Honor Thesis on Hamiltonian Circuit in Cayley Graphs

Jiaming Zhang

April 2025

1 Thesis Overview

This thesis addresses a long-standing open problem in algebraic graph theory:

Conjecture 1 (Lovász-type Conjecture for Cayley Graphs)**.** *Every finite connected Cayley graph is Hamiltonian.*

While partial progress has been made over the decades, a complete resolution remains elusive. In exploring the foundational literature, I carefully analyzed a 1983 paper by Dragan Marušič, which presented a construction intended to prove the Hamiltonicity of Cayley graphs for certain group classes. [1] Upon close examination, I identified a critical gap in the proof—specifically, a lack of rigorous justification for the completeness of the proposed algorithm. Motivated by this, my thesis establishes a corrected and extended version of Marušič's method, providing a formal proof for the algorithm's ability to generate Hamiltonian sequences (Lemma 3.2 below). The core contribution is a recursive construction framework that, when combined with Marušič's original approach, produces dynamic Hamiltonian paths across group layers. This work not only fills a crucial logical gap in a well-cited result, but also contributes a validated method that may aid further exploration of Hamiltonian properties in group-theoretic graph structures. [2] [3]

2 Preliminaries

In this section, we keep the original notation and definition from Marušič's paper.

Definition 1. *If Γ is a graph, then $V(\Gamma)$ and $E(\Gamma)$ will denote the set of vertices and the set of edges of Γ, and A graph Γ is said to be Hamiltonian if it has a Hamiltonian circuit, that is, a circuit of length $|V(F)|$.*

Definition 2. *Let G be a group, with identity element e. If $g \in G$, then $|g|$ will denote the order of g. If $M \subseteq G$, then we define the following*

(a) $M^{-1} = \{x^{-1} : x \in M\}$, *the set of inverses of elements in* M.

(b) $M_0 = M - \{e\}$, *the set of elements in* M *excluding the identity element.*

(c) $M^* = M_0 \cup M_0^{-1}$, *the union of* M_0 *and the set of inverses of* M_0.

(d) M = *The subgroup of* G *generated by* M.

Example 1. *Let* $G = \mathbb{Z}_{12}$, $M = \{0, 2, 3, 6\}$. *Then,* $M^{-1} = \{0, 6, 9, 10\}$, $M_0 = \{2, 3, 6\}$, $M^* = M_0 \cup M_0^{-1} = \{2, 3, 6\} \cup \{10, 9, 6\} = \{2, 3, 10, 9, 6\}$, *and* $M = \langle M\rangle = \mathbb{Z}_{12}$.

Definition 3 (Sequence)**.** *A sequence* $S = [s_1, s_2, \ldots, s_r]$ *on* G *is a sequence all of whose terms are elements of* G. *By* $\Box$ *we shall denote the empty sequence on* G, *that is, the sequence with no terms. All other sequences on* G *will be called non-empty. For a sequence* P, *denoted by* r_P *its length.*

Definition 4 (Partial Product of Sequence)**.** *Let* $S = [s_1, s_2, \ldots, s_r]$ *be a sequence on* G. *Then, the* i*-th partial product* $\pi_i(S)$ *of* S *is* $s_1 s_2 \ldots s_i$. *We also set* $\pi(S) \colon = \pi_r(S)$.

Example 2 (following the previous example)**.** *: Let* $G = \mathbb{Z}_{12}$ *and* $S = [s_1, s_2, \ldots, s_r] = [1, 6, 9, 3, 1, 2, 5]$. *Then* $\pi_3(S) = 1 \cdot 6 \cdot 9 = 1 + 6 + 9 = 16 = 4$, $\pi(S) = 1 \cdot 6 \cdot 9 \cdot 3 \cdot 1 \cdot 2 \cdot 5 = 1 + 6 + 9 + 3 + 1 + 2 + 5 = 27 = 3$, *and* $r_S = r$.

Definition 5 (Hamiltonian Sequence)**.** *We say that* S *is hamiltonian if* $r_S = |G|$, $\pi(S) = e$, *and the partial products* $\pi_i(S)$, $i = 1, 2, \ldots, r-1$, *are all distinct non-identity elements of* G.

