qn, qn(n-1)) \\ &= qn(1, n-1) \end{aligned}$$

so $(\operatorname{hcf}(m,n), 0) \in H$. This implies that $v_i \in V_1$ if and only if $v_{i+\operatorname{hcf}(m,n)} \in V_1$. If $v_{1+\operatorname{hcf}(m,n)} = (d_m, d_n) = v_1 + (d_m, d_n)$, then $d_m + d_n = \operatorname{hcf}(m,n)$ with $d_m, d_n > 0$.

Furthermore, by applying this repeatedly, for $k \in \mathbb{Z}$, $v_{1+k\operatorname{hcf}(m,n)} = v_1 + (kd_m, kd_n)$. Let $k = |\langle (d_m, d_n) \rangle|$. This implies that $v_1 + (kd_m, kd_n) = v_1$ by definition of the order. Since there are $\operatorname{hcf}(m,n)$ vertices between v_i and $v_{i+\operatorname{hcf}(m,n)}$ in the Hamiltonian cycle, $k\operatorname{hcf}(m,n) = mn$ and so $k = \frac{mn}{\operatorname{hcf}(m,n)} = \operatorname{lcm}(m,n)$. If d_m has order k_m in $\mathbb{Z}/m\mathbb{Z}$ and d_n has order k_n in $\mathbb{Z}/n\mathbb{Z}$, then $k = \operatorname{lcm}(k_m, k_n)$, so $\operatorname{lcm}(m,n) = \operatorname{lcm}(k_m, k_n)$.

Suppose there is some prime p such that $p \mid d_m$ and $p \mid m$. If $p \mid d_n$, then $p \mid \operatorname{hcf}(m,n)$ since $d_m + d_n = \operatorname{hcf}(m,n)$, and so $p \mid n$. By definition of the order, k_m is the smallest integer such that $m \mid k_m d_m$ and similarly k_n is the smallest integer such that $n \mid k_n d_n$.

This implies that $k_m \mid \frac{m}{p}$ and $k_n \mid \frac{n}{p}$ as $d_m\left(\frac{m}{p}\right) = \left(\frac{d_m}{p}\right)m$ and $d_n\left(\frac{n}{p}\right) = \left(\frac{d_n}{p}\right)n$. This implies that

$$\begin{aligned} \operatorname{lcm}(k_m, k_n) &\leq \operatorname{lcm}\left(\frac{m}{p}, \frac{n}{p}\right) \\ &= \frac{mn}{p \operatorname{hcf}(m,n)} \\ &< \frac{mn}{\operatorname{hcf}(m,n)} \\ &= \operatorname{lcm}(m,n) \end{aligned}$$

which is a contradiction. Hence, $p \nmid d_n$. This implies that $p \nmid \operatorname{hcf}(m,n)$ since $d_m + d_n = \operatorname{hcf}(m,n)$, and so $p \nmid n$. By a similar argument as above, this implies that $k_m \mid \frac{m}{p}$ and $k_n \mid n$ and so

$$\begin{aligned} \operatorname{lcm}(k_m, k_n) &\leq \operatorname{lcm}\left(\frac{m}{p}, n\right) \\ &= \frac{mn}{p \operatorname{hcf}(m,n)} \\ &< \frac{mn}{\operatorname{hcf}(m,n)} \\ &= \operatorname{lcm}(m,n) \end{aligned}$$

which is again a contradiction. This implies that $\operatorname{hcf}(m, d_m) = 1$, and $\operatorname{hcf}(n, d_n) = 1$ by the same argument.

Hence, if $C_m \times C_n$ has a Hamiltonian cycle, then $\operatorname{hcf}(m,n) \geq 2$ and there exists integers $d_m, d_n > 0$ such that $d_m + d_n = \operatorname{hcf}(m,n)$ and $\operatorname{hcf}(m, d_m) = \operatorname{hcf}(n, d_n) = 1$. □

Corollary 3.3.5
For directed graphs $\Gamma = (V, E)$ and $\Gamma = (V', E')$ with Hamiltonian cycles where $|V| = m$ and $|V'| = n$, if $\operatorname{hcf}(m,n) \geq 2$ and there exists integers $d_m, d_n > 0$ such that $d_m + d_n = \operatorname{hcf}(m,n)$ and $\operatorname{hcf}(m, d_m) = \operatorname{hcf}(n, d_n) = 1$, then $\Gamma \times \Gamma'$ has a Hamiltonian cycle.

