# Basic Properties of Cayley Graphs

Andrew Duncan and Andrew Cortis

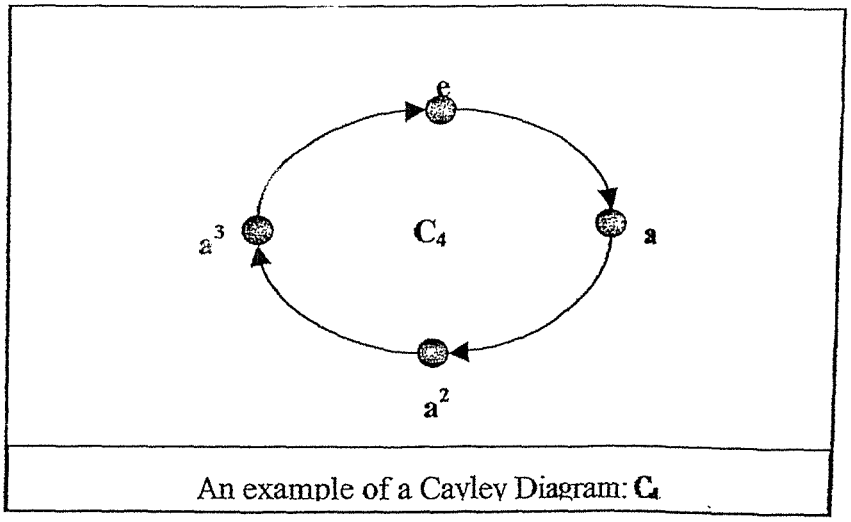
## Introduction

Cayley Diagrams are one of many representations of finite groups. They provide a means of representing a group diagrammatically and various properties of groups including commutativity can be extracted from the graph. The Cayley diagram also provides sufficient information to test for isomorphism between groups, and thus is a useful tool for recognizing the type of a given group. This technique of representing groups as graphs was introduced by Cayley in 1878. The Cayley diagrams described below are a variant of the actual Cayley diagram and are referred to as Cayley Digraphs.

Let $S = \{g_1, g_2, \ldots, g_n\}$ be a set of distinct elements and let $G = < g_1, g_2, \ldots, g_n >$, i.e. G is the group generated by the set S.

We can define a relation ~ on G such that $a \sim b$ iff $b = g_i a$ , where $g_i \in S$. Then the Cayley Digraph Cay(G,S) is the digraph formed from the relation ~, where the vertex set of the graph is the group G.

Informally, the Cayley Digraph is a digraph with the elements of G as vertices, and there is an edge from a to b if $b = g_i a$, where $g_i$ is some generator of G.




An example of a Cayley Diagram: $C_4$

Here are various simple properties of Cayley Digraphs:

1. Let $a$ be a vertex in Cay(G, S), and $|S| = n$, then $\deg^+(a) = \deg^-(a) = n$.

   **Proof:**

   Let $a \in G$, then $g_1^{-1}a, g_2^{-1}a, g_3^{-1}a, \ldots, g_n^{-1}a$ are n distinct elements in G (by closure), since suppose that:

   $$g_i^{-1}a = g_j^{-1}a, \quad g_i, g_j \in S,$$
   $$\Rightarrow g_i^{-1} = g_j^{-1} \Rightarrow g_i = g_j,$$

   since inverse elements are unique, contradicting the premise that elements of S are distinct.

   $$g_i^{-1}a \sim a, \; i = 1 \ldots n. \quad \therefore \deg^-(a) = n$$

   Similarly,

   $g_1a, g_2a, \ldots, g_na$ are n distinct elements in G (by closure), and $a \sim g_ia$, for all $i = 1 \ldots n$.

   $$\therefore \deg^+(a) = n$$

2. Cay(G,S) is strongly connected (ie. *there is a path from a to b and from b to a whenever a and b are vertices in the graph*)

   Proof:

   Let $a, b \in G$.

   $b = (ba^{-1})a$ and $ba^{-1} \in G$ (closure in G)

   Now since S is the generator set for G, $ba^{-1}$ can be expressed as :

   $ba^{-1} = a^{1`}a^{2`}a^{3`}\ldots a^{k`}$ such that $a^{1`}, \ldots, a^{k`} \in S$ (not necc. distinct).