Example 3. *Let* $G = \mathbb{Z}_{12}$, $S = [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]$. *Then,* $r_S = |G| = 12$, $\pi(S) = 12 = e$, *and each of the partial products are all distinct non-identity elements of* G.

Definition 6 (M-Sequence)**.** *If* $s_i \in M$, *for* $i = 1, 2, \ldots, r$, *then* S *is called an* M*-sequence on* G, *and we define* $\mathcal{H}(M, G)$ *denote the set of all hamiltonian* M^**-sequences on* G.

Example 4 (following the previous example)**.** *Let* $G = \mathbb{Z}_{12}$ *and* $M = \{0, 2, 3, 6\}$, *then* $S = [2, 3, 6, 3, 2, 2, 3]$ *is a* M*-sequence on* G.

Definition 7 (Operations on Sequences)**.** *Let* $S = [s_1, s_2, \ldots, s_r]$, $T = [t_1, t_2, \ldots, t_q]$ *be sequences on* G. *Then:*

(a) $S^{-1} \colon = [s_r^{-1}, s_{r-1}^{-1}, \ldots, s_1^{-1}]$, *is called the inverse sequence of sequence* S.

(b) $l_S \colon = s_r$, $r \geq 2$.

(c) *We define* $\overline{S}$ *by* $[s_1, s_2, \ldots, s_{r-1}]$, $r \geq 2$, *as the sequence* S *without the last element.*

(d) *We define* $\hat{S}$ *by*
$\hat{S}\colon = [s_2, s_3, \ldots, s_{r-1}]$, $r \geq 3$.
$\hat{S}\colon = \Box$, $r = 2$.

(e) $ST\colon = [s_1, s_2, \ldots, s_r, t_1, t_2, \ldots, t_q]$

(f) (S, T)
$(S,T)\colon = [t_1]\hat{S}^{-1}[t_2]\hat{S}\ldots[t_{q-2}]\hat{S}^{-1}[t_{q-1}]\hat{S}$ *if* $q \geq 3$ *is odd.*
$(S,T)\colon = [t_1]\hat{S}^{-1}[t_2]\hat{S}\ldots[t_{q-3}]\hat{S}^{-1}[t_{q-2}]\hat{S}$ *if* $q \geq 4$ *is even.*
$(S,T)\colon = \Box$ *if* $q \in \{1, 2\}$.

(g) S^n, *for* $n \in \mathbb{N} \cup \{0\}$
$S^n\colon = \Box$ *if* $n = 0$.
$S^n\colon = S^{n-1}S$ *if* $n \geq 1$.

(h) $\Box S = S\Box = S$ *and* $\Box^n = \Box^m = \Box$.

Example 5 (follow the previous example)**.** *:*
Let $S = [2, 3, 6, 3, 2, 3]$, $T = [1, 2, 3]$, $R = [11, 10]$, *and* $U = [5, 6, 7, 8]$ *be sequences on* $G = \mathbb{Z}_{12}$. *Then:*
$S^{-1} = [9, 10, 9, 6, 9, 10]$,
$l_S = 3$,
$\overline{S} = [2, 3, 6, 3, 2]$,
$\hat{S} = [3, 6, 3, 2]$.
$\hat{R} = \Box$.
$ST = [2, 3, 6, 3, 2, 3, 1, 2, 3]$
$(S, T) = [1, 10, 9, 6, 9, 2, 3, 6, 3, 2]$
$(S, U) = [5, 10, 9, 6, 9, 6, 3, 6, 3, 2]$
$(S, R) = \Box$.
$S^0 = \Box$.
$S^3 = [2, 3, 6, 3, 2, 3, 2, 3, 6, 3, 2, 3, 2, 3, 6, 3, 2, 3]$.

Definition 8 (Cayley graph)**.** *Letting* M *be a generating set of* G*, the Cayley graph* $\Gamma(G, M)$ *is defined to be a graph such that* $V(\Gamma(G, M)) = G$ *and two vertices* x, y *of* G *are adjacent in* $\Gamma(G, M)$ *if and only if* $xy^{-1} \in M^*$.