Proof. As Γ has a Hamiltonian cycle, it has the directed cycle graph C_m on m vertices as a spanning subgraph; similarly, Γ' has the directed cycle graph on n vertices C_n as a spanning subgraph. This implies that $C_m \times C_n$ is a spanning subgraph of $\Gamma \times \Gamma'$ by definition of the Cartesian product. By Theorem 3.3.4, this spanning subgraph is a Hamiltonian cycle. □

3.4 Hamiltonian Paths and Cycles in Cayley Graphs

Although Hamiltonian cycles in Cayley graphs have not been studied in as great detail as their underlying counterparts, progress has been made on determining which Cayley graphs of certain families of finite groups have Hamiltonian cycles. In particular, research has focused on which groups have a minimal generating set with respect to which its Cayley graph has a Hamiltonian cycle. Note that if a Cayley graph with respect to a minimal generating set X has a Hamiltonian cycle, then the Cayley graph with respect to any generating set $Y \supset X$ has a Hamiltonian cycle, so research has focused on Cayley graphs with respect to minimal generating sets.

For example, in the following result adapted from [13, p. 67], this is shown for abelian groups. This uses a special case of Theorem 3.3.4, stated as a lemma below.

Lemma 3.4.1
For integers $m, n \geq 3$ such that $n \mid m$, if C_m and C_n are directed cycle graphs on m and n vertices respectively, then $C_m \times C_n$ has a Hamiltonian cycle.

Proof. By Theorem 3.3.4, $C_m \times C_n$ has a Hamiltonian cycle if and only if $\text{hcf}(m,n) \geq 2$ and there exists integers $d_m, d_n > 0$ such that $d_m + d_n = \text{hcf}(m,n)$ and $\text{hcf}(m, d_m) = \text{hcf}(n, d_n) = 1$.

When $n \mid m$, $\text{hcf}(m,n) = n \geq 3$. If $d_m = 1$ and $d_n = n-1$, then $d_m + d_n = 1$ and $\text{hcf}(m, d_m) = \text{hcf}(n, d_n) = 1$. Hence, $C_m \times C_n$ has a Hamiltonian cycle. $\square$

Theorem 3.4.2
If G is a finite abelian group, then there is a minimal generating set $X \subset G$ such that $\text{Cay}(G, X)$ has a Hamiltonian cycle.

Proof. By the fundamental theorem of finite abelian groups, $G \cong \bigoplus_{i=1}^{k} \mathbb{Z}/d_i\mathbb{Z}$ where $d_{i+1} \mid d_i$ for $i \in \{1, \dots, k-1\}$ such that $|G| = d_1 \dots d_k$. If $k = 1$, then G is cyclic and so $\text{Cay}(G, \{1\})$, is a cycle graph and so has a Hamiltonian cycle. Suppose the result holds for all $k < n$.

When $k = n$, let $G' \cong \bigoplus_{i=1}^{n-1} \mathbb{Z}/d_i\mathbb{Z}$. As $G' \oplus \{0\} \leq G$, by the inductive hypothesis, there is a minimal generating set $X' \subset G'$ such that $\text{Cay}(G', X')$ has a Hamiltonian cycle. It follows from the minimality of X' that $X = (X' \times \{0\}) \cup \{(0, \dots, 0, 1)\}$ is a minimal generating set of G.

As $\text{Cay}(G', X')$ has a Hamiltonian cycle, it has the directed cycle graph $C_{d_1 \dots d_{n-1}}$ as a spanning subgraph. The Cayley graph $\text{Cay}(\mathbb{Z}/d_n\mathbb{Z}, \{\{1\}\})$ is the directed cycle graph C_{d_n}. By Proposition 2.3.10, $\text{Cay}(G, X) \cong \text{Cay}(G', X') \times \text{Cay}(\mathbb{Z}/d_n\mathbb{Z}, \{\{1\}\})$ and so $C_{d_1 \dots d_{n-1}} \times C_{d_n}$ is a spanning subgraph of $\text{Cay}(G, X)$. By Lemma 3.4.1, as $d_n \mid d_{n-1}$, $d_n \mid d_1 \dots d_{n-1}$, $C_{d_1 \dots d_{n-1}} \times C_{d_n}$ has a Hamiltonian cycle and so $\text{Cay}(G, X)$ has a Hamiltonian cycle.

Hence, by induction, every finite abelian group has a minimal generating set with respect to which its Cayley graph has a Hamiltonian cycle. $\square$

A similar result for the dihedral groups can be proven directly from their standard presentations.