   Therefore, one can follow the edges defined by the sequence of generators $a^{1`}a^{2`}a^{3`}\ldots a^{k`}$, starting from vertex **a** to form a path from a to **b**.

   Using the same approach one can also find a path from b to a

3. If $G \neq \{e\}$ then $\sim$ is irreflexive i.e. Cay(G,S) has no loops

Proof:

If $G \neq \{e\}$, then $\{e\} \neq S$, and so $a \neq g_i a$ for any $g_i \in S$.

Thus, a is not related to itself, and so there are no reflexive loops in Cay(G,S).

4. If for all $g \in S$, $g^{-1} \in S$, then ~ is a symmetric relation, ie Cay(G,S) is an undirected graph.

The following proposition is stated without proof. This proposition can be possibly used as a test to check whether two groups are not isomorphic from their Cayley Digraph.

5. Let $G_1 = \langle S_1 \rangle$, $G_2 = \langle S_2 \rangle$ be isomorphic groups, $|S_1| \leq |S_2|$, then $Cay(G_1,S_1)$ is isomorphic to a sub graph of $Cay(G_2,S_2)$.

## Paths in Cayley Digraphs

**Definition:** A Hamiltonian Path in a directed graph is a path passing through every vertex exactly once.

It was noted that there appeared to be Hamiltonian paths in all the Cayley diagrams sketched. As of yet, however, no proof or disproof exists that every Cayley diagraph has a Hamiltonian path. To make matters worse, searching for Hamiltonian paths in a graph is intractable, thus making testing of large Cayley diagrams for Hamiltonian paths prohibitive.

This is known as *Lovàsz conjecture* and is stated as follows:

**Conjecture**: (*Lovàsz*) All Cayley Diagrams have a Hamiltonian path.

ie. For any group $G = \langle S \rangle$, Cay(G,S) has a Hamiltonian path.

By exhaustively testing various Cayley digraphs, Willis [3] found a group ($C_2 x A_4$) which doesn't have a Hamiltonian path for a **particular generating set**. However, choosing a different generating set for the above will yield a Cayley Diagram with a Hamiltonian path.

The conjecture should thus be revised to the following form:

**Conjecture**: Let G be a finite group, then Cay(G,S) has a Hamiltonian path for some appropriate choice of the generating set S.

The following propositions prove the conjecture for various classes of groups. Many stronger proofs are available, usually using complex graph theory. For more information see [2]

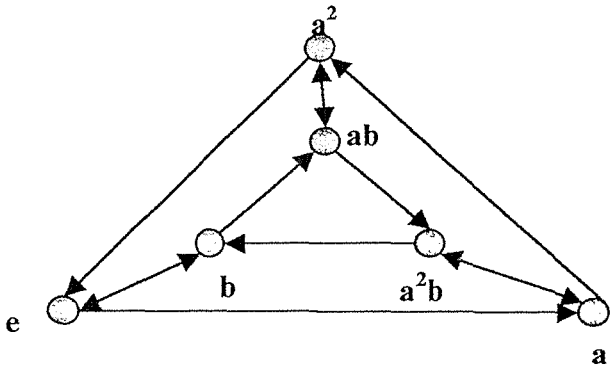
**Prop 1:** $Cay(C_n,\{a\})$ has a Hamiltonian cycle, for any $n \in \dot{U}^+$.

**Proof:**

Basis : $Cay(C_1,\{a\})$ is Hamiltonian since it consists of a single vertex.

Assume Cay(Ck, {a}) is Hamiltonian where $Ck = \{e, a, a^2, a^3,\ldots, a^{k-1}\}$

We can construct $Cay(C_{k+1},\{a\})$ from Cay(Ck, {a}) by inserting a vertex $a^k$ between $a^{k-1}$ and e. Inserting this element does not affect Hamiltonicity, hence by inductive hypothesis, $Cay(C_{k+1},\{a\})$ is also Hamiltonian.