Remark 1. $\Gamma(G, M)$ *is a connected vertex symmetric graph, if and only if* M *is a generating set for* G*. All Cayley graphs dealt with in this thesis will be assumed to have at least three vertices.*

Lemma 2.1. *For any surjective group homomorphism* $\varepsilon\colon G \to \overline{G}$, $\varepsilon(x) = xH$ $\forall x \in G$*, where* $\overline{G} = G/H$ *as the quotient group. For any generating set* X *of* G*, we have*

$$\overline{G} = \langle \varepsilon(X) \rangle.$$

Proof. Let G be a group and H a normal subgroup of G, so the quotient group G/H is well-defined. Let X be a generating set of G, meaning $G = \langle X \rangle$. Define a group homomorphism $\varepsilon : G \to G/H$ by $\varepsilon(x) = xH$ for all $x \in G$. We aim to prove that

$$G/H = \langle \varepsilon(X) \rangle$$

by double inclusion. By the definition of ε, for any $x \in X$, $\varepsilon(x) = xH \in G/H$. Thus, $\varepsilon(X) \subseteq G/H$, and $\langle \varepsilon(X) \rangle$ is a subgroup of G/H. Therefore, $\langle \varepsilon(X) \rangle \subseteq G/H$. For any $gH \in G/H$, there exists $g \in G$. Since X generates G, g can be written as $g = x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ for some $x_i \in X$ and $k_i \in \mathbb{Z}$. Applying the homomorphism ε, we have:

$$\varepsilon(g) = \varepsilon(x_1)^{k_1} \varepsilon(x_2)^{k_2} \dots \varepsilon(x_n)^{k_n},$$

where $\varepsilon(x_i) \in \varepsilon(X)$. Hence, $gH = \varepsilon(g) \in \langle \varepsilon(X) \rangle$. $\square$

Lemma 2.2. *Let G be a finite abelian group, $H \leq G$, $g \in G$, $g \notin H$. Let also $j \in \mathbb{N}$ be the smallest positive integer such that $g^j \in H$. Suppose that $G = \langle H \cup \{g\} \rangle$. Then*

$$|H| \cdot j = |G|.$$

Proof. Since G is abelian, $H \trianglelefteq G$. Consider $\overline{G} = G/H$ and let $\varepsilon(x) = xH$, $\forall x \in G$ be the natural homomorphism. Clearly,

$$\overline{G} = \langle \varepsilon(H \cup \{g\}) \rangle = \langle \{eH, gH\} \rangle = \langle gH \rangle = \langle \varepsilon(g) \rangle$$

by Lemma 1.1. Further, $|\varepsilon(g)| = j$. Indeed, as ε is a homomorphism,

$$(\varepsilon(g))^j = \varepsilon(g^j) = \varepsilon(e) = eH = H,$$

and j is the smallest integer with this property as defined. Therefore, $|\overline{G}| = j$, and $|\overline{G}| \cdot |H| = |G|$ by Lagrange's theorem ($|\overline{G}| = [G : H]$), which implies

$$|H| \cdot j = |G|.$$

$\square$

3 Theorems and Lemmas

Lemma 3.1. *The Cayley graph $F(G, M)$ is hamiltonian if and only if $\mathcal{H}(M, G)$ is not empty.*

Lemma 3.2 (Corrected version of Lemma 3.1 of [1])**.** *Let M be a generating set of an abelian group G and M' be a non-empty subset of M_0. If $S \in \mathcal{H}(M', \langle M' \rangle)$, then there exists a sequence T on G such that $\overline{S}T \in \mathcal{H}(M, G)$.*

Proof. We proceed by induction on the cardinality of $M_0 \setminus M'$. The assertion of Lemma 3.1 is clearly true if $M_0 \setminus M' = \emptyset$. Let $M_0 \setminus M' \neq \emptyset$, $g \in M_0 \setminus M'$, $H = \langle M \setminus \{g\} \rangle$, and j be the smallest positive integer such that $g^j \in H$. By the induction hypothesis, there exists a sequence Q of elements of H such that $\overline{S}Q, \in \mathcal{H}(M \setminus \{g\}, H)$. If $W = \overline{S}Q$, Let T be the sequence:

$$T = \begin{cases} \overline{Q}(W, [g]^j)[l_W][g^{-1}]^{j-1}, & \text{if } j \text{ is odd;} \\ \overline{Q}(W, [g]^j)[g](\overline{W})^{-1}[g^{-1}]^{j-1}, & \text{if } j \text{ is even.} \end{cases}$$

Then $\overline{S}T \in \mathcal{H}(M, G)$.