Proposition 3.4.3
For all $n \geq 3$, the dihedral group D_{2n} has a minimal generating set $X \subset D_{2n}$ such that $\text{Cay}(D_{2n}, X)$ has a Hamiltonian cycle.

Proof. A standard presentation of D_{2n} is $\langle a, b \mid a^n = 1, b^2 = 1, ba = a^{-1}b \rangle$. Clearly $X = \{a, b\}$ is a minimal generating set, as D_{2n} is not abelian and hence not cyclic. A cycle $(v_1, v_2), \dots, (v_{2n-1}, v_{2n})$ can be defined as follows:

$$\begin{aligned} v_1 &= 1 \\ v_2 &= a \\ v_3 &= a^2 \\ &\vdots \\ v_n &= a^{n-1} \\ v_{n+1} &= a^{n-1}b \\ v_{n+2} &= a^{n-1}ba \\ &= a^{n-2}b \end{aligned}$$

$$\vdots$$
$$v_{2n-1} = ab$$
$$v_{2n} = b$$

It follows from the presentation that $\big(v_i, v_{i+1 \pmod{2n}}\big)$ is an edge in $\mathrm{Cay}(D_{2n}, X)$, as $(v_1, v_2), \ldots, (v_{n-1}, v_n)$ and $(v_{n+1}, v_{n+2}), \ldots, (v_{2n-1}, v_{2n})$ are each generated by a and $\{v_n, v_{n+1}\}$ and $\{v_1, v_{2n}\}$ are generated by b and so are undirected. Furthermore, $v_i \neq v_j$ for every $i, j \in \{1, \ldots, mn\}$ where $i \neq j$. Hence, $(v_1, v_2), \ldots, (v_{2n-1}, v_{2n})$ is a Hamiltonian cycle in $\mathrm{Cay}(D_{2n}, X)$. $\square$

The weaker condition of which Cayley graphs contain a Hamiltonian path has also been considered. For example, the following theorem, taken from [19, pp. 7–8], shows that every Cayley graph of every finite Dedekind group has a Hamiltonian path.[9]

Definition 3.4.4 **Dedekind Group**
A Dedekind group is a group where every subgroup is normal.

Lemma 3.4.5
If G is a group with $N \trianglelefteq G$ and there is a surjective homomorphism $\phi : G \to H$, then $\phi(N) \trianglelefteq H$.

Proof. Since ϕ is a surjective homomorphism, for every $h \in H$, there exists $g \in G$ such that $f(g) = h$. This implies that for every $h \in H$ and $n \in N$,

$$\begin{aligned} h\phi(n)h^{-1} &= \phi(g)\phi(n)\phi(g)^{-1} \\ &= \phi(g)\phi(n)\phi\big(g^{-1}\big) \\ &= \phi\big(gng^{-1}\big) \end{aligned}$$

Since N is normal, $gng^{-1} \in N$ and so $\phi\big(gng^{-1}\big) \in \phi(N)$. This implies that $\phi(N)$ is normal. $\square$

Theorem 3.4.6
If G is a Dedekind group and $X \subset G$ is a minimal generating set of G, then $\mathrm{Cay}(G, X)$ has a Hamiltonian path.

Proof. If $|X| = 1$, then G is a cyclic group and so $\mathrm{Cay}(G, X)$ is a directed cycle graph; in particular, it has a Hamiltonian cycle.

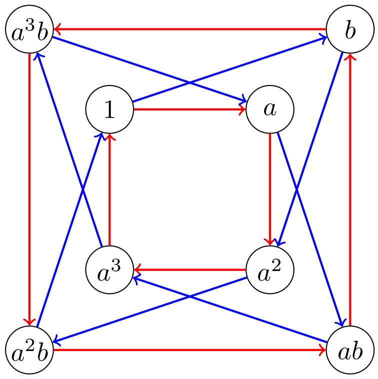
Suppose that the result holds for all minimal generating sets X' with $|X'| < |X|$. Let $Y = X - \{x\}$ for some $x \in X$. By Lemma 3.4.5, any quotient group of a Dedekind group is Dedekind, using the canonical surjection between a group and its quotient group, so $H = G/\langle x \rangle$ is Dedekind. Let $\phi : Y \to H$ be the coset map $\phi(y) = y\langle x \rangle$. Since $Y \cup \{x\}$ generates G, $\phi(Y)$ generates H. As $|Y| < |X|$, this implies that $\mathrm{Cay}(H, \phi(Y))$ has a Hamiltonian path by the inductive hypothesis. If $(y_1\langle x \rangle, y_2\langle x \rangle), \ldots, (y_{n-1}\langle x \rangle, y_n\langle x \rangle)$ is a Hamiltonian path in H and x has order k, then a Hamiltonian path can be defined in G starting at 1 by a sequence of edges

$$\underbrace{x, \ldots, x}_{k-1 \text{ times}}, y_1, \underbrace{x, \ldots, x}_{k-1 \text{ times}}, y_2, \ldots, \underbrace{x, \ldots, x}_{k-1 \text{ times}}, y_n, \underbrace{x, \ldots, x}_{k-1 \text{ times}}$$