The Dihedral group $D_3$

Dn can be regarded as two n-polygons inset in each other

**Prop 2:** $Cay(D_n,S)$, S= {a,b} is Hamiltonian

Proof:

Dn = <a,b>, st o(a) = n

o(b) = 2

$o(Dn) = 2n$

From the definition of $D_n$, we can also derive:

$(ab)^2 = e$

$(ba^i) = a^{n-i}b$ *

We can identify two cyles in Cay(Dn, S), namely

$$e \sim a \sim a^2 \sim a^3 \sim, \ldots, \sim a^{n-1}$$

and

$$b \sim ab \sim a^2b \sim, \ldots, \sim a^{n-1}b$$

The number of elements in these two cycles totals to 2n, so every element must be a member of one of the cycles. In fact, every element must be a member of exactly one of these cycles.

Since suppose $\exists\ d \in D_n$ such that $d = a^i = a^jb,\ 0 < i \neq j < n$

$\Rightarrow a^j = a^ib$ using *

$\Rightarrow a^j = a^ib^2$

$\Rightarrow a^i = a^j$ but this only holds when $i,j = 0$ or n, which is a contradiction.

In the case where $i = j$, then

$a^i = a^jb \Rightarrow e = b$, which is also a contradiction

Also, we have $a^{n-1} \sim ab$ since ($ba^{n-1} = ab$ by *), and $b \sim e$ (since $b^2 = e$).

We can now define the following path:

$e \rightarrow a \rightarrow a^2 \rightarrow \ldots \rightarrow a^{n-1} \rightarrow ab \rightarrow a^2b \rightarrow a^3b \rightarrow \ldots \rightarrow a^{n-1}b \rightarrow b \rightarrow e$, which is a cycle containing every vertex in $Cay(D_n,S)$ exactly once, hence it is a Hamiltonian Path.

**Prop 3:** Cay(Cm x Cn, S), S = {(a,e) , (e,b)} is Hamiltonian

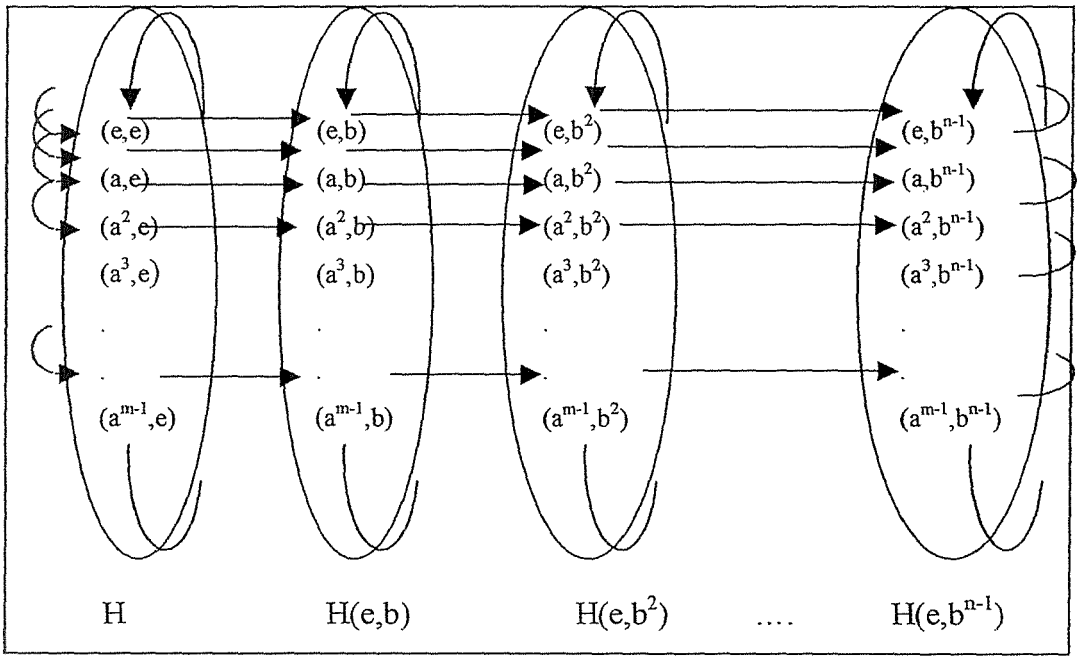
**Proof:**

Let $H = \langle a \rangle$. Then $H < Cm \times Cn$ and $o(H) = m$.