Now, we verify that $\overline{S}T$ is a *Hamiltonian* sequence on G. Specifically, we must show:

(a) $r_{\overline{S}T} = |G|$

(b) $\pi(\overline{S}T) = \text{e}$

(c) The partial products $\pi_i(\overline{S}T)(i = 1, 2, \dots, r-1)$ are all distinct non-identity elements of G.

(a) As what we assumed for the inductive steps, $W = \overline{S}Q$ is already a *hamiltonian* sequence on H, which means the length of $r_W = |H| = |G|/j$ by Lemma 1.2. For the odd j case:

$$\overline{S}T = \overline{S}\,\overline{Q}(W, [g]^j)[l_W][g^{-1}]^{j-1}$$

$$\begin{aligned} r_{\overline{S}T} &= r_{\overline{S}\,\overline{Q}} + r_{(W,[g]^j)} + r_{l_W} + r_{[g^{-1}]^{j-1}} \\ &= \frac{|G|}{j} - 1 + (j-1) \cdot \left(\frac{|G|}{j} - 2 \right) + (j-1) + 1 + (j-1) \\ &= |G|. \end{aligned}$$

For the even j case:

$$\overline{S}T = \overline{S}\,\overline{Q}(W, [g]^j)[g](\overline{W})^{-1}[g^{-1}]^{j-1}$$

$$\begin{aligned} r_{\overline{S}T} &= r_{\overline{S}\,\overline{Q}} + r_{(W,[g]^j)} + r_{[g]} + r_{(\overline{W})^{-1}} + r_{[g^{-1}]^{j-1}} \\ &= \frac{|G|}{j} - 1 + (j-2) * (\frac{|G|}{j} - 2) + (j-2) + 1 + \frac{|G|}{j} - 1 + (j-1) \\ &= |G|. \end{aligned}$$

Thus the length of sequence, $r_{\overline{S}T}$, in both cases regarding the parity of j, are identical with the of order of the group G.

(b) We now verify that $\pi(\overline{S}T) = \mathrm{e}$, i.e., the product of all elements in the sequence $\overline{S}T$ equals the identity element of G. By the inductive hypothesis, $W = \overline{S}Q$ is already a *Hamiltonian* sequence on H, which means

$$\pi(\overline{S}Q) = \mathrm{e}.$$

For the odd j case:

$$\overline{S}T = \overline{S}\,\overline{Q}(W, [g]^j)[l_W][g^{-1}]^{j-1}$$

Given that G is abelian, we can pair up $\overline{S}\,\overline{Q}$ and $[l_W]$ to form $\pi(\overline{S}Q) = \mathrm{e}$. Since j is odd, there are $j-1$ times $[g]$ in sequence $(W, [g]^j)$, and we can pair up with $[g^{-1}]^{j-1}$ at the end, which means $\pi([g]^{j-1}[g^{-1}]^{j-1}) = \mathrm{e}$. Also, since $j-1$ is even, as the alternating definition of $(W, [g]^j)$, $\widehat{\overline{S}Q}^{-1}$ and $\widehat{\overline{S}Q}$ each show up $\frac{j-1}{2}$ times, which means they can be canceled out. This is easy to observe as: (suppose $\widehat{\overline{S}Q} = [\alpha_1, \alpha_2, \ldots, \alpha_n]$)

$$\begin{aligned}\widehat{\overline{S}Q}^{-1}\widehat{\overline{S}Q} &= [\alpha_n^{-1}, \alpha_{n-1}^{-1}, \ldots, \alpha_1^{-1}][\alpha_1, \alpha_2, \ldots, \alpha_n] \\ &= \alpha_1\alpha_1^{-1}\alpha_2\alpha_2^{-1}\ldots\alpha_n\alpha_n^{-1} \text{ (by abelian)} \\ &= \mathrm{e}.\end{aligned}$$

Thus, all the elements in $\overline{S}T$ canceled out into identity element, which means $\pi(\overline{S}T) = \mathrm{e}$, and for the even j case:

$$\overline{S}T = \overline{S}\,\overline{Q}(W, [g]^j)[g](\overline{W})^{-1}[g^{-1}]^{j-1}$$