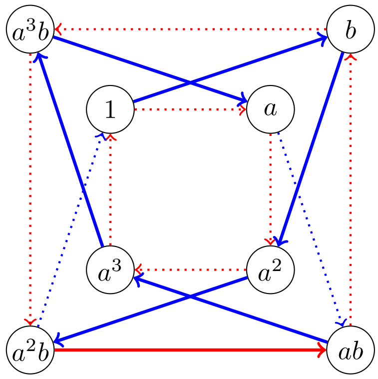
[9]Note that every abelian group is Dedekind, but the converse does not hold. Non-abelian Dedekind groups are often called Hamiltonian, but this terminology will be avoided in this essay to avoid confusion with Hamiltonian paths and cycles.

This is indeed a Hamiltonian path, as each subsequence of repetitions of x generates a different coset of $\langle x \rangle$ and cosets are disjoint and partition the group. Hence, by induction, every Dedekind group has a Hamiltonian path in any Cayley graph with respect to a minimal generating set. $\square$

For example, Figure 11 gives an example of this construction in the smallest non-abelian Dedekind group, the quaternion group Q_8, which is the more common name for the dicyclic group of order 8.



(a) $\mathrm{Cay}(Q_8, \{a, b\})$



(b) A Hamiltonian path in $\mathrm{Cay}(Q_8, \{a, b\})$.

Figure 11: A demonstration using $\mathrm{Cay}(Q_8, \{a, b\})$ of the method of constructing a Hamiltonian path in a Cayley graph of a Dedekind group given in the proof of Theorem 3.4.6.

A similar result can be proven for certain groups with index 2 subgroups, as given in [23, pp. 102–103], which in particular shows that every Cayley graph of a dihedral group has a Hamiltonian path.

Proposition 3.4.7

For a group G with a minimal generating set $X \subset G$, if there is some $N \leq G$ such that $[G : N] = 2$ and every subgroup of N is normal in G, then $\mathrm{Cay}(G, X)$ *has a Hamiltonian path.*

Proof. The proof will proceed by induction on $n = |G|$, showing that there is a Hamiltonian path $(v_1, v_2), \ldots, (v_{n-1}, v_n)$ such that $v_1 = 1$ and $v_n \notin N$. If $|G| = 2$, then $\{1\} \trianglelefteq G$ with $[G : \{1\}] = 2$, and clearly the result holds.

Suppose that the result holds for all groups G' with $|G'| < |G|$. If X is a minimal generating set of G, then let $H = \langle X - \{x\} \rangle$ for some $x \in X - N$, with $|H| = m$. If $H \leq N$, then $H \trianglelefteq G$ must be a Dedekind group by the hypothesis and by Theorem 3.4.6, H has a Hamiltonian path. If $e_1, e_2, \ldots, e_{m-1} \in X - \{x\}$ is the sequence of edges that generate the path, so $v_{i+1} = v_i e_i$ for each $i \in \{1, \ldots, m-1\}$, then

$$e_1, e_2, \ldots, e_{m-1}, \underbrace{x, e_1, e_2, \ldots, e_{m-1}}_{[G:H]-1 \text{ times}}$$

is a Hamiltonian path in $\mathrm{Cay}(G, X)$. This is because the sequence moves through all the elements of the cosets $H, v_m x H, \ldots, (v_m x)^{[G:H]-1} H$. If $(v_m x)^i H = (v_m x)^j H$ for $i, j \in \{0, \ldots, [G : H] - 1\}$, with $i \leq j$, then $(v_m x)^{j-i} \in H$. Since $H \trianglelefteq G$ and $v_m \in H$, $v_m x = xh$ for some $h \in H$ and, by applying this inductively, $(v_m x)^{j-i} = x^{j-i} \tilde{h}$ for some $\tilde{h} \in H$. Since $(v_m x)^{j-i} \in H$, this implies that $x^{j-i} \in H$. As $G = \langle x, H \rangle$, $G/H = \langle xH \rangle$ and so $|x| = [G : H]$. As $x^{j-i} \in H$, $x^{j-i} H = H$ and so $[G : H] \mid j - i$, meaning that

$i = j$ and the cosets are distinct. This implies that this defines a Hamiltonian path in $\mathrm{Cay}(G, X)$.