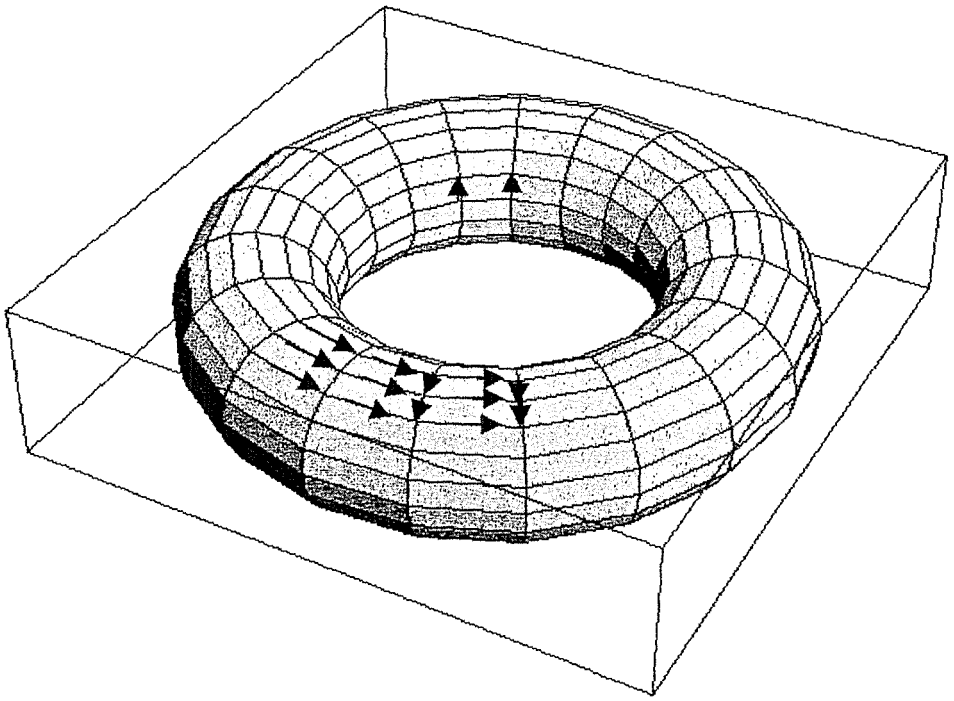
Therefore we can partition Cm x Cn into n cosets: H, H(e,b), …, $H(e,b^{n-1})$

Clearly in each coset we have $(a^i,b^j) \rightarrow (a^{i+1},b^j)$. Thus each coset forms a cycle within itself as shown in the diagram below. Between consecutive cosets we

also have that $(a^i,b^j) \rightarrow (a^i, b^{j+1})$. These relations impose a directed grid on the set set of elements in Cm x Cn.




In fact, the graph Cay(Cm x Cn, S) can be regarded as a directed grid on a torus in 3D space. Each ring in the torus represents a coset in the group. Finding a Hamiltonian in Cay(Cn x Cm, S) is reduced to finding a Hamiltonian path along the surface of this torus.