Since j is even, $(W, [g]^j)$ has $j-2$ times $[g]$. Together with the following $[g]$, there are $j-1$ times $[g]$, which can be canceled out with the $[g^{-1}]^{j-1}$ sequence at the end of the formula. Additionally, with the same reason in the odd j case, as the alternating definition of $(W, [g]^j)$, $\widehat{\overline{S}Q}^{-1}$ and $\widehat{\overline{S}Q}$ each show up $\frac{j-2}{2}$ times, which means they can also be canceled. Also,

$$\overline{W} = \overline{\overline{S}Q} = \overline{S}\,\overline{Q} \implies (\overline{W})^{-1} = (\overline{S}\,\overline{Q})^{-1}$$

Hence the initial $\overline{S}\,\overline{Q}$ can be canceled with $(\overline{W})^{-1}$. Thus, all the elements in $\overline{S}T$ canceled out into identity element, which means $\pi(\overline{S}T) = \mathrm{e}$.

(c) For the odd j case:

$$\overline{S}T = \overline{S}\,\overline{Q}(W, [g]^j)[l_W][g^{-1}]^{j-1}$$

To expand this expression,

$$\overline{S}T = \overline{S}\,\overline{Q}[g]\hat{W}^{-1}[g]\hat{W}\ldots[g]\hat{W}^{-1}[g]\hat{W}[l_W][g^{-1}]^{j-1}$$

we can easily see that $\overline{S}\,\overline{Q}$ is a sequence on H, and the first $[g]\hat{W}^{-1}$ is part of a sequence on gH, the second $[g]\hat{W}^{-1}$ is part of sequence on g^2H, and the last $[g]\hat{W}^{-1}$ combining $[l_W]$ is part of sequence on $g^{j-1}H$. The last $[g^{-1}]^{j-1}$ will trace the sequence through $g^{j-1}H$ to gH and back to the end vertex to form a Hamiltonian circuit on G by connecting the last identity element after the algorithm. Each partial fraction the partial product inside the sequence is product from different quotient groups, which means all are non-identity elements. For the even j case:

$$\overline{S}T = \overline{S}\,\overline{Q}(W, [g]^j)[g](\overline{W})^{-1}[g^{-1}]^{j-1}$$

After expanding this sequence,

$$\overline{S}T = \overline{S}\,\overline{Q}[g]\hat{W}^{-1}[g]\hat{W}\dots[g]\hat{W}^{-1}[g]\hat{W}[g](\overline{W})^{-1}[g^{-1}]^{j-1}$$

By a similar idea, we can easily see that $\overline{S}\,\overline{Q}$ is a sequence on H, and the first $[g]\hat{W}^{-1}$ is part of sequence on gH, the second $[g]\hat{W}^{-1}$ is part of sequence on g^2H, and the last $[g]\hat{W}^{-1}$ is part of sequence on $g^{j-2}H$ by definition of even case. The following $[g](\overline{W})^{-1}$ part is in $g^{j-1}H$ to complete the traverse of elements in the last quotient group because of the definition of $(W, [g]^j)$ would end for $j-2$ if j is even. At last, $[g^{-1}]^{j-1}$ will trace back the sequence through $g^{j-1}H$ to gH and back to the end vertex to form a Hamiltonian circuit on G by connecting the last identity element after the algorithm. Each partial fraction in the partial product inside the sequence is a product from different quotient groups, which means all are non-identity elements. □

To get a better understanding of this lemma, here is an example to get an idea how the algorithm works for a specific case.

Example 6. *Let $G = \mathbb{Z}_{12}$, with generating set $M = \{0, 2, 3, 6\}$. Then:*

$M_0 = \{2, 3, 6\}$.

Let $M' = \{2, 6\}$, and hence $M'^* = \{2, 10, 6\}$.

$\langle M' \rangle = \{0, 2, 4, 6, 8, 10\}$

For sequence from $\mathcal{H}(M', \langle M' \rangle)$: $S = [2, 6, 2, 6, 2, 6]$, and $\overline{S} = [2, 6, 2, 6, 2]$.

then there exists a sequence T on G, s.t. $\overline{S}T \in \mathcal{H}(M, G)$.