If $H \not\leq N$, then as $[H : H \cap N] \leq [G : N] = 2$, $[H : H \cap N] = 2$ and so by the inductive hypothesis, $\mathrm{Cay}(H, X - \{x\})$ has a Hamiltonian path $(v_1, v_2), \ldots, (v_{m-1}, v_m)$ where $v_1 = 1$ and $v_m \notin N$. By Corollary 2.3.7, each connected component of $\mathrm{Cay}(G, X - \{x\})$ is a coset of H in G and so has a copy of this Hamiltonian path. If $e_1, e_2, \ldots, e_{m-1} \in X - \{x\}$ is the sequence of edges that generate the path, so $v_{i+1} = v_i e_i$ for each $i \in \{1, \ldots, m-1\}$, then it suffices to show that

$$e_1, e_2, \ldots, e_{m-1}, \underbrace{x, e_1, e_2, \ldots, e_{m-1}}_{[G:H]-1 \text{ times}}$$

is a Hamiltonian path in $\mathrm{Cay}(G, X)$. Note that $v_m = e_1 \ldots e_{m-1}$ by definition. To prove that the vertices in this path are distinct, suppose that $(v_m x)^k e_1 \ldots, e_j = e_1 \ldots e_l$ for some $k \in \{0, \ldots, [G : H] - 1\}$ and $j, l \in \{0, \ldots, m-1\}$.

For any $g, h \notin N$, $gh \in N$ as g and h, and hence g^{-1}, must be in the same coset of N in G, and $hN = g^{-1}N$ if and only if $gh \in N$. Using this, if $K = \langle H \cap N, v_m x, x^2 \rangle$, then $K \leq N$ since $v_m x, x^2 \in N$. As $G = \langle H, x \rangle = \langle H \cap N, v_m, x \rangle = \langle K, x \rangle$, $[G : K] = 2$ and so $N = K = \langle H \cap N, v_m x, x^2 \rangle$. Furthermore, since $v_m \in H$, $v_m^2 \in H \cap N$ and hence $v_m^{-2} \in H \cap N$.

Since every subgroup of N is normal in G, $\langle v_m x \rangle \trianglelefteq G$ and so $x v_m, x^2 v_m x^{-1} \in \langle v_m x \rangle$ by conjugating by x and x^2 respectively. If $x v_m = (v_m x)^r$ and $x^2 v_m x^{-1} = (v_m x)^s$ for some $r, s \in \mathbb{N}$, then $x^2 v_m = (v_m x)^s x$ and so $x^2 v_m^2 = (v_m x)^s (v_m x)^r = (v_m x)^{r+s}$, which implies that $x^2 v_m^2 \in \langle v_m x \rangle$. Since $v_m^{-2} \in H \cap N$ and $x^2 v_m^2 \in \langle v_m x \rangle$, $N = \langle H \cap N, v_m x \rangle$.

Since $(v_m x)^k \in H$ by hypothesis and $v_m x \in N$, $(v_m x)^k \in H \cap N$. As $N = \langle H \cap N, v_m x \rangle$ and $H \cap N \trianglelefteq N$, $N/(H \cap N) = \langle v_m x (H \cap N) \rangle$ and so either $k = 0$ or $[N : H \cap N] \mid k$. However, as

$$\begin{aligned}
[G : H \cap N] &= [G : H][H : H \cap N] \\
&= 2[G : H] \\
[G : H \cap N] &= [G : N][N : H \cap N] \\
&= 2[N : H \cap N]
\end{aligned}$$

it must be that $[N : H \cap N] = [G : H]$. Since $k \in \{0, \ldots, [G : H] - 1\}$, this implies that $k = 0$ and hence that $j = l$. This shows that each vertex in the given path is distinct and so it defines a Hamiltonian path in $\mathrm{Cay}(G, X)$. □

Lemma 3.4.8
If G is a group and $N \trianglelefteq G$ is cyclic, then every $H \leq N$ is normal in G.