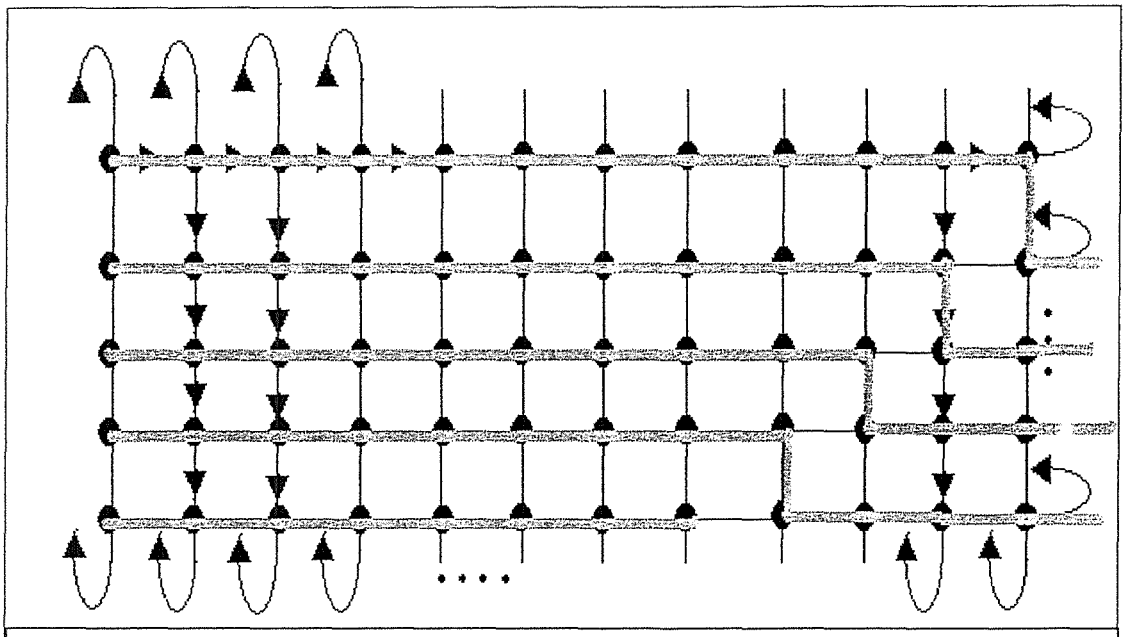


For each $i \in \mathbf{N}$, $0 < i < m$, we can define path Pi as:

$$Pi = (a^i,b^{n-i}) \rightarrow (a^i,b^{n-i+1}) \rightarrow \ldots \rightarrow (a^i,b^{n-1})$$
$$\rightarrow (a^i,e) \rightarrow (a^i,b) \rightarrow (a^i,b^2) \rightarrow \ldots \rightarrow (a^i,b^{n-i-1})$$

$P_i$ represents a Hamiltonian path of the ith row of the Cayley digraph and contains n vertices

Also for all $i,j \in \mathbf{N}$, $0 \leq i < m, 0 \leq j < n$, $(a^i,b^j) \rightarrow (a^{i+1},b^j)$
Using these edges we can join each Pi, i = 1...m-1 to form a Hamiltonian path for the entire graph as illustrated in the diagram below:



An illustration of the path taken to form a Hamiltonian path on the surface of a torus

The path $(e,e) \rightarrow (e,b) \rightarrow (e,b^2) \rightarrow \ldots \rightarrow (e,b^{n-1}) \rightarrow P_1 \rightarrow P_2 \rightarrow P_3 \rightarrow \ldots \rightarrow P_{m-1}$ contains mn = o(Cm x Cn) elements, each element exactly once, therefore it is a Hamiltonian path as required.

While this proof only applies for the direct products of 2 cyclic groups, it could be used as a basis for a proof for the direct product of an arbitrary number of elements. Instead of considering a grid of vertices on a torus in 3D space, one must search for a Hamiltonian path in a grid of vertices on an n-dimensional torus. Since every Abelian group a direct product of cyclic groups, proving Hamiltonicity for an arbitrary direct

product will automatically imply the Hamiltonicity of all Abelian groups.

## Applications

One application of Cayley Diagrams is in that on binary representation of data, namely Gray Codes. A gray code of length n is a sequence of n bit binary strings, with the property that consecutive words differ by at most one element. Gray codes are useful in mechanical encoders since a slight change in location only affects one bit. Using a typical binary code, up to n bits could change, and slight misalignments between reading elements could cause high levels of error since flipping a bit will increase/ decrease the value by a power of two. For example, an error flipping the MSB of an 8-bit word will change the value by $2^7$.

Gray Codes can be represented by the direct product $(C_2)^n$. The difference between Gray Code and normal binary code is the ordering of the elements. In Gray code the "greater than" relation $\geq$ is defined as follows:

$$\text{For } a, b \in (C_2)^n, \quad a \geq b \text{ iff } a \rightarrow^* b$$

The fact that $((C_2)^n, \geq)$ is a totally-ordered set follows from that we can always find a Hamiltonian path in $Cay((C_2)^n,S)$ (since every two elements in the path are comparable) Thus $((C_2)^n, \geq)$ is a well ordered set by choosing the starting vertex (element) of the Hamiltonian path as the least element.

## References

[1] The Fascination of Groups, F. J. Budden, 1972

[2] Hamiltonian Paths in Cayley Graphs, I. Pak; R. Radocic, Department of Mathematics, MIT, June 2002

[3] Hamiltonian Paths and Cayley Digraphs of Algebraic Groups, S. Willis, UCSD Honors Thesis 2001