Next, to proceed the proof part, $g = 3 \in M_0 \setminus M'$, and $H = \langle M \setminus \{3\} \rangle = \langle \{0, 2, 6\} \rangle = \{0, 2, 4, 6, 8, 10\}$, and $j = 2$ s.t. $3^2 = 3 + 3 = 6 \in H$.

By the induction hypothesis there exists a sequence Q on H, s.t. $\overline{S}Q \in \mathcal{H}(M \setminus \{3\}, H)$

$\mathcal{H}(M \setminus \{3\}, H)$ denotes the set of all hamiltonian $(\{0,2,6\})^*$-sequences on $\{0,2,4,6,8,10\}$, and $(\{0,2,6\})^* = \{2,10,6\}$. Let $Q = [6]$, and $W = \overline{S}Q = [2,6,2,6,2,6]$.

Since $j = 2$ is even, $T = \overline{Q}(W,[g]^j)[g](\overline{W})^{-1}[g^{-1}]^{j-1}$

$\overline{Q} = \square$.

$(W,[g]^j) = \square$, since $j = 2$, following $\hat{W} = [6,2,6,2]$, and $(\hat{W})^{-1} = [10,6,10,6]$.

$[g] = [3]$

$(\overline{W})^{-1} = [10,6,10,6,10]$

$[g^{-1}]^{j-1} = [3^{-1}]^{2-1} = [9]$

$T = \square\square[3][10,6,10,6,10][9] = [3,10,6,10,6,10,9]$.

$\overline{S}T = [2,6,2,6,2,3,10,6,10,6,10,9]$, $r_{\overline{S}T} = 12 = |\mathbb{Z}_{12}|$, and $\pi(\overline{S}T) = 2+6+2+6+2+3+10+6+10+6+10+9 = 72 = 12*6 = 0$. Additionally, each partial is $2,8,10,4,6,9,7,1,11,5,3,12 \neq 0$, matching the requirement that each partial product is distinct and not identity zero, except the last on, which $\pi(\overline{S}T) = 0$.

Thus, $\overline{S}T$ is a hamiltonian sequence.

Theorem 1. *Every connected Cayley graph of an abelian group of order at least three is hamiltonian.*

Proof. By Lemma 3.1, it suffices to show that if M is a generating set of an abelian group G of order at least 3, then $\mathcal{H}(M,G) \neq \emptyset$.

Case 1: If M contains an element x of order $n \geq 3$, then let $M' = \{x\}$ and $S = [x]^n$.

Case 2:If M contains no element of order at least 3, then it contains (since G has order at least 3) two distinct elements y, z of order 2. Then let $M' = \{y,z\}$ and $S = ([y][z])^2$.

It follows by Lemma 3.2 that $\mathcal{H}(M,G) \neq \emptyset$. $\square$

Example 7. *Let $G \cong V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.*

Let $M = \{(0,1),(1,0)\}$. In this case, we could focus on the non-trivial case 2 with element only order 2, and obviously M generates V_4.

$M' = M = \{(0,1),(1,0)\}$, and $S = ([(0,1)],[(1,0)])^2 = [(0,1),(1,0),(0,1),(1,0)]$.

By Lemma 2, since $S \in \mathcal{H}(M', \langle M' \rangle) = \mathcal{H}(M', V_4)$, there exists a sequence T on G such that $\overline{S}T \in \mathcal{H}(H, V_4)$.

Acknowledgements

- Thanks to my Honor Thesis advisor, Professor Denis Osin, for continuous support and guidance throughout this project.
- Previous foundational work by Dragan Marušić, which inspired and informed my research on Hamiltonian circuits in Cayley graphs.

References

[1] D. Marušić, *Hamiltonian Circuits in Cayley Graphs*, Discrete Mathematics, Volume 46, Issue 1, 1983, Pages 49–54.

[2] M. Stelow, *Hamiltonicity in Cayley Graphs and Digraphs of Finite Abelian Groups*, University of Chicago REU Paper, August 2017. Available at: `https://math.uchicago.edu/~may/REU2017/REUPapers/Stelow.pdf`

[3] E. Bajo Calderon, *An Exploration on the Hamiltonicity of Cayley Digraphs*, Master's Thesis, Youngstown State University, 2021. Available at: `https://etd.ohiolink.edu/acprod/odb_etd/ws/send_file/send?accession=ysu161982054497591&disposition=inline`