Proof. Since $N = \langle n \rangle$, $H = \langle n^k \rangle$ for some $k \in \mathbb{N}$. For any $g \in G$, $gng^{-1} = n^i$ for some $i \in \mathbb{N}$ by definition of N being normal in G. As

$$\begin{aligned}
gn^k g^{-1} &= \left(gng^{-1}\right)^k \\
&= \left(n^i\right)^k \\
&= \left(n^k\right)^i
\end{aligned}$$

$gn^k g^{-1} \in H$ and so $H \trianglelefteq G$. □

Corollary 3.4.9
For all $n \geq 3$, the Cayley graph $\mathrm{Cay}(D_{2n}, X)$ has a Hamiltonian path for any minimal generating set $X \subset D_{2n}$.

Proof. Since D_{2n} has a cyclic subgroup of index 2, namely $N = \langle a \rangle$ where $D_{2n} = \langle a, b \mid a^{2n} = 1, a^n = b^2, ba = a^{-1}b \rangle$, and by Lemma 3.4.8 every subgroup of N is normal in G, $\mathrm{Cay}(D_{2n}, X)$ has a Hamiltonian path. □

Corollary 3.4.10
For all $n \geq 2$, the Cayley graph $\mathrm{Cay}(\mathrm{Dic}_{4n}, X)$ has a Hamiltonian path for any minimal generating set $X \subset \mathrm{Dic}_{4n}$.

Proof. Since Dic_{4n} has a cyclic subgroup of index 2, namely $N = \langle a \rangle$ where $\mathrm{Dic}_{4n} = \langle a, b \mid a^n = 1, b^2 = 1, ba = a^{-1}b \rangle$, and by Lemma 3.4.8 every subgroup of N is normal in G, $\mathrm{Cay}(\mathrm{Dic}_{4n}, X)$ has a Hamiltonian path. □

These results raise the question of whether there exists families of groups for which all Cayley graphs have Hamiltonian cycles, just as there are for Hamiltonian paths. However, knowing which groups contain a Hamiltonian path in all their Cayley graphs does not greatly simplify the issue of finding a Hamiltonian cycle; for example, it has been conjectured that every Cayley graph of a dihedral group contains a Hamiltonian cycle but there is not yet a proof of this even for three-element generating sets [22, p. 296].

3.5 Hamiltonian Cycles in the Underlying Graphs of Cayley Graphs

Much of the research surrounding Hamiltonian cycles in Cayley graphs has focused on an outstanding problem in graph theory known as the Lovász conjecture [1, p. 25].

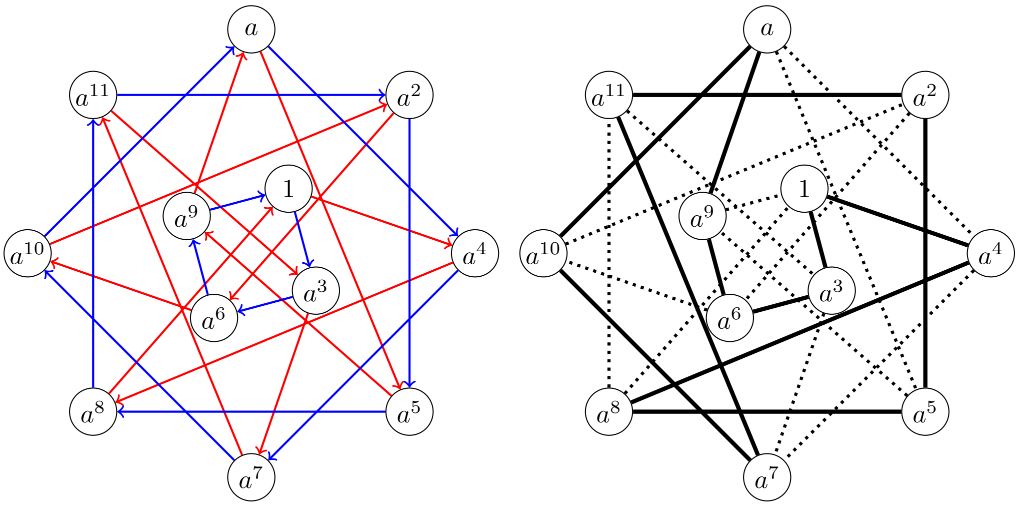
Conjecture 3.5.1 **Original Lovász Conjecture**
Every connected vertex transitive graph on at least three vertices contains a Hamiltonian cycle.

There have been some connected vertex transitive graphs for which the original Lovász conjecture does not hold, such as the Petersen graph, although these all have Hamiltonian paths. However, none of the counterexamples currently known are the underlying graphs to any Cayley graphs, leading to the following weaker conjecture [1, p. 25].

Conjecture 3.5.2 **Weaker Lovász Conjecture**
The underlying graph of any finite connected Cayley graph on at least three vertices contains a Hamiltonian cycle.

Although it followed from Theorem 3.2.2 that a Cayley graph has an Eulerian cycle if and only if its underlying graph has an Eulerian cycle, this does not hold for Hamiltonian cycles in Cayley graphs. Clearly a Cayley graph having a Hamiltonian cycle is a stronger condition than its underlying graph having a Hamiltonian cycle.

For example, the Cayley graph $\mathrm{Cay}\big(C_{12}, \{a^3, a^4\}\big)$ has not got any Hamiltonian cycles; this is shown by contradiction. If $\mathrm{Cay}\big(C_{12}, \{a^3, a^4\}\big)$ had a Hamiltonian cycle with an edge $\big(a^{i \pmod{12}}, a^{i+4 \pmod{12}}\big)$ in the cycle, then $\big(a^{i+1 \pmod{12}}, a^{i+4 \pmod{12}}\big)$ cannot also be an edge in the cycle. This means that $\big(a^{i+1 \pmod{12}}, a^{i+5 \pmod{12}}\big)$ must be the edge from $a^{i+1 \pmod{12}}$ instead. This implies that every edge in the Hamiltonian cycle must be generated by a^4 by applying this argument inductively, which is a contradiction since these edges generate four cycles of length three in $\mathrm{Cay}\big(C_{12}, \{a^3, a^4\}\big)$, as seen in Figure 12. By the same argument, if a Hamiltonian cycle in $\mathrm{Cay}\big(C_{12}, \{a^3, a^4\}\big)$ has an edge generated by a^3, then all edges in the cycle must be generated by a^3, producing a contradiction as these edges generate three cycles of length four in $\mathrm{Cay}\big(C_{12}, \{a^3, a^4\}\big)$, as seen in Figure 12. However, the underlying graph of $\mathrm{Cay}\big(C_{12}, \{a^3, a^4\}\big)$ does contain a Hamiltonian cycle, which is highlighted in Figure 12.



(a) $\mathrm{Cay}\big(C_{12}, \{a^3, a^4\}\big)$

(b) A Hamiltonian cycle in the underlying graph of $\mathrm{Cay}\big(C_{12}, \{a^3, a^4\}\big)$.

Figure 12: A demonstration using $\mathrm{Cay}\big(C_{12}, \{a^3, a^4\}\big)$ that Cayley graphs with Hamiltonian cycles in their underlying graphs do not necessarily have Hamiltonian cycles.

Although the weaker Lovász conjecture is not true for Cayley graphs when considered as directed graphs, no counterexamples have yet been found when considering their underlying graphs. However, some results proving the conjecture for certain families of finite groups are known. For example, a stronger statement than Theorem 3.4.6 holds for the underlying graphs of abelian groups; as given in [19, p. 9], the weaker Lovász conjecture holds for all underlying graphs of Cayley graphs of abelian groups.

Theorem 3.5.3
If G is a finite abelian group and $X \subset G$ is a minimal generating set of G, then the underlying graph of $\mathrm{Cay}(G, X)$ *has a Hamiltonian cycle.*

One of the strongest results regarding the weaker Lovász conjecture for non-abelian groups regards those with cyclic p-group commutator subgroups.

Theorem 3.5.4
If G is a finite group such that its commutator subgroup $[G, G] \cong C_{p^n}$ for some prime p and $n \in \mathbb{N}$ and $X \subset G$ is a minimal generating set of G, then the underlying graph of $\mathrm{Cay}(G, X)$ *has a Hamiltonian cycle.*

Although the proof will be omitted from this essay, a sketch proof can be found in [22, p. 295]. This shows that, for example, D_{2p^k} for any prime p and $k \in \mathbb{N}$ has a Hamiltonian cycle in the underlying graph of every Cayley graph, since $[D_{2n}, D_{2n}] = \langle x^2 \rangle$ and

$$\left|x^2\right| = \begin{cases} \frac{n}{2} & n \text{ is even} \\ n & n \text{ is odd} \end{cases}$$

where $D_{2n} = \langle x, y \mid x^n = 1, y^2 = 1, yx = x^{-1}y \rangle$.

4 Conclusion

Cayley graphs provide an intriguing alternative perspective of the groups they represent, allowing their properties to be viewed in a graph-theoretic rather than purely algebraic way. Although they are constructed in a fairly intuitive way, it is clear that they provide a significant amount of insight into important questions in both graph theory and group theory. In this essay, we have explored many key properties of Cayley graphs and their cycles, including their importance in studying the Lovász conjecture, a famous open problem in graph theory.

Although this essay has provided an introduction to the study of Cayley graphs, they are related to many problems in wide-ranging areas of mathematics, computer science and even molecular biology [14]. Furthermore, here the focus has been primarily on Cayley graphs of finite groups, but the same constructions can be made for infinite groups. The construction of infinite Cayley graphs is related to several important problems, such as the solvability of the word problem, which is the question of whether two given words in the generators represent the identity element [15, pp. 109–113].

References

[1] Lázló Babai. Automorphism groups, isomorphism, reconstruction. In Ronald L. Graham, Martin Grotschel, and Lázló Lovász, editors, *Handbook of Combinatorics*, volume 2, chapter 27. Elsevier, 1995. ISBN 9780444823519.

[2] Jørgen Bang-Jensen and Gregory Gutin. *Digraphs: Theory, Algorithms and Applications*. Springer-Verlag, 2007. ISBN 9781852336110.

[3] Stanley Burris and H. P. Sankappanavar. *A Course in Universal Algebra*. 2012. ISBN 9780988055209. Originally published by Springer-Verlag, 1981 as part of *Graduate Texts in Mathematics*. This edition made available freely online at `https://www.math.uwaterloo.ca/~snburris/htdocs/ualg.html`.

[4] Marek Cygan, Dániel Marx, Marcin Pilipczuk, Michał Pilipczuk, and Ildikó Schlotter. Parameterized complexity of Eulerian deletion problems. *Algorithmica*, 68: 41–61, 2014.

[5] Vassilios V. Dimakopoulos, Leonidas Palios, and Athanasios S. Poulakidas. On the Hamiltonicity of the Cartesian product. *Information Processing Letters*, 96(2): 49–53, 2005.

[6] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, Inc., 2004. ISBN 9780471433347.

[7] Michael R. Garey and David S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. A Series of Books in the Mathematical Sciences. W. H. Freeman and Company, 1979. ISBN 9780716710455.

[8] Chris Godsil and Gordon Royle. *Algebraic Graph Theory*, volume 207 of *Graduate Texts in Mathematics*. Springer-Verlag, 2001. ISBN 9780387952208.

[9] Jonathan L. Gross, Jay Yellen, and Mark Anderson. *Graph Theory and its Applications*. CRC Press, 2019. ISBN 9780429757099.

[10] Lorenz Halbeisen, Martin Hamilton, and Pavel Růžička. Minimal generating sets of groups, rings, and fields. *Quaestiones Mathematicae*, 30(3):355–363, 2007.

[11] Nicholas Jackson. MA249 Algebra II: Groups and Rings. Lecture notes, University of Warwick, 2022.

[12] William T. Trotter Jr. and Paul Erdös. When the Cartesian product of directed cycles is Hamiltonian. *Journal of Graph Theory*, 2(2):137–142, 1978.

[13] Joseph B. Klerlein. Hamiltonian cycles in Cayley color graphs. *Journal of Graph Theory*, 2(1):65–68, 1978.

[14] Elena Konstantinova. Some problems on Cayley graphs. *Linear Algebra and its Applications*, 429(11–12):2754–2769, 2008.

[15] John Meier. *Groups, Graphs and Trees*. Cambridge University Press, 2012. ISBN 9781139167505.

[16] Joseph J. Rotman. *An Introduction to the Theory of Groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, 1994. ISBN 9780387942858.

[17] Gert Sabidussi. On a class of fixed-point free graphs. *Proceedings of the American Mathematical Society*, 9(5):800–804, 1958.

[18] Rob Silversmith. MA241 Combinatorics. Lecture notes, University of Warwick, 2022.

[19] Mary Stelow. Hamiltonicity in Cayley graphs and digraphs of finite abelian groups. The University of Chicago Mathematics REU 2017, 2017.

[20] Gareth Tracey. MA3K4 Introduction to Group Theory. Lecture notes, University of Warwick, 2022.

[21] Tanakorn Udomworarat and Teerapong Suksumran. An algorithm for finding minimal generating sets of finite groups. *Algebraic Structures and their Applications*, 8 (2):131–143, 2021.

[22] David Witte and Joseph A. Gallian. A survey: Hamiltonian cycles in Cayley graphs. *Discrete Mathematics*, 51(3):293–304, 1984.

[23] David S. Witte. On Hamiltonian circuits in Cayley diagrams. *Discrete Mathematics*, 38(1):99–108, 1982.